**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 1 OF 7 (JA0001–JA0919)

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

APPEAL,CLOSED

# U.S. District Court
# District of Maryland (Baltimore)
# CIVIL DOCKET FOR CASE #: 1:15-cv-00662-TSE

Wikimedia Foundation et al v. National Security Agency/Central Security Service et al
Assigned to: Judge T. NA S. Ellis
Case in other court: USCA, 15-02560
US Court of Appeals for the 4th Circuit, 20-01191
Cause: 05:706 Judicial Review of Agency Action

Date Filed: 03/10/2015
Date Terminated: 10/23/2015
Jury Demand: None
Nature of Suit: 440 Civil Rights: Other
Jurisdiction: U.S. Government Defendant

**Plaintiff**

**Wikimedia Foundation** represented by **Alex Abdo**
Knight First Amendment Institute at Columbia University
475 Riverside Dr. Ste. 302
New York, NY 10115
6467458500
Email: alex.abdo@knightcolumbia.org
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Ashley Marie Gorski**
American Civil Liberties Union Foundation
125 Broad St
18th Floor
New York, NY 10004
2122847305
Fax: 2125492654
Email: agorski@aclu.org
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Benjamin Hansel Kleine**
Cooley LLP
101 California St. 5th Floor
San Francisco, CA 94111
4156932000
Fax: 4156932222
Email: bkleine@cooley.com
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Charles Sims**
Proskauer Rose LLP
11 Times Square
New York, NY 10036
2129693950

Fax: 2129692900
Email: csims@proskauer.com
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Alexander Munkittrick**
Proskauer Rose LLP
11 Times Square
New York, NY 10036
2129693226
Fax: 2129692900
Email: dmunkittrick@proskauer.com
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Robert Rocah**
ACLU of Maryland
3600 Clipper Mill Rd, #350
Baltimore, MD 21211
14108898555
Fax: 14103667838
Email: rocah@aclu-md.org
*ATTORNEY TO BE NOTICED*

**Devon Cook**
Cooley LLP
101 California St. 5th Floor
San Francisco, CA 94111
4156932000
Fax: 4156932222
Email: dhanleycook@cooley.com
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jameel Jaffer**
Knight First Amendment Institute at
Columbia University
475 Riverside Drive
Suite 302
New York, NY 10115
6467458500
Email: jameel.jaffer@knightcolumbia.org
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**John Browning**
Proskauer Rose LLP
11 Times Square
New York, NY 10036
2129693452
Fax: 2129692900
Email: jbrowning@proskauer.com
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jonathan Hafetz**
American Civil Liberties Union Foundation
125 Broad St. 18th Fl.
New York, NY 10004
2122847319
Fax: 2125492517
Email: jhafetz@aclu.org
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Molly Smolen**
Cooley LLP
101 California St. 5th Floor
San Francisco, CA 94111
4156932000
Fax: 4156932222
Email: msmolen@cooley.com
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Patrick Toomey**
American Civil Liberties Union Foundation
125 Broad St
18th Floor
New York, NY 10004
2125197816
Fax: 2125492654
Email: ptoomey@aclu.org
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Deborah A Jeon**
American Civil Liberties Union of Maryland Foundation
3600 Clipper Mill Rd Ste 350
Baltimore, MD 21211
14108898555
Fax: 14103667838
Email: jeon@aclu-md.org
*ATTORNEY TO BE NOTICED*

**Plaintiff**

**National Association of Criminal Defense Attorneys**

represented by

**Alex Abdo**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Ashley Marie Gorski**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Charles Sims**

(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Alexander Munkittrick**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Robert Rocah**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Jameel Jaffer**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**John Browning**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jonathan Hafetz**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Patrick Toomey**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Deborah A Jeon**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Plaintiff**

**Human Rights Watch** represented by **Alex Abdo**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Ashley Marie Gorski**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Charles Sims**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Alexander Munkittrick**

(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Robert Rocah**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Jameel Jaffer**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**John Browning**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jonathan Hafetz**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Patrick Toomey**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Deborah A Jeon**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Plaintiff**

**Pen American Center** represented by **Alex Abdo**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Ashley Marie Gorski**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Charles Sims**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Alexander Munkittrick**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Robert Rocah**

(See above for address)
*ATTORNEY TO BE NOTICED*

**Jameel Jaffer**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**John Browning**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jonathan Hafetz**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Patrick Toomey**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Deborah A Jeon**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Plaintiff**

**Global Fund for Women** represented by **Alex Abdo**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Ashley Marie Gorski**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Charles Sims**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Alexander Munkittrick**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Robert Rocah**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Jameel Jaffer**
(See above for address)

*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**John Browning**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jonathan Hafetz**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Patrick Toomey**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Deborah A Jeon**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Plaintiff**

**The Nation Magazine** represented by **Alex Abdo**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Ashley Marie Gorski**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Charles Sims**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Alexander Munkittrick**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Robert Rocah**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Jameel Jaffer**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**John Browning**
(See above for address)

*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jonathan Hafetz**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Patrick Toomey**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Deborah A Jeon**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Plaintiff**

**The Rutherford Institute** represented by **Alex Abdo**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Ashley Marie Gorski**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Charles Sims**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Alexander Munkittrick**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Robert Rocah**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Jameel Jaffer**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**John Browning**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jonathan Hafetz**
(See above for address)

*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Patrick Toomey**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Deborah A Jeon**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Plaintiff**

**Washington Office on Latin America** represented by **Alex Abdo**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Ashley Marie Gorski**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Charles Sims**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Alexander Munkittrick**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Robert Rocah**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Jameel Jaffer**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**John Browning**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jonathan Hafetz**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Patrick Toomey**
(See above for address)

*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Deborah A Jeon**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Plaintiff**

**Amnesty International USA** represented by **Alex Abdo**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Ashley Marie Gorski**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Charles Sims**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Alexander Munkittrick**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**David Robert Rocah**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Jameel Jaffer**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**John Browning**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jonathan Hafetz**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Patrick Toomey**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Deborah A Jeon**

(See above for address)
*ATTORNEY TO BE NOTICED*

V.

**Defendant**

**National Security Agency/Central Security Service**

represented by **James Jordan Gilligan**
United States Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, N.W.
Room 11200
Washington, DC 20005
2025143358
Fax: 2026168470
Email: james.gilligan@usdoj.gov
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Julia Alexandra Berman**
United States Department of Justice
Civil Division Federal Programs Branch
1100 L Street, NW
Washington, DC 20005
2026168480
Fax: 2026168470
Email: julia.heiman@usdoj.gov
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Olivia R. Hussey Scott**
USDOJ Civil Division
1100 L Street, N.W.
Room 11112
Washington, DC 20005
2026168491
Fax: 2026168470
Email: Olivia.Hussey.Scott@usdoj.gov
*ATTORNEY TO BE NOTICED*

**Rodney Patton**
United States Department of Justice
20 Massachusetts Ave
Rm 7320
Washington, DC 20530
2023057919
Fax: 2026168470
Email: rodney.patton@usdoj.gov
*ATTORNEY TO BE NOTICED*

**Timothy A Johnson**
Dept. of Justice
20 Massachusetts Ave NW
Washington, DC 20530

2025141359
Fax: 2026168470
Email: timothy.johnson4@usdoj.gov

**Defendant**

**Adm. Michael S. Rogers**
*in his official capacity as Director of the National Security Agency and Chief of the Central Security Service*

represented by **James Jordan Gilligan**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Julia Alexandra Berman**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Olivia R. Hussey Scott**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Rodney Patton**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Timothy A Johnson**
(See above for address)

**Defendant**

**Office of the Director of National Intelligence**

represented by **James Jordan Gilligan**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Julia Alexandra Berman**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Olivia R. Hussey Scott**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Rodney Patton**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Timothy A Johnson**
(See above for address)

**Defendant**

**James R. Clapper**
*in his official capacity as Director of National Intelligence*

represented by **James Jordan Gilligan**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Julia Alexandra Berman**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Olivia R. Hussey Scott**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Rodney Patton**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Timothy A Johnson**
(See above for address)

**Defendant**

**Department of Justice** represented by **James Jordan Gilligan**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Julia Alexandra Berman**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Olivia R. Hussey Scott**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Rodney Patton**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Timothy A Johnson**
(See above for address)

**Defendant**

**Eric H. Holder** represented by **James Jordan Gilligan**
*in his official capacity as Attorney General of the United States*
*TERMINATED: 06/22/2015*
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Julia Alexandra Berman**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Olivia R. Hussey Scott**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Rodney Patton**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Defendant**

**Loretta E. Lynch**
*in her official capacity as Attorney General of the United States*

represented by **James Jordan Gilligan**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Julia Alexandra Berman**
(See above for address)
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Olivia R. Hussey Scott**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Rodney Patton**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Timothy A Johnson**
(See above for address)

**Amicus**

**CloudFlare**
*CloudFlare*

represented by **Jeffrey Landis**
ZwillGen PLLC
1900 M Street, NW
Suite 250
Washington, DC 20036
12027065203
Fax: 12027065298
Email: jeff@zwillgen.com

**Jennifer Stisa Granick**
Stanford Center for Internet and Society
559 Nathan Abbot Way
Stanford, CA 94305
6507368675
Email: jennifer@law.stanford.edu
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Amicus**

**The Tor Project, Inc.**
*The Tor Project, Inc.*

represented by **Jeffrey Landis**
(See above for address)

**Jennifer Stisa Granick**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Amicus**

**RiseUp**
*RiseUp*

represented by **Jeffrey Landis**
(See above for address)

**Jennifer Stisa Granick**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Amicus**

**First Amendment Legal Scholars**

represented by **Emily Lange Levenson**
Brown, Goldstein & Levy LLP
120 E. Baltimore St
Suite 1700
Baltimore, MD 21202
4109621030
Fax: 4103850869
Email: elevenson@browngold.com
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Joshua R Treem**
Brown Goldstein Levy LLP
120 E Baltimore St Ste 1700
Baltimore, MD 21202
14109621030
Fax: 14103850869
Email: jtreem@browngold.com
*LEAD ATTORNEY*
*ATTORNEY TO BE NOTICED*

**Margot E Kaminski**
Moritz College of Law, The Ohio State University
55 W 12th Ave
Columbus, OH 43210
6142922092
Email: kaminski.217@osu.edu
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Amicus**

**The American Booksellers Association**

represented by **Andrew Gellis Crocker**
Electronic Frontier Foundation
815 Eddy St
San Franscisco, CA 94109
4154369333
Fax: 4154369993
Email: andrew@eff.org
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jan Ingham Berlage**

Gohn Hankey & Berlage, LLP
201 N Charles St Ste 2101
Baltimore, MD 21201
14107529300
Fax: 14107522519
Email: jberlage@ghsllp.com
*ATTORNEY TO BE NOTICED*

**Amicus**

**American Library Association** represented by **Andrew Gellis Crocker**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jan Ingham Berlage**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Amicus**

**Association of Research Libraries** represented by **Andrew Gellis Crocker**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jan Ingham Berlage**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Amicus**

**Freedom to Read Foundation** represented by **Andrew Gellis Crocker**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jan Ingham Berlage**
(See above for address)
*ATTORNEY TO BE NOTICED*

**Amicus**

**International Federation of Library Associations and Institutions** represented by **Andrew Gellis Crocker**
(See above for address)
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**Jan Ingham Berlage**
(See above for address)
*ATTORNEY TO BE NOTICED*

| Date Filed | # | Docket Text |
|---|---|---|
| 03/10/2015 | 1 | COMPLAINT *for Declaratory and Injunctive Relief* against All Defendants ( Filing fee $ 400 receipt number 0416-5260730.), filed by The Nation Magazine, Human Rights Watch, The Rutherford Institute, National Association of Criminal Defense Attorneys, |

| | | |
|---|---|---|
| | | Washington Office on Latin America, Pen American Center, Wikimedia Foundation, Global Fund for Women, Amnesty International USA. (Attachments: # 1 Civil Cover Sheet, # 2 Summonses)(Jeon, Deborah) (Entered: 03/10/2015) |
| 03/10/2015 | 2 | NOTICE by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation *Summons to U.S. Attorney* (Jeon, Deborah) (Entered: 03/10/2015) |
| 03/10/2015 | 3 | Summons Issued 60 days as to James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers, U.S. Attorney and U.S. Attorney General (bmhs, Deputy Clerk) (Entered: 03/10/2015) |
| 03/10/2015 | 4 | MOTION to Appear Pro Hac Vice for Alex Abdo ( Filing fee $ 50, receipt number 0416-5262165.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015) |
| 03/10/2015 | 5 | MOTION to Appear Pro Hac Vice for Ashley Gorski ( Filing fee $ 50, receipt number 0416-5262203.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015) |
| 03/10/2015 | 6 | MOTION to Appear Pro Hac Vice for Jameel Jaffer ( Filing fee $ 50, receipt number 0416-5262236.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015) |
| 03/10/2015 | 7 | MOTION to Appear Pro Hac Vice for Patrick Toomey ( Filing fee $ 50, receipt number 0416-5262246.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Rocah, David) (Entered: 03/10/2015) |
| 03/10/2015 | 8 | QC NOTICE: 4 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015) |
| 03/10/2015 | 9 | QC NOTICE: 5 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015) |
| 03/10/2015 | 10 | QC NOTICE: 6 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See |

| | | |
|---|---|---|
| | | attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015) |
| 03/10/2015 | 11 | QC NOTICE: 7 Motion to Appear Pro Hac Vice, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA needs to be modified. See attachment for details and corrective actions needed regarding the signature(s) on the motion. (bu, Deputy Clerk) (Entered: 03/10/2015) |
| 03/11/2015 | 12 | CORRECTED MOTION to Appear Pro Hac Vice for Alex Abdo by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 13 | CORRECTED MOTION to Appear Pro Hac Vice for Ashley Gorski by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 14 | PAPERLESS ORDER granting 12 Corrected Motion to Appear Pro Hac Vice on behalf of Alex Abdo. Directing attorney Alex Abdo to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015) |
| 03/11/2015 | 15 | PAPERLESS ORDER granting 13 Corrected Motion to Appear Pro Hac Vice on behalf of Ashley Gorski. Directing attorney Ashley Gorski to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015) |
| 03/11/2015 | 16 | CORRECTED MOTION to Appear Pro Hac Vice for Jameel Jaffer by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 17 | CORRECTED MOTION to Appear Pro Hac Vice for Patrick Toomey by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page). The fee has already been paid.(Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 18 | MOTION to Appear Pro Hac Vice for Charles Sims ( Filing fee $ 50, receipt number 0416-5265356.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page)(Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 19 | MOTION to Appear Pro Hac Vice for David Munkittrick ( Filing fee $ 50, receipt number 0416-5265372.) by Amnesty International USA, Global Fund for Women, |

| | | |
|---|---|---|
| | | Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page)(Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 20 | MOTION to Appear Pro Hac Vice for John Browning ( Filing fee $ 50, receipt number 0416-5265384.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation (Attachments: # 1 Signature page)(Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 21 | PAPERLESS ORDER granting 16 Corrected Motion to Appear Pro Hac Vice on behalf of Jameel Jaffer. Directing attorney Jameel Jaffer to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015) |
| 03/11/2015 | 22 | PAPERLESS ORDER granting 17 Corrected Motion to Appear Pro Hac Vice on behalf of Patrick Toomey. Directing attorney Patrick Toomey to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015) |
| 03/11/2015 | 23 | PAPERLESS ORDER granting 18 Motion to Appear Pro Hac Vice on behalf of Charles Sims. Directing attorney Charles Sims to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015) |
| 03/11/2015 | 24 | PAPERLESS ORDER granting 19 Motion to Appear Pro Hac Vice on behalf of David Munkittrick. Directing attorney David Munkittrick to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015) |
| 03/11/2015 | 25 | PAPERLESS ORDER granting 20 Motion to Appear Pro Hac Vice on behalf of John Browning. Directing attorney John Browning to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 3/11/2015. (bu, Deputy Clerk) (Entered: 03/11/2015) |
| 03/11/2015 | 26 | Local Rule 103.3 Disclosure Statement by Amnesty International USA. (Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 27 | Local Rule 103.3 Disclosure Statement by Global Fund for Women. (Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 28 | Local Rule 103.3 Disclosure Statement by Human Rights Watch. (Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 29 | Local Rule 103.3 Disclosure Statement by National Association of Criminal Defense Attorneys identifying Other Affiliate Foundation for Criminal Justice for National Association of Criminal Defense Attorneys.. (Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 30 | Local Rule 103.3 Disclosure Statement by Pen American Center. (Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 31 | Local Rule 103.3 Disclosure Statement by The Rutherford Institute. (Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 32 | Local Rule 103.3 Disclosure Statement by The Nation Magazine. (Rocah, David) (Entered: 03/11/2015) |

| | | |
|---|---|---|
| 03/11/2015 | 33 | Local Rule 103.3 Disclosure Statement by Wikimedia Foundation. (Rocah, David) (Entered: 03/11/2015) |
| 03/11/2015 | 34 | Local Rule 103.3 Disclosure Statement by Washington Office on Latin America. (Rocah, David) (Entered: 03/11/2015) |
| 03/17/2015 | 35 | (FILED IN ERROR) AFFIDAVIT of Service for Summons served on United States Attorney for the District of Maryland on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015) |
| 03/17/2015 | 36 | (FILED IN ERROR) AFFIDAVIT of Service for Summons served on Office of the Director of National Intelligence on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015) |
| 03/17/2015 | 37 | (FILED IN ERROR) AFFIDAVIT of Service for Summons served on National Security Agency / Central Security Service on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015) |
| 03/17/2015 | 38 | (FILED IN ERROR) AFFIDAVIT of Service for Summons served on Department of Justice on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015) |
| 03/17/2015 | 39 | (FILED IN ERROR) AFFIDAVIT of Service for Summons served on Adm. Michael S. Rogers on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015) |
| 03/17/2015 | 40 | (FILED IN ERROR) AFFIDAVIT of Service for Summons served on Director of National Intelligence James R. Clapper on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015) |
| 03/17/2015 | 41 | (FILED IN ERROR) AFFIDAVIT of Service for Summons served on Attorney General Eric H. Holder, Jr. on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) Modified on 3/17/2015 (bmhs, Deputy Clerk). (Entered: 03/17/2015) |
| 03/17/2015 | 42 | QC NOTICE: 35 Affidavit of Service filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, |

| | | |
|---|---|---|
| | | Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA was filed incorrectly. ***Incorrect event was selected. Please refile using the event under Service of Process - Summons Returned Executed as to USA AND case caption and case number are missing. It has been noted as FILED IN ERROR, and the document link has been disabled.* (bmhs, Deputy Clerk) (Entered: 03/17/2015) |
| 03/17/2015 | 43 | QC NOTICE: 36 37 38 39 40 41 Affidavits of Service filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA were filed incorrectly. ***Case caption and case number are missing. It has been noted as FILED IN ERROR, and the document link has been disabled.* (bmhs, Deputy Clerk) (Entered: 03/17/2015) |
| 03/17/2015 | 44 | SUMMONS Returned Executed by The Nation Magazine, Amnesty International USA, Human Rights Watch, The Rutherford Institute, National Association of Criminal Defense Attorneys, Washington Office on Latin America, Wikimedia Foundation, Pen American Center, Global Fund for Women. James R. Clapper served on 3/10/2015, answer due 5/11/2015; Department of Justice served on 3/10/2015, answer due 5/11/2015; Eric H. Holder served on 3/10/2015, answer due 5/11/2015; National Security Agency/Central Security Service served on 3/10/2015, answer due 5/11/2015; Office of the Director of National Intelligence served on 3/10/2015, answer due 5/11/2015; Michael S. Rogers served on 3/10/2015, answer due 5/11/2015. (Toomey, Patrick) (Entered: 03/17/2015) |
| 03/17/2015 | 45 | AFFIDAVIT of Service for Summons served on Office of the Director of National Intelligence on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015) |
| 03/17/2015 | 46 | AFFIDAVIT of Service for Summons served on National Security Agency / Central Security Service on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015) |
| 03/17/2015 | 47 | AFFIDAVIT of Service for Summons served on Director of National Intelligence James R. Clapper on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015) |
| 03/17/2015 | 48 | AFFIDAVIT of Service for Summons served on Department of Justice on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015) |
| 03/17/2015 | 49 | AFFIDAVIT of Service for Summons served on Adm. Michael S. Rogers on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015) |
| 03/17/2015 | 50 | AFFIDAVIT of Service for Summons served on Attorney General Eric H. Holder, Jr. on 3/10/2015, filed by Amnesty International USA, Global Fund for Women, Human Rights |

| | | |
|---|---|---|
| | | Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. (Toomey, Patrick) (Entered: 03/17/2015) |
| 03/19/2015 | 51 | NOTICE of Appearance by James Jordan Gilligan on behalf of All Defendants (Gilligan, James) (Entered: 03/19/2015) |
| 03/23/2015 | 52 | NOTICE of Appearance by Rodney Patton on behalf of James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Patton, Rodney) (Entered: 03/23/2015) |
| 03/24/2015 | 53 | NOTICE of Appearance by Julia Alexandra Berman on behalf of All Defendants (Berman, Julia) (Entered: 03/24/2015) |
| 03/26/2015 | | Case reassigned to Judge T. S. Ellis. Judge Richard D Bennett no longer assigned to the case. (cags, Deputy Clerk) (Entered: 03/26/2015) |
| 04/24/2015 | 54 | MOTION to Set a Status Conference by James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 5/11/2015 (Attachments: # 1 Exhibit 1, # 2 Text of Proposed Order)(Berman, Julia) (Entered: 04/24/2015) |
| 04/28/2015 | 55 | RESPONSE to Motion re 54 MOTION to Set a Status Conference filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. Replies due by 5/15/2015. (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 04/28/2015) |
| 04/30/2015 | 56 | ORDER granting 54 Defendants' Motion to set a status conference; and scheduling a status conference for 3:30 p.m. on Wednesday, May 13, 2015. Signed by Judge T. S. Ellis on 4/30/2015. (bmhs, Deputy Clerk) (Entered: 04/30/2015) |
| 05/06/2015 | 57 | Correspondence re: Request Pursuant to D. Md. Local Rule 101.1(b)(i) for May 13, 2015 Status Conference (Toomey, Patrick) (Entered: 05/06/2015) |
| 05/11/2015 | 58 | ORDER granting 57 Plaintiffs' Letter Motion. Signed by Judge T. S. Ellis on 5/11/15. (bmhs, Deputy Clerk) (Entered: 05/11/2015) |
| 05/12/2015 | 59 | PAPERLESS ORDER, for good cause, it is hereby ORDERED that the status conference scheduled to be heard at the Greenbelt Courthouse at 3:30 p.m. on Wednesday, May 13, 2015, is CANCELED. Instead, a telephone conference is SCHEDULED for the same date and time (3:30 p.m. on Wednesday, May 13, 2015). In this regard, all participating counsel are DIRECTED first to conference themselves together on one phone line and then to call Chambers at (703) 299-2114 to commence the conference call. Signed by Judge T. S. Ellis on 5/12/2015. (bmhs, Deputy Clerk) (Entered: 05/12/2015) |
| 05/14/2015 | 60 | Telephone Conference held on 5/14/2015 before Judge T. S. Ellis. (bmhs, Deputy Clerk) (Entered: 05/15/2015) |
| 05/14/2015 | 61 | ORDER directing parties to comply with the briefing and argument schedule. Signed by Judge T. S. Ellis on 5/13/2015. (bmhs, Deputy Clerk) (Entered: 05/15/2015) |
| 05/27/2015 | 62 | MOTION to Set a Date for the Filing of Amicus Briefs by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by |

| | | |
|---|---|---|
| | | 6/15/2015 (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 05/27/2015) |
| 05/28/2015 | 63 | ORDER denying 62 Motion to Set a Date for the Filing of Amicus Briefs. Signed by Judge T. S. Ellis on 5/28/2015. (bmhs, Deputy Clerk) (Entered: 05/28/2015) |
| 05/29/2015 | 64 | Joint MOTION to Conduct Hearings in Alexandria, Virginia by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 6/15/2015 (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 05/29/2015) |
| 05/29/2015 | 65 | ORDER granting 64 Joint Motion to Conduct Hearings in Alexandria, Virginia. Signed by Judge T. S. Ellis on 5/29/2015. (bmhs, Deputy Clerk) (Entered: 05/29/2015) |
| 05/29/2015 | 66 | MOTION to Dismiss for Lack of Jurisdiction *Under Rule 12(b)(1)* by James R. Clapper, Department of Justice, Eric H. Holder, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 6/15/2015 (Attachments: # 1 Memorandum of Law in Support of Motion to Dismiss, # 2 Text of Proposed Order, # 3 Exhibit Exhibit List, # 4 Exhibit Exhibit 1, # 5 Exhibit Exhibit 2, # 6 Exhibit Exhibit 3, # 7 Exhibit Exhibit 4A, # 8 Exhibit Exhibit 4B, # 9 Exhibit Exhibit 4C, # 10 Exhibit Exhibit 4D, # 11 Exhibit Exhibit 5, # 12 Exhibit Exhibit 6)(Patton, Rodney) (Entered: 05/29/2015) |
| 06/12/2015 | 67 | Joint MOTION to Amend the Briefing Schedule by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 6/29/2015 (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 06/12/2015) |
| 06/12/2015 | 68 | ORDER granting 67 Joint Motion to Amend the Briefing Scheduling governing Defendants' Motion to Dismiss; and postponing the oral argument on Defendants' Motion to Dismiss. Signed by Judge T. S. Ellis on 6/12/2015. (bmhs, Deputy Clerk) (Entered: 06/15/2015) |
| 06/12/2015 | 69 | ORDER amending the briefing schedule. Signed by Judge T. S. Ellis on 6/12/2015. (bmhs, Deputy Clerk) (Entered: 06/15/2015) |
| 06/19/2015 | 70 | MOTION to Amend/Correct 1 Complaint, by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 7/9/2015 (Attachments: # 1 First Amended Complaint, # 2 First Amended Complaint - Redline, # 3 Text of Proposed Order)(Toomey, Patrick) (Entered: 06/19/2015) |
| 06/22/2015 | 71 | ORDER granting 70 Plaintiffs' Motion to Amend the Complaint; and denying as moot 66 Defendants' Motion to Dismiss. Signed by Judge T. S. Ellis on 6/22/2015. (bmhs, Deputy Clerk) (Entered: 06/22/2015) |
| 06/22/2015 | 72 | AMENDED COMPLAINT against James R. Clapper, Department of Justice, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers, Loretta E. Lynch filed by The Nation Magazine, Amnesty International USA, Human Rights Watch, The Rutherford Institute, National Association of Criminal Defense Attorneys, Washington Office on Latin America, Wikimedia Foundation, Pen American Center, Global Fund for Women. (Attachments: # 1 Red Line Complaint)(bmhs, Deputy Clerk) (Entered: 06/22/2015) |

| | | |
|---|---|---|
| 06/27/2015 | 73 | Consent MOTION for Extension of Time by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 7/16/2015 (Attachments: # 1 Text of Proposed Order)(Berman, Julia) (Entered: 06/27/2015) |
| 06/29/2015 | 74 | ORDER granting 73 Consent Motion for Extension of Time. Signed by Judge T. S. Ellis on 6/29/2015. (bmhs, Deputy Clerk) (Entered: 06/29/2015) |
| 07/31/2015 | 75 | MOTION to Appear Pro Hac Vice for Jennifer Stisa Granick ( Filing fee $ 50, receipt number 0416-5525629.) by CloudFlare, The Tor Project, Inc., RiseUp (Landis, Jeffrey) (Entered: 07/31/2015) |
| 08/03/2015 | 76 | PAPERLESS ORDER granting 75 Motion to Appear Pro Hac Vice on behalf of Jennifer Stisa Granick. Directing attorney Jennifer Stisa Granick to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 8/3/2015. (bu, Deputy Clerk) (Entered: 08/03/2015) |
| 08/06/2015 | 77 | MOTION to Dismiss for Lack of Jurisdiction by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers Responses due by 8/24/2015 (Attachments: # 1 (Memorandum in Support), # 2 Affidavit (Salzberg Declaration), # 3 Affidavit (Lee Declaration Part 1), # 4 Affidavit (Lee Declaration Part 2), # 5 Affidavit (Lee Declaration Part 3), # 6 Affidavit (Lee Declaration Part 4), # 7 Affidavit (Lee Declaration Part 5), # 8 Exhibit 1, # 9 Exhibit 2, # 10 Exhibit 3, # 11 Exhibit 4, # 12 Exhibit 5, # 13 Exhibit 6, # 14 Exhibit 7, # 15 Exhibit 8, # 16 Exhibit 9, # 17 (Index of Exhibits), # 18 Text of Proposed Order)(Gilligan, James) (Entered: 08/06/2015) |
| 09/03/2015 | 78 | NOTICE of Appearance by Joshua R Treem on behalf of First Amendment Legal Scholars (Treem, Joshua) (Entered: 09/03/2015) |
| 09/03/2015 | 79 | NOTICE of Appearance by Emily Lange Levenson on behalf of First Amendment Legal Scholars (Levenson, Emily) (Entered: 09/03/2015) |
| 09/03/2015 | 80 | MOTION to Appear Pro Hac Vice ( Filing fee $ 50, receipt number 0416-5581832.) by First Amendment Legal Scholars (Treem, Joshua) (Entered: 09/03/2015) |
| 09/03/2015 | 81 | NOTICE of Appearance by Jan Ingham Berlage on behalf of The American Booksellers Association, American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions (Berlage, Jan) (Entered: 09/03/2015) |
| 09/03/2015 | 82 | MOTION for Leave to File *to File Brief of Amici Curiae in Support of Plaintiffs' Opposition to Defendants' Motion to Dismiss* by American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions, The American Booksellers Association Responses due by 9/21/2015 (Attachments: # 1 Brief in Opposition to Defendants' Motion to Dismiss)(Berlage, Jan) (Entered: 09/03/2015) |
| 09/03/2015 | 83 | MOTION to Appear Pro Hac Vice for Andrew Crocker ( Filing fee $ 50, receipt number 0416-5582368.) by American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions, The American Booksellers Association (Berlage, Jan) (Entered: 09/03/2015) |
| 09/03/2015 | 84 | NOTICE by American Library Association, Association of Research Libraries, Freedom to Read Foundation, International Federation of Library Associations and Institutions, The American Booksellers Association re 81 Notice of Appearance, 82 MOTION for Leave to File *to File Brief of Amici Curiae in Support of Plaintiffs' Opposition to Defendants' Motion to Dismiss*, 83 MOTION to Appear Pro Hac Vice for Andrew |

| | | |
|---|---|---|
| | | Crocker ( Filing fee $ 50, receipt number 0416-5582368.) *of Service* (Berlage, Jan) (Entered: 09/03/2015) |
| 09/03/2015 | 85 | MOTION for Leave to File *Brief of Amicus Curiae* by First Amendment Legal Scholars Responses due by 9/21/2015 (Attachments: # 1 Brief of Amicus Curiae First Amendment Legal Scholars, # 2 Text of Proposed Order)(Treem, Joshua) (Entered: 09/03/2015) |
| 09/03/2015 | 86 | RESPONSE in Opposition re 77 MOTION to Dismiss for Lack of Jurisdiction filed by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. Replies due by 9/21/2015. (Toomey, Patrick) (Entered: 09/03/2015) |
| 09/09/2015 | 87 | PAPERLESS ORDER granting 80 Motion to Appear Pro Hac Vice on behalf of Margot E Kaminski. Directing attorney Margot E Kaminski to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 9/9/2015. (srd, Intern) (Entered: 09/09/2015) |
| 09/09/2015 | 88 | PAPERLESS ORDER granting 83 Motion to Appear Pro Hac Vice on behalf of Andrew Crocker. Directing attorney Andrew Crocker to register online for CM/ECF at https://www.mdd.uscourts.gov/attyregB/inputProHac.asp. Signed by Clerk on 9/9/2015. (srd, Intern) (Entered: 09/09/2015) |
| 09/17/2015 | 89 | REPLY to Response to Motion re 77 MOTION to Dismiss for Lack of Jurisdiction filed by James R. Clapper, Department of Justice, Eric H. Holder, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers. (Attachments: # 1 Exhibit 1)(Gilligan, James) (Entered: 09/17/2015) |
| 09/25/2015 | 90 | Status Conference held on 9/25/2015 before Judge T. S. Ellis. (Court Reporter: M. Pham) (bmhs, Deputy Clerk) (Entered: 09/28/2015) |
| 09/25/2015 | 91 | ORDER taking under advisment 77 Defendant's MOTION to Dismiss for Lack of Jurisdiction. Signed by Judge T. S. Ellis on 9/25/2015. (bmhs, Deputy Clerk) (Entered: 09/28/2015) |
| 10/22/2015 | 92 | MOTION to Withdraw as Attorney by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation Responses due by 11/9/2015 (Attachments: # 1 Text of Proposed Order)(Rocah, David) (Entered: 10/22/2015) |
| 10/23/2015 | 93 | MEMORANDUM OPINION. Signed by Judge T. S. Ellis on 10/23/2015. (bmhs, Deputy Clerk) (Entered: 10/23/2015) |
| 10/23/2015 | 94 | ORDER granting 82 85 amici curiae's Motions for Leave to File amicus curiae briefs. Signed by Judge T. S. Ellis on 10/23/2015. (bmhs, Deputy Clerk) (Entered: 10/23/2015) |
| 10/23/2015 | 95 | ORDER granting 77 Defendants' Motion to Dismiss. Signed by Judge T. S. Ellis on 10/23/2015. (bmhs, Deputy Clerk) (Entered: 10/23/2015) |
| 12/15/2015 | 96 | NOTICE OF APPEAL as to 95 Order on Motion to Dismiss/Lack of Jurisdiction by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation. Filing fee $ 505, receipt number 0416-5759619. (Toomey, Patrick) (Entered: 12/15/2015) |
| 12/17/2015 | 97 | Transmission of Notice of Appeal and Docket Sheet to US Court of Appeals re 96 Notice of Appeal. IMPORTANT NOTICE: To access forms which you are required to file with the United States Court of Appeals for the Fourth Circuit please go to |

| | | |
|---|---|---|
| | | http://www.ca4.uscourts.gov and click on Forms & Notices. (sls, Deputy Clerk) (Entered: 12/17/2015) |
| 12/18/2015 | 98 | USCA Case Number 15-2560 for 96 Notice of Appeal, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA. Case Manager - RJ Warren (ko, Deputy Clerk) (Entered: 12/18/2015) |
| 12/29/2015 | 99 | (ELECTRONICALLY FILED IN ERROR)TRANSCRIPT REQUEST by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation for proceedings held on September 25, 2015 before Judge T.S. Ellis, III.. (Toomey, Patrick) Modified on 12/29/2015 (slss, Deputy Clerk). (Entered: 12/29/2015) |
| 01/04/2016 | 100 | NOTICE OF FILING OF OFFICIAL TRANSCRIPT for dates of September 25, 2015, before Judge T.S. Ellis, III, re 96 Notice of Appeal, Court Reporter/Transcriber Michael A. Rodriquez, Telephone number 301-213-4913. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Does this satisfy all appellate orders for this reporter? - Y. Redaction Request due 1/25/2016. Redacted Transcript Deadline set for 2/4/2016. Release of Transcript Restriction set for 4/4/2016. (jbps, Deputy Clerk) (Entered: 01/04/2016) |
| 05/23/2017 | 101 | JUDGMENT of USCA (certified copy) affirming in part and vacating in part the judgment of the district court; remanding the case to the district court for further proceedings consistent with the court's decision as to 96 Notice of Appeal, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA (kr2, Deputy Clerk) (Entered: 05/23/2017) |
| 07/17/2017 | 102 | MANDATE of USCA issued as to 96 Notice of Appeal, filed by Wikimedia Foundation, Pen American Center, The Nation Magazine, National Association of Criminal Defense Attorneys, Global Fund for Women, Human Rights Watch, Washington Office on Latin America, The Rutherford Institute, Amnesty International USA (ko, Deputy Clerk) (Entered: 07/17/2017) |
| 07/17/2017 | 103 | MOTION for a Status Conference by Wikimedia Foundation (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 07/17/2017) |
| 07/31/2017 | 104 | RESPONSE to Motion re 103 MOTION for a Status Conference filed by National Security Agency/Central Security Service, Office of the Director of National Intelligence. (Attachments: # 1 Text of Proposed Order)(Berman, Julia) (Entered: 07/31/2017) |
| 08/02/2017 | 105 | ORDER granting 103 Motion for a Status Conference and Briefing Schedule; directing Plaintiff to submit a brief; and scheduling a hearing. Signed by Judge T. S. Ellis on 8/2/2017. (bmhs, Deputy Clerk) (Entered: 08/02/2017) |
| 08/03/2017 | 106 | MOTION to Appear Pro Hac Vice for Jonathan Hafetz (Filing fee $100, receipt number 0416-6813625.) by Amnesty International USA, Global Fund for Women, Human Rights Watch, National Association of Criminal Defense Attorneys, Pen American Center, The Nation Magazine, The Rutherford Institute, Washington Office on Latin America, Wikimedia Foundation(Rocah, David) (Entered: 08/03/2017) |
| 08/11/2017 | 107 | RESPONSE re 105 Order on Motion for Miscellaneous Relief filed by Wikimedia |

| | | |
|---|---|---|
| | | Foundation.(Toomey, Patrick) (Entered: 08/11/2017) |
| 08/15/2017 | 108 | PAPERLESS ORDER granting 106 Motion to Appear Pro Hac Vice on behalf of Jonathan Hafetz. Directing attorney Jonathan Hafetz to register online for CM/ECF at http://www.mdd.uscourts.gov/electronic-case-filing-registration. Signed by Clerk on 8/15/2017. (srd, Deputy Clerk) (Entered: 08/15/2017) |
| 08/26/2017 | 109 | RESPONSE re 107 Response *(Defendants' Response to Plaintiff's Brief Regarding How This Matter Should Proceed)* filed by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers.(Gilligan, James) (Entered: 08/26/2017) |
| 08/28/2017 | 110 | Consent MOTION for Extension of Time *(Unopposed Motion For An Eight-Hour Extension Of Time Nunc Pro Tunc To File Defendants Response To Plaintiffs Brief Regarding How This Matter Should Proceed)* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 08/28/2017) |
| 09/01/2017 | 111 | RESPONSE re 109 Response, filed by Wikimedia Foundation.(Toomey, Patrick) (Entered: 09/01/2017) |
| 09/06/2017 | 112 | PAPERLESS ORDER rescheduling the status conference from September 8, 2017 to September 22, 2017 at 1:00 p.m. Signed by Judge T. S. Ellis on 9/6/2017. (bmhs, Deputy Clerk) (Entered: 09/06/2017) |
| 09/13/2017 | 113 | NOTICE of Appearance by Timothy A Johnson on behalf of All Defendants (Johnson, Timothy) (Entered: 09/13/2017) |
| 09/22/2017 | 115 | Status Conference held on 9/22/2017 before Judge T. S. Ellis.(Court Reporter: Michael A. Rodriquez) (bmhs, Deputy Clerk) (Entered: 09/28/2017) |
| 09/27/2017 | 114 | ORDER directing parties to file a joint status plan for discovery on jurisdictional issues. Signed by Judge T. S. Ellis on 9/25/2017. (bmhs, Deputy Clerk) (Entered: 09/27/2017) |
| 09/28/2017 | 116 | REPORT of Rule 26(f) Planning Meeting (Attachments: # 1 Text of Proposed Order) (Patton, Rodney) (Entered: 09/28/2017) |
| 10/03/2017 | 117 | ORDER granting parties 5 months of discovery to commence on 10/17/17. Signed by Judge T. S. Ellis on 10/3/2017. (bmhs, Deputy Clerk) (Entered: 10/05/2017) |
| 10/16/2017 | 118 | ANSWER to 72 Amended Complaint,, by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers.(Gilligan, James) (Entered: 10/16/2017) |
| 12/28/2017 | 119 | NOTICE by Wikimedia Foundation *of Stipulated Protective Order* (Gorski, Ashley) (Entered: 12/28/2017) |
| 12/29/2017 | 120 | STIPULATED PROTECTIVE ORDER Approving terms and conditions of parties re: confidential information. Signed by Judge T. S. Ellis on 12/29/2017 (cags, Deputy Clerk) (Entered: 12/29/2017) |
| 01/12/2018 | 121 | NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on 9/22/17, before Judge T.S. Ellis, III. Court Reporter/Transcriber Tonia M. Harris. Total number of pages filed: 50. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Redaction Request due 2/2/2018. Redacted Transcript Deadline set for |

| | | |
|---|---|---|
| | | 2/12/2018. Release of Transcript Restriction set for 4/12/2018.(bmhs, Deputy Clerk) (Entered: 01/12/2018) |
| 03/12/2018 | 122 | Joint MOTION for Other Relief *(Joint Motion to Continue Discovery Deadline Pending Parties Submission of a Proposed Schedule for Completion of Jurisdictional Discovery)* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 03/12/2018) |
| 03/15/2018 | 123 | ORDER denying 122 Joint Motion to Continue Discovery Deadline Pending Parties Submission of a Proposed Schedule for Completion of Jurisdictional Discovery. Signed by Judge T. S. Ellis on 3/15/2018. (bmhs, Deputy Clerk) (Entered: 03/16/2018) |
| 03/22/2018 | 124 | Joint MOTION for Other Relief *(Joint Motion to Set Briefing Schedule for Motions to Compel)* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order, # 2 Exhibit A - Memorandum from Attorney General)(Johnson, Timothy) (Entered: 03/22/2018) |
| 03/26/2018 | 125 | Local Rule 104.7 Certificate (Attachments: # 1 Motion to Compel Discovery Responses and Deposition Testimony, # 2 Memorandum in Support of Motion to Compel, # 3 Affidavit Declaration of Patrick Toomey, # 4 Exhibit 1, # 5 Exhibit 2, # 6 Exhibit 3, # 7 Exhibit 4, # 8 Exhibit 5, # 9 Exhibit 6, # 10 Exhibit 7, # 11 Exhibit 8, # 12 Exhibit 9, # 13 Exhibit 10, # 14 Exhibit 11, # 15 Exhibit 12, # 16 Exhibit 13, # 17 Exhibit 14, # 18 Exhibit 15, # 19 Exhibit 16, # 20 Exhibit 17, # 21 Exhibit 18, # 22 Exhibit 19, # 23 Exhibit 20, # 24 Exhibit 21, # 25 Exhibit 22, # 26 Exhibit 23, # 27 Exhibit 24, # 28 Exhibit 25, # 29 Exhibit 26, # 30 Exhibit 27, # 31 Exhibit 28, # 32 Exhibit 29, # 33 Exhibit 30, # 34 Text of Proposed Order)(Toomey, Patrick) (Entered: 03/26/2018) |
| 03/26/2018 | 126 | MOTION to Compel *Discovery* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Exhibit (Memorandum in Support), # 2 Exhibit (Exhibit 1), # 3 Exhibit (Exhibit 2), # 4 Errata (Exhibit 3), # 5 Text of Proposed Order)(Gilligan, James) (Entered: 03/26/2018) |
| 03/28/2018 | 127 | NOTICE of Appearance by Olivia R. Hussey Scott on behalf of All Defendants (Scott, Olivia) (Entered: 03/28/2018) |
| 04/06/2018 | 128 | MOTION to Appear Pro Hac Vice for Molly A. Smolen (Filing fee $100, receipt number 0416-7257344.) by Wikimedia Foundation(Rocah, David) (Entered: 04/06/2018) |
| 04/06/2018 | 129 | MOTION to Appear Pro Hac Vice for Benjamin H. Kleine (Filing fee $100, receipt number 0416-7257347.) by Wikimedia Foundation(Rocah, David) (Entered: 04/06/2018) |
| 04/06/2018 | 130 | MOTION to Appear Pro Hac Vice for Devon Hanley Cook (Filing fee $100, receipt number 0416-7257349.) by Wikimedia Foundation(Rocah, David) (Entered: 04/06/2018) |
| 04/06/2018 | 132 | ORDER re: 124 parties' Joint Motion to Set Briefing Schedule for Motions to Compel. Signed by Judge T. S. Ellis on 4/6/2018. (bmhs, Deputy Clerk) (Entered: 04/09/2018) |
| 04/07/2018 | 131 | NOTICE by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers re 126 MOTION to Compel *Discovery (Notice of Withdrawal of Motion to Compel)* (Gilligan, James) (Entered: 04/07/2018) |
| 04/10/2018 | 133 | PAPERLESS ORDER granting 128 Motion to Appear Pro Hac Vice on behalf of Molly Smolen. Directing attorney Molly Smolen to register online for CM/ECF at |

| | | |
|---|---|---|
| | | http://www.mdd.uscourts.gov/electronic-case-filing-registration. Signed by Clerk on 4/10/2018. (srd, Deputy Clerk) (Entered: 04/10/2018) |
| 04/10/2018 | 134 | PAPERLESS ORDER granting 129 Motion to Appear Pro Hac Vice on behalf of Benjamin Kleine. Directing attorney Benjamin Kleine to register online for CM/ECF at http://www.mdd.uscourts.gov/electronic-case-filing-registration. Signed by Clerk on 4/10/2018. (srd, Deputy Clerk) (Entered: 04/10/2018) |
| 04/10/2018 | 135 | PAPERLESS ORDER granting 130 Motion to Appear Pro Hac Vice on behalf of Devon Cook. Directing attorney Devon Cook to register online for CM/ECF at http://www.mdd.uscourts.gov/electronic-case-filing-registration. Signed by Clerk on 4/10/2018. (srd, Deputy Clerk) (Entered: 04/10/2018) |
| 04/18/2018 | 136 | Supplemental to 125 Local Rule,,, filed by Wikimedia Foundation *Supplement to Plaintiff's Motion to Compel 125* (Toomey, Patrick) (Entered: 04/18/2018) |
| 04/27/2018 | 137 | NOTICE by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Patton, Rodney) (Entered: 04/27/2018) |
| 04/28/2018 | 138 | RESPONSE re 125 Local Rule,,, *in Opposition to Plaintiff's Motion to Compel Discovery Responses and Deposition Testimony* filed by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers. (Attachments: # 1 Exhibit A, # 2 Exhibit B, # 3 Exhibit C, # 4 Exhibit D, # 5 Text of Proposed Order)(Gilligan, James) (Entered: 04/28/2018) |
| 04/28/2018 | 139 | MOTION for Extension of Time to File *Out of Time* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 04/28/2018) |
| 04/30/2018 | 140 | ORDER granting 139 Defendants' Out-of-Time Motion for a Five and One-Half Hour Extension of Time. Signed by Judge T. S. Ellis on 4/30/2018. (bmhs, Deputy Clerk) Modified on 5/1/2018 (bmhs, Deputy Clerk). (Entered: 05/01/2018) |
| 05/11/2018 | 141 | NOTICE by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers *(Notice of Filing Unclassified (Redacted) Version of Classified Declaration Lodged With the Court In Camera and Ex Parte on April 27, 2018, in Support of the Government's Assertion of the State Secrets Privilege and Related Statutory Privileges)* (Attachments: # 1 Exhibit (Redacted Declaration of George C. Barnes, Deputy Director, National Security Agency))(Gilligan, James) (Entered: 05/11/2018) |
| 05/17/2018 | 142 | RESPONSE re 132 Order on Motion for Other Relief . *Joint Response to Court Order re: June 1, 2018 Hearing* filed by Wikimedia Foundation.(Toomey, Patrick) (Entered: 05/17/2018) |
| 05/18/2018 | 143 | RESPONSE re 138 Response, *Reply Brief in Support of Plaintiff's Motion to Compel* filed by Wikimedia Foundation. (Attachments: # 1 Declaration of Ashley Gorski, # 2 Exhibit 1, # 3 Exhibit 2)(Gorski, Ashley) (Entered: 05/18/2018) |
| 05/29/2018 | 144 | ORDER rescheduling the upcoming hearing on Plaintiff's Motion to Compel. Signed by Judge T. S. Ellis on 5/29/2018. (bmhs, Deputy Clerk) (Entered: 05/29/2018) |
| 06/08/2018 | 145 | Consent MOTION to Withdraw as Attorney *(Timothy A. Johnson)* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security |

| | | |
|---|---|---|
| | | Service, Office of the Director of National Intelligence, Michael S. Rogers(Johnson, Timothy) (Entered: 06/08/2018) |
| 06/22/2018 | 146 | ORDER granting 145 Motion to Withdraw as Attorney. Attorney Timothy A Johnson terminated. Signed by Judge T. S. Ellis on 6/21/2018. (bmhs, Deputy Clerk) (Entered: 06/22/2018) |
| 06/28/2018 | 147 | Correspondence Correcting Earlier Submission: 138 Response, (Attachments: # 1 Attachment Corrected Version of Defendants' Memorandum of Points and Authorities in Opposition to Plaintiff's Motion to Compel Discovery Responses and Deposition Testimony)(Scott, Olivia) (Entered: 06/28/2018) |
| 07/06/2018 | 148 | Supplemental to 125 Local Rule,,, filed by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers *(Defendants' Supplemental Memorandum in Opposition to Plaintiffs' Motion to Compel)* (Gilligan, James) (Entered: 07/06/2018) |
| 07/06/2018 | 149 | Supplemental to 125 Local Rule,,, filed by Wikimedia Foundation *(Plaintiff's Supplemental Brief in Response to the Court's June 29, 2018 Order)* (Gorski, Ashley) (Entered: 07/06/2018) |
| 08/20/2018 | 150 | MEMORANDUM OPINION. Signed by Judge T. S. Ellis on 8/20/2018. (bmhs, Deputy Clerk) (Entered: 08/20/2018) |
| 08/20/2018 | 151 | ORDER denying 126 Plaintiff's Motion to Compel Discovery Responses and Deposition Testimony. Signed by Judge T. S. Ellis on 8/20/2018. (bmhs, Deputy Clerk) (Entered: 08/20/2018) |
| 08/31/2018 | 152 | ORDER scheduling a status conference. Signed by Judge T. S. Ellis on 8/31/2018. (bmhs, Deputy Clerk) (Entered: 09/04/2018) |
| 09/04/2018 | 153 | ORDER scheduling a status conference. Signed by Judge T. S. Ellis on 9/4/2018. (bmhs, Deputy Clerk) (Entered: 09/04/2018) |
| 09/18/2018 | 154 | MOTION for Other Relief *(Motion to Set a Summary Judgment Briefing Schedule)* by Wikimedia Foundation (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 09/18/2018) |
| 09/20/2018 | 155 | MOTION to Set a Summary Judgment Briefing Schedule and Response to Plaintiff's Motion to Set a Summary Judgment Briefing Schedule re 154 MOTION for Other Relief *(Motion to Set a Summary Judgment Briefing Schedule)* by James R. Clapper, Department of Justice, Eric H. Holder, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Scott, Olivia) (Entered: 09/20/2018) |
| 09/21/2018 | 156 | ORDER granting in part and denying in part 154 Plaintiff's Motion to Set a Summary Judgment Briefing Schedule; and granting in part and denying in part 155 Defendants' Motion to Set a Summary Judgment Briefing Schedule. Signed by Judge T. S. Ellis on 9/21/2018. (bmhs, Deputy Clerk) (Entered: 09/24/2018) |
| 09/21/2018 | 157 | Status Conference held on 9/21/2018 before Judge T. S. Ellis.(Court Reporter: Tonia Harris) (bmhs, Deputy Clerk) (Entered: 09/26/2018) |
| 09/26/2018 | 158 | ORDER setting briefing and oral argument schedule. Signed by Judge T. S. Ellis on 9/25/2018. (bmhs, Deputy Clerk) (Entered: 09/26/2018) |
| 11/06/2018 | 159 | MOTION for Extension of Time to File *MSJ - Unopposed Motion for Extension of One* |

| | | |
|---|---|---|
| | | *Business Day to Submit Defendants Summary Judgment Motion* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Berman, Julia) (Entered: 11/06/2018) |
| 11/13/2018 | 160 | MOTION for Extension of Time to File *Motion for Summary Judgment; Defendants Out-of-Time Motion for Extension of One Business Day to Submit Defendants Summary Judgment Motion* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Berman, Julia) (Entered: 11/13/2018) |
| 11/13/2018 | 161 | MOTION for Summary Judgment by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order, # 2 Memorandum in Support (Filed Under Seal), # 3 Exhibit List (Filed Under Seal), # 4 Exhibit 1 (Filed Under Seal), # 5 Exhibit 2 (Filed Under Seal), # 6 Exhibit 3 (Filed Under Seal), # 7 Exhibit 4 (Filed Under Seal), # 8 Exhibit 5 (Filed Under Seal))(Gilligan, James) (Entered: 11/13/2018) |
| 11/13/2018 | 162 | -SEALED - NOTICE of Filing Under Seal Sealed Brief in Support of Defendants' Motion for Summary Judgment and Sealed Exhibits by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers re 161 MOTION for Summary Judgment (Attachments: # 1 Sealed Exhibit List, # 2 Sealed Exhibit 1, # 3 Sealed Exhibit 2, # 4 Sealed Exhibit 3, # 5 Sealed Exhibit 4, # 6 Sealed Exhibit 5)(Gilligan, James) (Entered: 11/13/2018) |
| 11/13/2018 | 163 | MOTION to Seal *Defendants' Summary Judgment Motion Pursuant to Civil Local Rule 105-11 and Protective Order Paragraph 12.3* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Gilligan, James) (Entered: 11/13/2018) |
| 12/07/2018 | 164 | MOTION for Leave to File *Updated Public Versions of the Under Seal Portions of Defendants' Motion for Summary Judgment* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order, # 2 Attachment A, # 3 Attachment B, # 4 Attachment C, # 5 Attachment D, # 6 Attachment E, # 7 Attachment F, # 8 Attachment G)(Scott, Olivia) (Entered: 12/07/2018) |
| 12/11/2018 | 165 | ORDER granting 163 Defendants' Motion to Seal; and granting 164 Defendants' Motion for Leave to File an Updated Public Version of Defendants' Sealed Motion for Summary Judgment. Signed by Judge T. NA S. Ellis on 12/11/2018. (bmhs, Deputy Clerk) (Entered: 12/11/2018) |
| 12/11/2018 | 166 | Supplemental Exhibits A-G to 161 Motion for Summary Judgment. (Attachments: # 1 Exhibit B, # 2 Exhibit C, # 3 Exhibit D, # 4 Exhibit E, # 5 Exhibit F, # 6 Exhibit G) (bmhs, Deputy Clerk) (Entered: 12/11/2018) |
| 12/18/2018 | 167 | MOTION for Extension of Time to File *Opposition to Motion for Summary Judgment; Plaintiff's Out-of-Time Motion for Extension to Submit Opposition to Defendants' Summary Judgment Motion* by Wikimedia Foundation (Attachments: # 1 Text of Proposed Order)(Toomey, Patrick) (Entered: 12/18/2018) |
| 12/18/2018 | 168 | RESPONSE in Opposition re 161 MOTION for Summary Judgment filed by Wikimedia Foundation. (Attachments: # 1 Exhibit List, # 2 Exhibit 1 - Declaration of Scott Bradner, |

| | | |
|---|---|---|
| | | # 3 Exhibit 1 - Appendix to Bradner Declaration [1/3], # 4 Exhibit 1 - Appendix to Bradner Declaration [2/3], # 5 Exhibit 1 - Appendix to Bradner Declaration [3/3], # 6 Exhibit 2 - Declaration of Jonathon Penney, # 7 Exhibit 3 - Declaration of Michelle Paulson, # 8 Exhibit 4 - Declaration of James Alexander, # 9 Exhibit 5 - Declaration of Tilman Bayer, # 10 Exhibit 6 - Declaration of Emily Temple-Wood, # 11 Exhibit 7 - Declaration of Patrick Toomey, # 12 Exhibit 8, # 13 Exhibit 9, # 14 Exhibit 10, # 15 Exhibit 11, # 16 Exhibit 12, # 17 Exhibit 13, # 18 Exhibit 14, # 19 Exhibit 15, # 20 Exhibit 16, # 21 Exhibit 17, # 22 Exhibit 18, # 23 Exhibit 19, # 24 Exhibit 20, # 25 Exhibit 21, # 26 Exhibit 22, # 27 Exhibit 23, # 28 Exhibit 24, # 29 Exhibit 25, # 30 Exhibit 26, # 31 Exhibit 27, # 32 Exhibit 28, # 33 Exhibit 29, # 34 Exhibit 30, # 35 Exhibit 31, # 36 Exhibit 32, # 37 Exhibit 33, # 38 Exhibit 34, # 39 Exhibit 35, # 40 Exhibit 36, # 41 Exhibit 37, # 42 Exhibit 38, # 43 Exhibit 39, # 44 Exhibit 40, # 45 Exhibit 41, # 46 Exhibit 42, # 47 Exhibit 43, # 48 Exhibit 44, # 49 Exhibit 45, # 50 Text of Proposed Order)(Toomey, Patrick) (Entered: 12/18/2018) |
| 12/19/2018 | 169 | ORDER granting 167 Plaintiff's Out-of-Time Motion for an Extension of Time to File Its Opposition to Defendants' Motion for Summary Judgment. Signed by Judge T. NA S. Ellis on 12/19/2018. (bmhs, Deputy Clerk) (Entered: 12/19/2018) |
| 12/19/2018 | 170 | ORDER granting 159 Defendants' Out-of-Time Motion for Extension of One Business Day to Submit Defendants' Summary Judgment Motion. Signed by Judge T. NA S. Ellis on 12/19/2018. (bmhs, Deputy Clerk) (Entered: 12/19/2018) |
| 12/26/2018 | 171 | MOTION to Stay *of Proceedings in Light of Lapse of Appropriations* by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers (Attachments: # 1 Text of Proposed Order)(Scott, Olivia) (Entered: 12/26/2018) |
| 12/27/2018 | 172 | RESPONSE re 171 MOTION to Stay *of Proceedings in Light of Lapse of Appropriations* filed by Wikimedia Foundation.(Gorski, Ashley) (Entered: 12/27/2018) |
| 01/02/2019 | 173 | ORDER granting 171 Motion to Stay; and vacating the 9/25/18 order establishing a briefing and oral argument schedule. Signed by Judge T. NA S. Ellis on 1/2/2019. (bmhs, Deputy Clerk) (Entered: 01/02/2019) |
| 01/28/2019 | 174 | NOTICE by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers *to the Court of Restoration of Appropriations* (Scott, Olivia) (Entered: 01/28/2019) |
| 01/31/2019 | 175 | Joint MOTION for Other Relief *(Joint Motion to Set Revised Schedule)* by Wikimedia Foundation (Attachments: # 1 Text of Proposed Order)(Gorski, Ashley) (Entered: 01/31/2019) |
| 01/31/2019 | 176 | ORDER LIFTING STAY. Signed by Judge T. NA S. Ellis on 1/31/2019. (kw2s, Deputy Clerk) (Entered: 01/31/2019) |
| 02/04/2019 | 177 | ORDER granting 175 Joint Motion to Set a Revised Schedule. Signed by Judge T. NA S. Ellis on 2/1/2019. (bmhs, Deputy Clerk) (Entered: 02/04/2019) |
| 02/15/2019 | 178 | REPLY to Response to Motion re 161 MOTION for Summary Judgment *(Reply Brief in Support of Defendants' Motion for Summary Judgment)* filed by James R. Clapper, Department of Justice, Eric H. Holder, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers. (Attachments: # 1 Exhibit List, # 2 Affidavit (Exh. 6 (Second) Schulzrinne Declaration), # 3 Affidavit (Exh. 7 Salzberg Declaration), # 4 Affidavit (Exh. 8 (Second) Gilligan Declaration), # 5 Exhibit 9, # 6 Exhibit 10, # 7 Exhibit 11, # 8 Exhibit 12, # 9 Exhibit 13, # 10 Exhibit 14, # 11 Exhibit 15)(Gilligan, James) (Entered: 02/15/2019) |

| | | |
|---|---|---|
| 03/01/2019 | 179 | MOTION for Leave to File Excess Pages *[Unopposed]* by Wikimedia Foundation (Attachments: # 1 Text of Proposed Order)(Gorski, Ashley) (Entered: 03/01/2019) |
| 03/04/2019 | 180 | ORDER granting 179 Unopposed Motion for Leave to File Excess Pages. Signed by Judge T. NA S. Ellis on 3/4/2019. (bmhs, Deputy Clerk) (Entered: 03/04/2019) |
| 03/08/2019 | 181 | RESPONSE in Opposition re 161 MOTION for Summary Judgment *(Sur-reply Brief in Opposition to Defendants' Motion for Summary Judgment)* filed by Wikimedia Foundation. (Attachments: # 1 Exhibit 1. Second Bradner Declaration, # 2 Exhibit 2. Second Penney Declaration, # 3 Exhibit 3. Second Paulson Declaration, # 4 Exhibit 4. Second Bayer Declaration, # 5 Exhibit 5. Second Temple-Wood Declaration)(Toomey, Patrick) (Entered: 03/08/2019) |
| 03/22/2019 | 182 | REPLY to Response to Motion re 161 MOTION for Summary Judgment *(Sur-Reply in Support of Defendants' Motion for Summary Judgment)* filed by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers. (Attachments: # 1 Exhibit List, # 2 Affidavit (Exh. 16 (Third) Schulzrinne Declaration), # 3 Affidavit (Exh. 17 Second Salzberg Declaration))(Gilligan, James) (Entered: 03/22/2019) |
| 04/03/2019 | 183 | ORDER Rescheduling Oral Argument for May, 30 2019 at 2:00 p.m.. Signed by Judge T. NA S. Ellis on 4/3/2019. (bas, Deputy Clerk) (Entered: 04/04/2019) |
| 04/29/2019 | 184 | NOTICE by James R. Clapper, Department of Justice, Loretta E. Lynch, National Security Agency/Central Security Service, Office of the Director of National Intelligence, Michael S. Rogers *of Recent Decision* (Attachments: # 1 Attachment)(Scott, Olivia) (Entered: 04/29/2019) |
| 05/03/2019 | 185 | RESPONSE re 184 Notice (Other), filed by Wikimedia Foundation.(Toomey, Patrick) (Entered: 05/03/2019) |
| 05/30/2019 | 186 | Civil Motion Hearing held on 5/30/2019 before Judge T. NA S. Ellis. (bmhs, Deputy Clerk) (Entered: 05/31/2019) |
| 08/09/2019 | 187 | (FILED IN ERROR) NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on 5/30/2019, before Judge T.S. Ellis, III. Court Reporter/Transcriber Tonia M. Harris, Telephone number 703-646-1438. Total number of pages filed: 69. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Redaction Request due 8/30/2019. Redacted Transcript Deadline set for 9/9/2019. Release of Transcript Restriction set for 11/7/2019.(bmhs, Deputy Clerk) Modified on 5/12/2020 (bmhs, Deputy Clerk). (Entered: 08/09/2019) |
| 12/16/2019 | 188 | MEMORANDUM OPINION. Signed by Judge T. NA S. Ellis on 12/13/2019. (kw2s, Deputy Clerk) (Entered: 12/16/2019) |
| 12/16/2019 | 189 | ORDER Granting 161 MOTION for Summary Judgment filed by National Security Agency/Central Security Service, Loretta E. Lynch, Michael S. Rogers, Office of the Director of National Intelligence, James R. Clapper, Department of Justice. Signed by Judge T.S. Ellis on 12/13/2019. (kw2s, Deputy Clerk) Modified on 12/17/2019 (kw2s, Deputy Clerk). (Entered: 12/16/2019) |
| 12/17/2019 | 190 | JUDGMENT in favor of Defendants against Plaintiff. Signed by Felicia C. Cannon, Clerk of Court on 12/16/2019. (bmhs, Deputy Clerk) (Entered: 12/17/2019) |
| 02/14/2020 | 191 | NOTICE OF APPEAL as to 190 Clerk's Judgment by Wikimedia Foundation. Filing fee $ 505, receipt number 0416-8516425.(Toomey, Patrick) (Entered: 02/14/2020) |

| | | |
|---|---|---|
| 02/19/2020 | 192 | Transmission of Notice of Appeal and Docket Sheet to US Court of Appeals re 191 Notice of Appeal. IMPORTANT NOTICE: To access forms which you are required to file with the United States Court of Appeals for the Fourth Circuit please go to http://www.ca4.uscourts.gov and click on Forms & Notices.(jb5, Deputy Clerk) (Entered: 02/19/2020) |
| 02/21/2020 | 193 | USCA Case Number 20-1191 for 191 Notice of Appeal filed by Wikimedia Foundation. Case Manager - Kirsten Hancock (jb5s, Deputy Clerk) (Entered: 02/21/2020) |
| 03/27/2020 | 194 | (FILED IN ERROR) NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on 6/29/2018, before Judge T.S. Ellis, III. Court Reporter/Transcriber Tonia M. Harris, Telephone number 703-646-1438. Total number of pages filed: 30. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Redaction Request due 4/17/2020. Redacted Transcript Deadline set for 4/27/2020. Release of Transcript Restriction set for 6/25/2020.(bmhs, Deputy Clerk) Modified on 5/12/2020 (bmhs, Deputy Clerk). (Entered: 03/30/2020) |
| 04/01/2020 | 195 | (ELECTRONICALLY FILED IN ERROR)TRANSCRIPT ORDER ACKNOWLEDGMENT by Wikimedia Foundation for proceedings held on Hearing: 06/29/2018 before Judge T. NA S. Ellis, re 191 Notice of Appeal - Transcript due by 6/8/2020. (Court Reporter: Tonia Harris)(slss, Deputy Clerk) Modified on 5/11/2020 (slss, Deputy Clerk). (Entered: 04/01/2020) |
| 05/11/2020 | | Set/Reset Transcript Deadlines re 195 Appeal Transcript Request. (slss, Deputy Clerk) (Entered: 05/11/2020) |
| 05/12/2020 | 196 | NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on 6/29/2018, before Judge T.S. Ellis, III. Court Reporter/Transcriber Tonia M. Harris, Telephone number 703-646-1438. Total number of pages filed: 29. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Redaction Request due 6/2/2020. Redacted Transcript Deadline set for 6/12/2020. Release of Transcript Restriction set for 8/10/2020.(bmhs, Deputy Clerk) (Entered: 05/12/2020) |
| 05/12/2020 | 197 | NOTICE OF FILING OF OFFICIAL TRANSCRIPT of Proceedings held on 5/30/2019, before Judge T.S. Ellis, III. Court Reporter/Transcriber Tonia M. Harris, Telephone number 703-646-1438. Total number of pages filed: 69. Transcript may be viewed at the court public terminal or purchased through the Court Reporter/Transcriber before the deadline for Release of Transcript Restriction. After that date it may be obtained from the Court Reporter or through PACER. Redaction Request due 6/2/2020. Redacted Transcript Deadline set for 6/12/2020. Release of Transcript Restriction set for 8/10/2020.(bmhs, Deputy Clerk) (Entered: 05/12/2020) |

| PACER Service Center | | | |
|---|---|---|---|
| Transaction Receipt | | | |
| 06/24/2020 09:54:38 | | | |
| **PACER Login:** | hshamsi12:4377808:4375869 | **Client Code:** | |
| **Description:** | Docket Report | **Search Criteria:** | 1:15-cv-00662-TSE |

| | | | |
|---|---|---|---|
| **Billable Pages:** | 30 | **Cost:** | 3.00 |

**UNITED STATES DISTRICT COURT**
**DISTRICT OF MARYLAND**

WIKIMEDIA FOUNDATION
149 New Montgomery Street, 6th Floor
San Francisco, CA 94105;

NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
1660 L Street, NW, 12th Floor
Washington, DC 20036;

HUMAN RIGHTS WATCH
350 Fifth Avenue, 34th Floor
New York, NY 10118;

AMNESTY INTERNATIONAL USA
5 Pennsylvania Plaza, 16th Floor
New York, NY 10001;

PEN AMERICAN CENTER
588 Broadway, Suite 303
New York, NY 10012;

GLOBAL FUND FOR WOMEN
222 Sutter Street, Suite 500
San Francisco, CA 94108;

THE NATION MAGAZINE
33 Irving Place, 8th Floor
New York, NY 10003;

THE RUTHERFORD INSTITUTE
P.O. Box 7482
Charlottesville, VA 22906;

WASHINGTON OFFICE ON LATIN AMERICA
1666 Connecticut Avenue, NW, Suite 400
Washington, DC 20009,

*Plaintiffs*,

v.

NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE

**FIRST AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF**

Civil Action No.
15-cv-00662-TSE

Hon. T. S. Ellis, III

9800 Savage Road
Fort Meade, Anne Arundel County, MD 20755;

ADM. MICHAEL S. ROGERS, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service,
National Security Agency / Central Security Service
9800 Savage Road
Fort Meade, Anne Arundel County, MD 20755;

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Washington, DC 20511;

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence,
Office of the Director of National Intelligence
Washington, DC 20511;

DEPARTMENT OF JUSTICE
950 Pennsylvania Avenue, NW
Washington, DC 20530;

LORETTA E. LYNCH, in her official capacity as Attorney General of the United States,
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530,

*Defendants*.

Deborah A. Jeon
(Bar No. 06905)
jeon@aclu-md.org
David R. Rocah
(Bar No. 27315)
rocah@aclu-md.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838

Patrick Toomey
(pro hac vice)
ptoomey@aclu.org
Jameel Jaffer
(pro hac vice)
jjaffer@aclu.org
Alex Abdo
(pro hac vice)
aabdo@aclu.org
Ashley Gorski
(pro hac vice)
agorski@aclu.org
AMERICAN CIVIL LIBERTIES UNION FOUNDATION

125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654

Charles S. Sims
(pro hac vice)
csims@proskauer.com
David A. Munkittrick
(pro hac vice)
dmunkittrick@proskauer.com
John M. Browning
(pro hac vice)
jbrowning@proskauer.com
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900

June 19, 2015

**FIRST AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF**

1. This lawsuit challenges the suspicionless seizure and searching of internet traffic by the National Security Agency ("NSA") on U.S. soil. The NSA conducts this surveillance, called "Upstream" surveillance, by tapping directly into the internet backbone inside the United States—the network of high-capacity cables, switches, and routers that today carry vast numbers of Americans' communications with each other and with the rest of the world. In the course of this surveillance, the NSA is seizing Americans' communications en masse while they are in transit, and it is searching the contents of substantially all international text-based communications—and many domestic communications as well—for tens of thousands of search terms. The surveillance exceeds the scope of the authority that Congress provided in the FISA Amendments Act of 2008 ("FAA") and violates the First and Fourth Amendments. Because it is predicated on programmatic surveillance orders issued by the Foreign Intelligence Surveillance Court ("FISC") in the absence of any case or controversy, the surveillance also violates Article III of the Constitution.

2. Plaintiffs are educational, legal, human rights, and media organizations that collectively engage in more than a trillion sensitive international communications over the internet each year. Plaintiffs communicate with, among many others, journalists, clients, experts, attorneys, civil society organizations, foreign government officials, and victims of human rights abuses. Plaintiff Wikimedia Foundation communicates with the hundreds of millions of individuals who visit Wikipedia webpages to read or contribute to the vast repository of human knowledge that Wikimedia maintains online. The ability to exchange information in confidence, free from warrantless government monitoring, is essential to each of

the Plaintiffs' work. The challenged surveillance violates Plaintiffs' privacy and undermines their ability to carry out activities crucial to their missions.

3. Plaintiffs respectfully request that the Court declare the government's Upstream surveillance to be unlawful; enjoin the government from continuing to conduct Upstream surveillance of Plaintiffs' communications; and require the government to purge from its databases all of Plaintiffs' communications that Upstream surveillance has already allowed the government to obtain.

## JURISDICTION AND VENUE

4. This case arises under the Constitution and the laws of the United States and presents a federal question within this Court's jurisdiction under Article III of the Constitution and 28 U.S.C. § 1331. The Court also has jurisdiction under the Administrative Procedure Act, 5 U.S.C. § 702. The Court has authority to grant declaratory relief pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201–2202. The Court has authority to award costs and attorneys' fees under 28 U.S.C. § 2412.

5. Venue is proper in this district under 28 U.S.C. § 1391(b)(2), (e)(1).

## PLAINTIFFS

6. Wikimedia Foundation ("Wikimedia") is a non-profit organization based in San Francisco, California, that operates twelve free-knowledge projects on the internet. Wikimedia's mission is to empower people around the world to collect and develop free educational content. Wikimedia does this by developing and maintaining "wiki"-based projects, and by providing the full contents of those projects to individuals around the world free of charge. Wikimedia sues on its own behalf and on behalf of its staff and users.

7. The National Association of Criminal Defense Lawyers ("NACDL") is a membership organization based in Washington, D.C. NACDL advocates for rational and humane criminal justice policies at all levels of federal, state, and local government, and seeks to foster the integrity, independence, and expertise of the criminal defense profession. NACDL sues on its own behalf and on behalf of its members.

8. Human Rights Watch ("HRW") is a non-profit, non-governmental human rights organization headquartered in New York City with offices around the world. It reports on abuses in all regions of the globe and advocates for the protection of human rights. HRW researchers conduct fact-finding investigations into human rights abuses in over 90 countries and publish their findings in hundreds of reports, multi-media products, and other documents every year, as well as through social media accounts. HRW sues on its own behalf and on behalf of its staff.

9. Amnesty International USA ("AIUSA"), headquartered in New York City, is the largest country section of Amnesty International, with hundreds of thousands of members and other supporters who work for human rights, including through national online networks, high schools, colleges, and community groups. AIUSA sues on its own behalf and on behalf of its staff and members.

10. PEN American Center ("PEN") is a human rights and literary association based in New York City. Committed to the advancement of literature and the unimpeded flow of ideas and information, PEN fights for freedom of expression; advocates on behalf of writers harassed, imprisoned, and sometimes killed for their views; and fosters international exchanges, dialogues, discussions, and debates. PEN sues on its own behalf and on behalf of its staff and members.

11. Global Fund for Women ("GFW") is a non-profit grantmaking foundation based in San Francisco, California, and New York City. GFW advances women's human rights worldwide by providing funds to women-led organizations that promote the economic security, health, safety, education, and leadership of women and girls. GFW sues on its own behalf and on behalf of its staff.

12. The Nation Magazine ("The Nation"), which is published by The Nation Company, LLC, and based in New York City, is America's oldest weekly magazine of opinion, news, and culture. It serves as a critical, independent voice in American journalism, exposing abuses of power through its investigative reporting, analysis, and commentary. In recent years, The Nation's journalists have reported on a wide range of issues relating to international affairs, including the wars in Iraq and Afghanistan, the Israel–Palestine conflict, protest activities in China and elsewhere in East Asia, and conflicts in Africa and Latin America. The Nation sues on behalf of itself, its staff, and certain of its contributing journalists.

13. The Rutherford Institute ("Rutherford") is a civil liberties organization based in Charlottesville, Virginia, committed to protecting the constitutional freedoms of Americans and the human rights of all people. Rutherford provides free legal services in defense of civil liberties and educates the public about constitutional and human rights issues. It also advocates on behalf of individuals abroad whose rights are threatened by foreign governments. Rutherford sues on its own behalf and on behalf of its staff.

14. The Washington Office on Latin America ("WOLA") is a non-profit, non-governmental organization based in Washington, D.C., that conducts research, advocacy, and education designed to advance human rights and social justice in the Americas. WOLA sues on its own behalf and on behalf of its staff.

**DEFENDANTS**

15. Defendant National Security Agency / Central Security Service ("NSA"), headquartered in Fort Meade, Maryland, is the agency of the United States government responsible for conducting the surveillance challenged in this case.

16. Defendant Adm. Michael S. Rogers is the Director of the NSA and the Chief of the Central Security Service. Defendant Rogers is sued in his official capacity.

17. Defendant Office of the Director of National Intelligence ("ODNI") is the agency of the United States government responsible for directing and coordinating the activities of the intelligence community, including the NSA.

18. Defendant James R. Clapper is the Director of National Intelligence ("DNI"). Together with the Attorney General, the DNI authorizes warrantless surveillance of U.S. citizens' and residents' international communications under the FAA, including Upstream surveillance. Defendant Clapper is sued in his official capacity.

19. Defendant Department of Justice ("DOJ") is one of the agencies of the United States government responsible for authorizing and overseeing surveillance conducted pursuant to the FAA, including Upstream surveillance.

20. Defendant Loretta E. Lynch is the Attorney General of the United States. Together with the DNI, the Attorney General authorizes warrantless surveillance of U.S. citizens' and residents' international communications under the FAA, including Upstream surveillance. Defendant Lynch is sued in her official capacity.

## LEGAL AND FACTUAL BACKGROUND

The Foreign Intelligence Surveillance Act

21. In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") to govern surveillance conducted for foreign intelligence purposes. The statute created the Foreign Intelligence Surveillance Court ("FISC") and empowered the court to grant or deny government applications for surveillance orders in certain foreign intelligence investigations.

22. Congress enacted FISA after years of in-depth congressional investigation by the committees chaired by Senator Frank Church and Representative Otis Pike, which revealed that the Executive Branch had engaged in widespread warrantless surveillance of United States citizens—including journalists, activists, and members of Congress—"who engaged in no criminal activity and who posed no genuine threat to the national security."

23. Congress has amended FISA multiple times since 1978.

24. Prior to 2007, FISA generally required the government to obtain an individualized order from the FISC before conducting electronic surveillance on U.S. soil. To obtain a traditional FISA order, the government was required to make a detailed factual showing with respect to both the target of the surveillance and the specific communications facility—often a telephone line or email account—to be monitored. The government was also required to certify that a "significant purpose" of the surveillance was to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(6)(B).

25. The FISC could issue such an order only if it found, among other things, that there was probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power," and that "each of the facilities or places at which the

electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2)(A)–(B).

26. The framework established by FISA remains in effect today, but it has been modified by the FAA to permit the acquisition of U.S. citizens' and residents' international communications without probable cause or individualized suspicion, as described below.

The Warrantless Wiretapping Program

27. On October 4, 2001, President George W. Bush secretly authorized the NSA to conduct a program of warrantless electronic surveillance inside the United States. This program, which was known as the President's Surveillance Program ("PSP"), was reauthorized repeatedly by President Bush between 2001 and 2007.

28. According to public statements by senior government officials, the PSP involved the warrantless interception of emails and telephone calls that originated or terminated inside the U.S. According to then-Attorney General Alberto Gonzales and then-NSA Director General Michael Hayden, NSA "shift supervisors" initiated surveillance when in their judgment there was a "reasonable basis to conclude that one party to the communication [was] a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda."

29. On January 17, 2007, then-Attorney General Alberto Gonzales publicly announced that a judge of the FISC had "issued orders authorizing the Government to target for collection international communications into or out of the United States where there [was] probable cause to believe that one of the communicants [was] a member or agent of al Qaeda or an associated terrorist organization." The Attorney General further stated that "[a]s a result of

these orders, any electronic surveillance that was occurring" as part of the PSP would thereafter "be conducted subject to the approval of the Foreign Intelligence Surveillance Court."

30. In April 2007, when the government sought reauthorization of the FISC's previous orders, a different judge of the FISC determined that key elements of the government's request were incompatible with FISA. Following the FISC's refusal to renew certain portions of its January 2007 orders, executive-branch officials appealed to Congress to amend the statute.

The Protect America Act

31. Congress enacted the Protect America Act ("PAA") in August 2007. The PAA expanded the executive's surveillance authority and provided legislative sanction for surveillance that the President had previously been conducting under the PSP. Because of a "sunset" provision, the amendments to FISA made by the PAA expired on February 17, 2008.

The FISA Amendments Act

32. President Bush signed the FISA Amendments Act ("FAA") into law on July 10, 2008. The FAA radically revised the FISA regime that had been in place since 1978 by authorizing the acquisition without individualized suspicion of a wide swath of communications, including U.S. persons' international communications, from companies inside the United States.[1]

33. In particular, the FAA allows the Attorney General and Director of National Intelligence to "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence

[1] Plaintiffs use the term "international" to describe communications that either originate or terminate outside the United States, but not both—*i.e.*, communications that are foreign at one end.

information." 50 U.S.C. § 1881a(a). The statute requires the Attorney General, in consultation with the Director of National Intelligence, to adopt "targeting procedures" and "minimization procedures," *id.* § 1881a(d)–(e), that govern who may be targeted for surveillance by executive-branch employees and how communications are to be handled once intercepted.

34. The FISC's role in overseeing the government's surveillance under the statute consists principally of reviewing these general procedures. The FISC never reviews or approves the government's individual surveillance targets or the facilities it intends to monitor. Rather, when the government wishes to conduct surveillance under the statute, it must certify to the FISC that the court has approved its targeting and minimization procedures or that it will shortly submit such procedures for the FISC's approval. *See id.* § 1881a(g), (i). If the government so certifies, the FISC authorizes the government's surveillance for up to a year at a time. A single such order may result in the acquisition of the communications of thousands of individuals.

35. The effect of the FAA is to give the government sweeping authority to conduct warrantless surveillance of U.S. persons' international communications. While the statute prohibits the government from intentionally *targeting* U.S. persons, it authorizes the government to acquire U.S. persons' communications with the foreigners whom the NSA chooses to target. Moreover the statute does not meaningfully restrict *which* foreigners the government may target. The statute does not require the government to make any finding—let alone demonstrate probable cause to the FISC—that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. The government may target any person for surveillance if it has a reasonable belief that she is a foreigner outside the United States who is likely to communicate "foreign intelligence information"—a term that is

defined so broadly as to encompass virtually any information relating to the foreign affairs of the United States. *Id.* §§ 1881a(a), 1801(e). The government may target corporations and associations under the same standard.

36. Thus, though the FAA is nominally concerned with the surveillance of individuals and groups outside the United States, it has far-reaching implications for U.S. persons' privacy. The targets of FAA surveillance may include journalists, academic researchers, human rights defenders, aid workers, business persons, and others who are not suspected of any wrongdoing. In the course of FAA surveillance, the government may acquire the communications of U.S. citizens and residents with all these persons.

**THE GOVERNMENT'S IMPLEMENTATION OF THE FAA**

37. The government has implemented the FAA expansively, with significant consequences for Americans' privacy. The Director of National Intelligence has reported that, in 2014, the government relied on the FAA to target 92,707 individuals, groups, or organizations for surveillance under a single court order. According to the FISC, the government gathered 250 million internet communications under the FAA in 2011 alone—at a time when the NSA had far fewer targets than it has today. Moreover, as described below, that figure does not reflect the far greater number of communications that the NSA searched for references to its targets before discarding them. Intelligence officials have declined to determine, or even estimate, how many of the communications intercepted under the FAA are to, from, or about U.S. citizens or residents. However, opinions issued by the FISC, reports by the President's Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board, and media accounts indicate that FAA

surveillance results in the wide-ranging and persistent interception of U.S. persons' communications.

38. In at least one respect, the government has engaged in surveillance that exceeds even the broad authority that Congress granted in the FAA. As described below, the government has interpreted the FAA to allow it to intercept, copy, and review essentially everyone's internet communications in order to search for identifiers associated with its targets. This intrusive and far-reaching practice has no basis in the statute. The statute authorizes surveillance only of *targets'* communications; it does not authorize surveillance of everyone.

Upstream Surveillance of Internet Communications

39. The government conducts at least two kinds of surveillance under the FAA. Under a program called "PRISM," the government obtains stored and real-time communications directly from U.S. companies—such as Google, Yahoo, Facebook, and Microsoft—that provide communications services to targeted accounts.

40. This case concerns a second form of surveillance, called Upstream. Upstream surveillance involves the NSA's seizing and searching the internet communications of U.S. citizens and residents en masse as those communications travel across the internet "backbone" in the United States. The internet backbone is the network of high-capacity cables, switches, and routers that facilitates both domestic and international communication via the internet.

*Background: Internet Communications*

41. The internet is a global network of networks. It allows machines of different types to communicate with each other through a set of intermediating networks. At its most basic level, it consists of (1) computers and the connections between them, (2) the

communications transmitted to, by, or through those computers and connections, and (3) the rules that direct the flow of these communications.

42. All communications on the internet are broken into "packets"—discrete chunks of information that are relatively small. The packets are sent from machine to machine (and network to network) and may traverse a variety of physical circuits connecting different machines before reaching their destination. Once the packets that make up a particular communication reach their final destination, they are reassembled so that the recipient can "read" the message being sent—whether an email, a webpage, or a video.

43. Internet packets can be thought of in layers. Although computer scientists describe these layers differently depending on the context, there are three layers relevant here:

- **The Networking Layer:** The Networking Layer of a packet is like an address block on an envelope. It contains, among other things, the packet's source and destination addresses. On the internet, addresses are represented as numeric strings known as Internet Protocol ("IP") addresses. To send a packet from one IP address to another, a computer on the internet creates a packet, addresses the packet with the source and destination IP addresses, and then transmits the packet to a neighboring computer that is closer to the destination. That computer then transmits the packet to another that is closer still to the destination. This process continues until the packet reaches its destination.

- **The Transport Layer:** The Transport Layer of a packet contains information that allows it to be grouped with other packets that are part of the same session or class of communication. For example, a packet sent using the most common Transport Layer protocol (the Transmission Control Protocol ("TCP")) contains, among other things, (1) a sequence number, which allows the recipient to reassemble the packets of a communication in order, and (2) source and destination "ports," which are, in effect, internal addresses used by the sending and receiving computers.

- **The Application Layer:** The Application Layer of a packet is akin to the inside of an envelope—it contains the actual content of the communications being transmitted. If the content is too large to fit into a single packet, then the Application Layers of several different packets would need to be reassembled in order for the recipient to be able to read or interpret the communication. For example, HTTP is the Application Layer protocol used to transmit webpages. Because most websites exceed the size of a single internet packet, their contents are transmitted in a series of HTTP packets that must be reassembled before display. Other common Application Layer protocols that, like

HTTP, contain text-searchable data are SMTP (for the sending of email), IMAP and POP (for the receiving of email), and DNS (which allows computers to learn a website's IP address based on its domain name).

44. In some cases, internet packets stay on a single network (e.g., two machines in the same office talking to each other), but in other cases, the packets may traverse dozens of intermediate networks before reaching their destination. The network path can change radically and dynamically as devices and connections are added or removed from the network.

45. Often, there are multiple routes that an internet packet could follow to reach its destination. Some connected networks may be faster, cheaper, or have a wider reach. Moreover, many high-bandwidth connections route traffic based on complex contractual arrangements, which take into account factors such as cost, the type of traffic, or the balance between inbound and outbound traffic. Networks that are strategically well-connected and have high bandwidth are likely to be used for transit by packets coming from other, less-well-connected networks. These more strategically connected networks, which often link large metropolitan areas, are collectively referred to as the internet "backbone." The overwhelming majority of backbone links are fiber-optic cables, because fiber-optic connections have high bandwidth and can distribute data over long distances.

46. The internet backbone includes the approximately 49 international submarine cables that carry internet communications into and out of the United States and that land at approximately 43 different points within the country. The vast majority of international traffic into and out of the United States traverses this limited number of submarine cables.

*Upstream Surveillance*

47. The NSA conducts Upstream surveillance by connecting surveillance devices to multiple major internet cables, switches, and routers on the internet backbone inside the United

States. These access points are controlled by the country's largest telecommunications providers, including Verizon Communications, Inc. and AT&T, Inc. In some or all instances, aspects of Upstream surveillance may be conducted by the telecommunications providers on the government's behalf.

48. Upstream surveillance is intended to enable the comprehensive monitoring of international internet traffic. With the assistance of telecommunications providers, the NSA intercepts a wide variety of internet communications, including emails, instant messages, webpages, voice calls, and video chats. It copies and reviews substantially all international emails and other "text-based" communications—*i.e.*, those whose content includes searchable text.

49. More specifically, Upstream surveillance encompasses the following processes, some of which are implemented by telecommunications providers acting at the NSA's direction:

- **Copying.** Using surveillance devices installed at key access points along the internet backbone, the NSA makes a copy of substantially all international text-based communications—and many domestic ones—flowing across certain high-capacity cables, switches, and routers. The copied traffic includes email, internet-messaging communications, web-browsing content, and search-engine queries.

- **Filtering.** The NSA attempts to filter out and discard some wholly domestic communications from the stream of internet data, using IP filters for instance, while preserving international communications. The NSA's filtering out of domestic communications is incomplete, however, for multiple reasons. Among them, the NSA does not eliminate bundles of domestic and international communications that transit the internet backbone together. Nor does it eliminate domestic communications that happen to be routed abroad.

- **Content Review.** The NSA reviews the copied communications—including their full content—for instances of its search terms. The search terms, called "selectors," include email addresses, phone numbers, IP addresses, and other identifiers that NSA analysts believe to be associated with foreign intelligence targets. Again, the NSA's targets are not limited to suspected foreign agents and terrorists, nor are its selectors limited to individual email addresses. The NSA may monitor or "task" selectors used by large

groups of people who are not suspected of any wrongdoing—such as the IP addresses of computer servers used by hundreds of different people.

- **Retention and Use.** The NSA retains all communications that contain selectors associated with its targets, as well as those that happened to be bundled with them in transit. As discussed further below, NSA analysts may read, query, data-mine, and analyze these communications with few restrictions, and they may share the results of those efforts with the FBI, including in aid of criminal investigations.

50. One aspect of the processes outlined above bears emphasis: Upstream surveillance is not limited to communications sent or received by the NSA's targets. Rather, it involves the surveillance of essentially *everyone's* communications. The NSA systematically examines the full content of substantially all international text-based communications (and many domestic ones) for references to its search terms. In other words, the NSA copies and reviews the communications of millions of innocent people to determine whether they are discussing or reading anything containing the NSA's search terms. The NSA's practice of reviewing the *content* of communications for selectors is sometimes called "about" surveillance. This is because its purpose is to identify not just communications that are to or from the NSA's targets but also those that are merely "about" its targets. This is the digital analogue of having a government agent open every piece of mail that comes through the post to determine whether it mentions a particular word or phrase. Most pieces of mail—or email—will contain nothing of interest, but the government must still look through each one to find out. Although it could do so, the government makes no meaningful effort to avoid the interception of communications that are merely "about" its targets; nor does it later purge those communications.

51. Prior to the summer of 2013, the government had not publicly disclosed the fact that, under the FAA, it routinely reviews communications that are neither to nor from its targets. As the Privacy and Civil Liberties Oversight Board observed, "The fact that the

government engages in such collection is not readily apparent from the face of the statute, nor was collection of information 'about' a target addressed in the public debate preceding the enactment of FISA or the subsequent enactment of the FISA Amendments Act."

Targeting and Minimization Procedures

52. As indicated above, the FAA requires the government to adopt targeting and minimization procedures that govern who may be targeted for surveillance by executive-branch employees and how communications are to be handled once intercepted. These procedures are extremely permissive, and to the extent they impose limitations, those restrictions are riddled with exceptions.

53. Nothing in the targeting procedures meaningfully constrains the government's selection of foreign targets. Nor do the targeting procedures require the government to take measures to avoid intercepting U.S. persons' international communications. The targeting procedures expressly contemplate "about" surveillance, and thus the interception and review of communications between non-targets.

54. The minimization procedures are equally feeble. They impose no affirmative obligation on the NSA to promptly identify and purge U.S. persons' communications once they have been obtained. Rather, they allow the NSA to retain communications gathered via Upstream surveillance for as long as three years by default. It can retain those communications indefinitely if the communications are encrypted; if they are found to contain foreign intelligence information (again, defined broadly); or if they appear to be evidence of a crime. Indeed, the NSA may even retain and share wholly domestic communications obtained through the accidental targeting of U.S. persons if the NSA determines that the communications contain "significant foreign intelligence information" or evidence of a crime. The minimization

procedures also expressly contemplate that the NSA will intercept, retain, and disseminate attorney-client privileged communications. The minimization procedures bar the NSA from querying Upstream data using identifiers associated with specific U.S. persons, but they do not otherwise prohibit the NSA from conducting queries designed to reveal information to, from, or about U.S. persons.

The Surveillance of Plaintiffs

55. Plaintiffs are educational, legal, human rights, and media organizations. Their work requires them to engage in sensitive and sometimes privileged communications, both international and domestic, with journalists, clients, experts, attorneys, civil society organizations, foreign government officials, and victims of human rights abuses, among others.

56. By intercepting, copying, and reviewing substantially all international text-based communications—and many domestic communications as well—as they transit telecommunications networks inside the United States, the government is seizing and searching Plaintiffs' communications in violation of the FAA and the Constitution.

57. The conclusion that the government is seizing and searching Plaintiffs' communications is well-founded for at least four reasons.

58. First, the sheer volume of Plaintiffs' communications makes it virtually certain that the NSA has intercepted, copied, and reviewed at least some of their communications. In the course of a year, Plaintiffs collectively engage in more than one trillion international internet communications. As explained further below, Upstream surveillance could achieve the government's stated goals only if it entailed the copying and review of a large percentage of international text-based traffic. However, even if one assumes a 0.00000001% chance—one one-hundred millionth of one percent—of the NSA copying and reviewing any particular

communication, the odds of the government copying and reviewing at least one of the Plaintiffs' communications in a one-year period would be greater than 99.9999999999%.

59. In reality, this calculation understates the likelihood that the NSA has intercepted, copied, and reviewed Plaintiffs' communications, because large swaths of internet traffic that are not amenable to the text-based searches conducted in the course of Upstream surveillance and are likely of no foreign-intelligence interest to the government. By some estimates, for example, two-thirds of internet traffic consists of video traffic. The NSA could readily configure its surveillance equipment to ignore that traffic, or at least the significant portions of it (e.g., Netflix traffic) that are almost certainly of no interest. Because of the substantial efficiency gains to be had, it is extremely likely that the government engages in this kind of filtering, allowing it to more comprehensively monitor text-searchable traffic like that of Plaintiffs.

60. Second, the geographic distribution of Plaintiffs' contacts and communications across the globe makes it virtually certain that the NSA has intercepted, copied, and reviewed Plaintiffs' communications. As noted above, the internet backbone includes the approximately 49 international submarine cables carrying the vast majority of internet traffic into and out of the United States. It also includes the limited number of high-capacity terrestrial cables that carry traffic between major metropolitan areas within the United States, or between the United States and Canada or Mexico. The junctions where these backbone cables meet are in essence "chokepoints"—because almost all international internet traffic (as well as a significant share of domestic traffic) flows through one or more of them. Prime examples are the points where international submarine cables come ashore. The government has acknowledged using

Upstream surveillance to monitor communications at "international Internet link[s]" on the internet backbone.

61. Given the relatively small number of international chokepoints, the immense volume of Plaintiffs' communications, and the fact that Plaintiffs communicate with individuals in virtually every country on earth, Plaintiffs' communications almost certainly traverse every international backbone link connecting the United States with the rest of the world.

62. Third, and relatedly, in order for the NSA to reliably obtain communications to, from, or about its targets in the way it has described, the government must be copying and reviewing all the international text-based communications that travel across a given link. That is because, as a technical matter, the government cannot know beforehand which communications will contain selectors associated with its targets, and therefore it must copy and review all international text-based communications transiting that circuit in order to identify those of interest. As the Privacy and Civil Liberties Oversight Board explained with respect to Upstream surveillance, "Digital communications like email, however, enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them." Because backbone cables carry vast amounts of internet traffic, the number of communications whose contents will be copied and reviewed will be enormous, regardless of how many the government ultimately retains.

63. There is an even more basic reason that, in conducting Upstream surveillance, the government must be monitoring all the international text-based communications that travel across a given link. To search the contents of any text-based communication for instances of the NSA's "selectors" as that communication traverses a particular backbone link, the

government must first copy and reassemble all of the packets that make up that communication. Those packets travel independently of one another, intermingled with packets of other communications in the stream of data. Where the government seeks to identify communications to, from, or about its many targets, as it does using Upstream surveillance, the packets of interest cannot be segregated from other, unrelated packets in advance. Rather, in order to reliably intercept the communications it seeks, the government must first copy *all* such packets traversing a given backbone link, so that it can reassemble and review the transiting communications in the way it has described.

64. In short, for every backbone link that the NSA monitors using Upstream surveillance, the monitoring must be comprehensive in order for the government to accomplish its stated goals. Accordingly, even if the NSA conducts Upstream surveillance on only a single internet backbone link, it must be intercepting, copying, and reviewing at least those communications of Plaintiffs traversing that link. In fact, however, the NSA has confirmed that it conducts Upstream surveillance at more than one point along the internet backbone, through the compelled assistance of multiple major telecommunications companies.

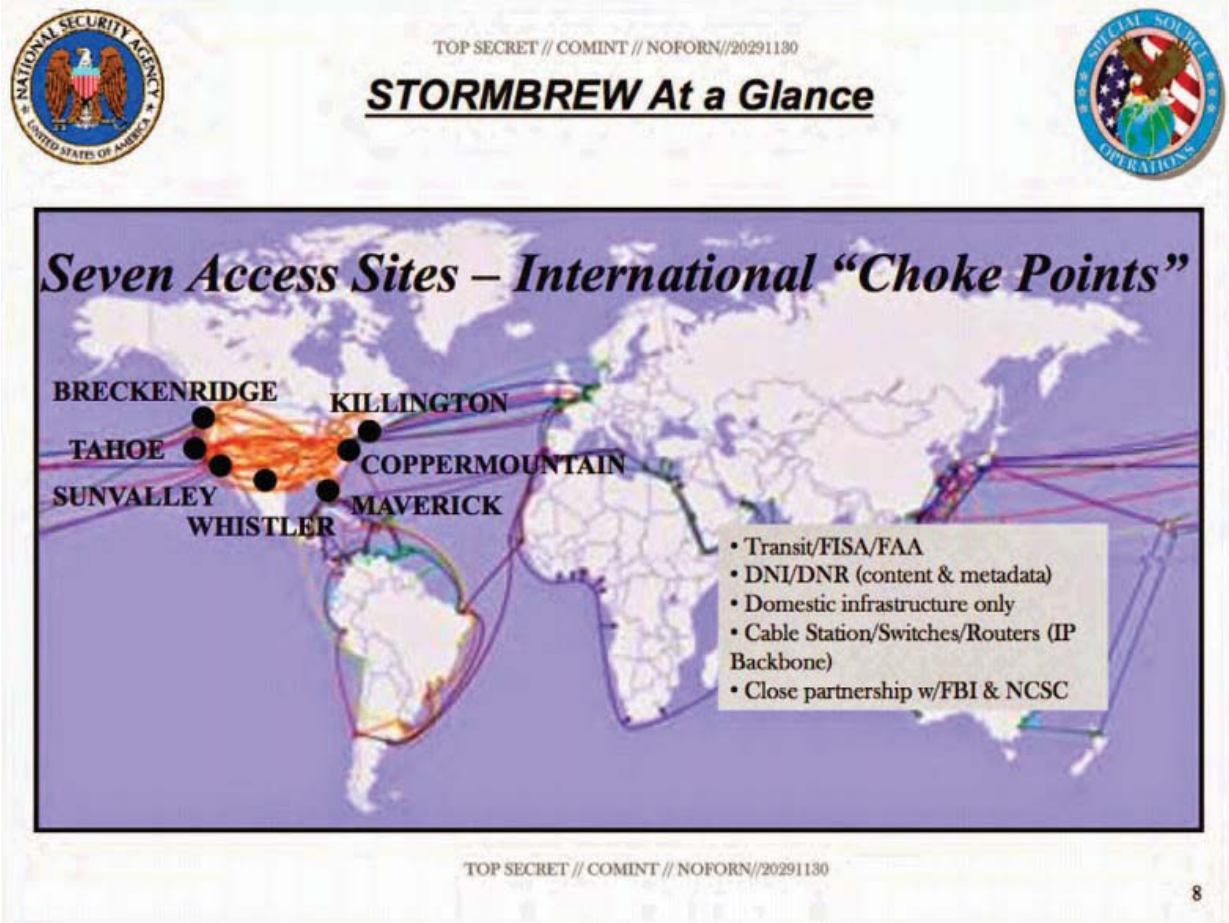
65. Fourth, given the way the government has described Upstream surveillance, it has a strong incentive to intercept communications at as many backbone chokepoints as possible. The government's descriptions of Upstream surveillance make clear that the government is interested in obtaining, with a high degree of confidence, all international communications to, from, or about its targets. For example, the Privacy and Civil Liberties Oversight Board has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." And it has said about Upstream

surveillance more generally that its "success . . . depends on collection devices that can reliably acquire data packets associated with the proper communications."

66. If the government's aim is to "comprehensively" and "reliably" obtain communications to, from, and about targets scattered around the world, it must conduct Upstream surveillance at many different backbone chokepoints. That is especially true because the communications of individual targets may take multiple paths when entering or leaving the United States. When two people communicate in real-time, the communications they exchange frequently take different routes across the internet backbone, even though the end-points are the same. In other words, in the course of a single exchange, the communications *from* a target frequently follow a different path than those *to* the target. Relatedly, a target's location may vary over time, as do the network conditions that determine a given communication's path from origin to destination. As a result, a target's communications may traverse one backbone cable or chokepoint at one moment, but a different one later. In fact, as the Privacy and Civil Liberties Oversight Board observed, even a single email "can be broken up into a number of data packets that take different routes to their common destination." Because of these variables, Upstream surveillance would be comprehensive only if it were implemented at a number of backbone chokepoints.

67. For the four reasons stated above, it is a virtual certainty that the NSA is intercepting, copying, and reviewing Plaintiffs' communications.

68. This conclusion is corroborated by government documents that have been published in the press. For example, one NSA slide illustrates the Upstream surveillance facilitated by just a single provider (referred to as "STORMBREW") at seven major international chokepoints in the United States:




69. Similarly, another NSA document states that, in support of FAA surveillance, the "NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." In fact, in describing the scale and operation of Upstream surveillance, *The New York Times* has reported, based on interviews with senior intelligence officials, that "the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border."

70. The government's interception, copying, and review of Plaintiffs' communications while in transit is a violation of Plaintiffs' reasonable expectation of privacy in

those communications. It is also a violation of Plaintiffs' right to control those communications and the information they reveal and contain.

71. Furthermore, because of the nature of their communications, and the location and identities of the individuals and groups with whom and about whom they communicate, there is a substantial likelihood that Plaintiffs' communications intercepted by the NSA through Upstream surveillance are retained, read, and disseminated.

72. The retention, reading, and dissemination of Plaintiffs' communications is a further, discrete violation of Plaintiffs' reasonable expectation of privacy in those communications. It is also a further, discrete violation of Plaintiffs' right to control those communications and the information they reveal and contain.

73. Plaintiffs, in connection with constitutionally protected activities, communicate with people whom the government is likely to target when conducting Upstream surveillance, including foreign government officials, journalists, experts, human rights defenders, victims of human rights abuses, and individuals believed to have information relevant to counterterrorism efforts.

74. A significant amount of the information that Plaintiffs exchange over the internet is "foreign intelligence information" within the meaning of the FAA.

75. Because of ongoing government surveillance, including Upstream surveillance, Plaintiffs have had to take burdensome and sometimes costly measures to minimize the chance that the confidentiality of their sensitive information will be compromised. Plaintiffs have variously had to develop new protocols for transmitting sensitive information, to travel long distances to collect information that could otherwise have been shared electronically, and in some circumstances to forgo particularly sensitive communications altogether.

76. Because of ongoing government surveillance, including Upstream surveillance, Plaintiffs are not able to gather and relay information, represent their clients, and engage in domestic and international advocacy as they would in the absence of the surveillance. Upstream surveillance reduces the likelihood that clients, users, journalists, witnesses, experts, civil society organizations, foreign government officials, victims of human rights abuses, and other individuals will share sensitive information with Plaintiffs.

77. Upstream surveillance is inhibiting the constitutionally protected communications and activities of Plaintiffs and others not before the Court.

Wikimedia Foundation

78. Wikimedia is a non-profit organization dedicated to encouraging the growth, development, and distribution of free, multilingual, educational content. In this effort, it develops and maintains "wiki"-based projects, and provides the full contents of those projects to individuals around the world free of charge. At present, Wikimedia operates twelve free-knowledge projects ("Projects") as well as other related websites and pages on the internet.

79. The best-known of Wikimedia's Projects is Wikipedia—a free internet encyclopedia that is one of the top ten most-visited websites in the world and one of the largest collections of shared knowledge in human history. In 2014, Wikipedia contained more than 33 million articles in over 275 languages, and Wikimedia sites received between approximately 412 and 495 million monthly visitors. Wikipedia's content is collaboratively researched and written by millions of volunteers, many of whom choose not to identify themselves, and is in most instances open to editing by anyone. Volunteers also use Wikipedia discussion forums and "discussion pages" to debate the editorial policies and decisions required for reliable and neutral content.

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

81. Wikimedia encourages individuals around the world to contribute to the Projects by communicating information to Wikimedia. Wikimedia receives and maintains this information, and subsequently communicates it to the many other individuals who seek to access, engage with, and further add to Wikimedia's store of knowledge. The principal way in which Wikimedia communicates with its community—which, at its broadest level, consists of individuals who access or contribute to the body of knowledge comprising the twelve Projects—is via the internet.

82. Wikimedia provides the technical infrastructure for the Projects, much of which is hosted on Wikimedia's servers in Virginia, Texas, and California. In addition, Wikimedia develops software and provides tools for others to develop software platforms; develops mobile phone applications and enters into partnerships; administers grants to support activity that benefits the Wikimedia user community and the Wikimedia movement; provides administrative support to grantees; works with community members to organize conferences and community-outreach events globally; and engages in advocacy on issues that affect the Wikimedia community.

83. Wikimedia maintains an active and close relationship with the volunteers, contributors, and many other users who comprise the Wikimedia community. Wikimedia exists for this community and depends upon it: the user community plays a vital role in many of

Wikimedia's functions, including the creation of Wikimedia content, the development and enforcement of Wikimedia policies, the donation of funds that help Wikimedia thrive, and the governance of the organization as a whole. In short, Wikimedia operates interdependently with its user community in pursuit of a shared set of free-knowledge values.

84. Wikimedia's corporate structure and decision-making reflect this interdependence. In accordance with Wikimedia's bylaws, at least half of Wikimedia's Board of Trustees is selected by Wikimedia community members. That Board relies, in turn, on several user-staffed committees to oversee Board elections, consider grant applications, and recommend new Wikimedia chapters or community organizations. More generally, Wikimedia makes core organizational decisions after soliciting the input and preferences of its users on topics including its public-policy positions, the creation of new features and Projects, corporate strategy, and budgetary matters. For instance, Wikimedia staff frequently engage in "Community Consultations," in which community members can offer their views on these and other matters directly.

85. Wikimedia's community of volunteers, contributors, and readers consists of individuals in virtually every country on earth. Among many others, the Wikimedia community includes U.S. persons who are located abroad and who engage in international communications with Wikimedia.

86. Upstream surveillance implicates at least three categories of Wikimedia communications: (i) Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other; (ii) Wikimedia's internal "log" communications, which help it to

monitor, study, and improve its community members' use of the Projects; and (iii) communications by Wikimedia staff.

87. As the operator of one of the most-visited websites in the world, Wikimedia engages in an extraordinarily high volume of internet communications. From April 1, 2014 to March 31, 2015, Wikimedia websites received over 255 billion "page views." Over the lifespan of the Wikimedia Projects, Wikimedia's users have edited its pages more than two billion times. Each of these activities involves internet communications between Wikimedia and its users—the majority of whom are located abroad.

88. Indeed, Wikimedia engages in more than one trillion international communications each year, with individuals who are located in virtually every country on earth. For a user to view, search, log in, edit, or contribute to a Wikimedia Project webpage, the user's device must send at least one HTTP or HTTPS "request" to a Wikimedia server. "HTTP" and "HTTPS" are common protocols for transmitting data via the internet, including the content of many webpages. The number of requests required for a user to access a particular webpage depends on the number of graphics, videos, and other specialized components featured on the page. After receiving such a user request, the Wikimedia server transmits an HTTP or HTTPS "response" to the user's device, where the content of the requested webpage component is rendered and displayed to the user. In May 2015, Wikimedia's U.S.-based servers received more than 88 billion HTTP or HTTPS requests from outside the United States. At this rate, Wikimedia receives more than one trillion HTTP or HTTPS requests annually, and transmits more than one trillion HTTP or HTTPS responses back to those Wikimedia users abroad.

89. Wikimedia's HTTP and HTTPS communications are essential to its organizational mission, as is its ability to control and maintain the privacy of these communications. The communications reveal and contain some of the most sensitive information that Wikimedia possesses: which specific webpages each particular person is editing or visiting. In other words, they reveal who is reading—or writing—what.

90. For example, among other private information, HTTP and HTTPS requests reveal or contain the user's IP address; the URL of the webpage sought by the user, which often conveys information about the content of the requested page; and the "user agent," which may identify the manufacturer, model, version, and other information about the user's device. Many requests also contain other types of private information, such as a user's log-in credentials; the referrer, which reflects information about the previous webpage the user visited; the search terms a user entered to query Wikimedia's webpages; "cookies," which include information that can be used to link a user to his or her prior Wikimedia requests and prior approximate geolocation; a user's non-public "draft" contributions to Wikimedia; or a user's private questions, comments, or complaints, submitted via Wikimedia's online feedback platform.

91. In much the same way, Wikimedia's HTTP and HTTPS responses may reveal or contain, among other private information, the user's IP address; the content of the requested webpage component; the URL of the webpage the user should be redirected to; "cookies," which include information used to link a user to subsequent Wikimedia requests and his or her approximate geolocation; search terms; a user's username; a user's non-public "draft" contributions; and a user's private questions, comments, or complaints.

92. In furtherance of its mission, Wikimedia also frequently engages in communications that permit its users to interact with one another more directly. For example, a

registered user of Wikimedia may send an email via Wikimedia to another registered user, so long as both have enabled email communications on their Wikimedia accounts. Similarly, Wikimedia engages in communications that allow users to interact in small or limited groups—including over wikis that only certain users, such as user-community leaders, have access to, and mailing lists with restricted membership. Some of these communications are transmitted via HTTP or HTTPS; others rely on different protocols. All of these interactions involve communications between Wikimedia and its community members.

93. The second category of Wikimedia communications are its internal, proprietary "log" communications, which help it to monitor, study, and improve the Projects. In particular, every time Wikimedia receives an HTTP or HTTPS request from a person accessing a Project webpage, it creates a corresponding log entry. Among other private information, logs contain the user's IP address; the URL of the webpage sought by the user; the time the request was received by Wikimedia's server; and the "user agent," which may identify the manufacturer, model, version, and other information about the user's device. Depending on the location of the user and the routing of her request, the log may be generated by Wikimedia's servers abroad, which in turn send the log to Wikimedia in the United States. In May 2015, Wikimedia transmitted more than 140 billion logs from its servers abroad to its servers in the United States. The organization relies on its logs for a variety of analytical projects, which are designed to improve Wikimedia's operations and the experience of those using the Projects.

94. Wikimedia's communications with its community members—as well as its internal logs—link each user's page views, searches, and contributions with his or her IP address, as well as with other user-specific information. As a rule, Wikimedia maintains as private the IP addresses associated with its community members and their individual

interactions with the Projects, except in those instances where an individual editor reveals his or her IP address publicly (i.e., is not logged in as a registered user). IP addresses, like telephone numbers, are often personally identifying, especially in conjunction with other information about a given communication or internet user. It is generally trivial to link a particular IP address with a particular person—thereby revealing his or her online activities—in part because internet service providers routinely maintain records of the IP addresses assigned to their network subscribers over time.

95. Because of the information they contain, Wikimedia's communications with its community members, as well as its internal communications related to the study and improvement of the Projects, are often sensitive and private. These communications reveal a detailed picture of the everyday concerns and reading habits of Wikimedia's users, and often constitute a record of their political, religious, sexual, medical, and expressive interests.

96. Seizing and searching Wikimedia's communications is akin to seizing and searching the patron records of the largest library in the world—except that Wikimedia's communications provide a more comprehensive and detailed picture of its users' interests than any previous set of library records ever could have offered.

97. Upstream surveillance permits the government to observe—continuously—which of Wikimedia's millions of webpages are being read or edited at any given moment, and by whom. Moreover, it allows the government to review those communications for any reference to its tens of thousands of search terms, and to retain a copy of any communication that is of interest.

98. As an organization, Wikimedia has an acute privacy interest in its communications—one on par with that of users themselves. That is because Wikimedia's

mission and existence depend on its ability to ensure that readers and editors can explore and contribute to the Projects privately when they choose to do so. Wikimedia's communications reveal who has contributed to the Projects or visited them in search of information—and, just as importantly, exactly *what* information Wikimedia has exchanged with any individual user. With the partial exception of editors who publicly disclose their IP addresses, these exchanges are not public; they are private interactions between Wikimedia and its community members. If it were otherwise, Wikimedia would have immense difficulty both gathering content and sharing information as widely as possible. This privacy is necessary to foster trust with community members and to encourage the growth, development, and distribution of free educational content.

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

100. Wikimedia takes steps to protect the privacy of its communications and the confidentiality of the information it thereby receives. For instance, because of the sensitivity of Wikimedia's communications with its community members, Wikimedia seeks to collect and retain as little information about those exchanges as possible. Where it does collect such information, Wikimedia strives to keep it for only a limited amount of time, consistent with the maintenance, understanding, and improvement of the Projects and with Wikimedia's legal obligations. Still, Wikimedia possesses a large volume of sensitive information about its interactions with its community members, and it transmits a large volume of sensitive information about those interactions every day.

101. Wikimedia defends the privacy of its communications in other ways, including through both technical measures and legal action. Wikimedia undertakes costly and burdensome measures to ensure the security of its communications and the data it retains as a result. Wikimedia also assures its community via policies, public statements, and guidelines that it will reject third-party requests for non-public user information unless it is legally required to disclose that information. In keeping with these assurances, Wikimedia resists third-party demands for information that are overly broad, unclear, or irrelevant; notifies users individually of information requests when legally permitted; and provides legal defense funds for certain community members who are subject to lawsuits or demands for non-public information as a result of their participation in the Projects.

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

103. Wikimedia's communications—with its community members, its internal communications, and its staff communications—are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of Wikimedia, its staff, and its users, and it violates their right to control those communications and the information they contain.

104. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Wikimedia's international communications because Wikimedia is communicating with or about persons the government has targeted for Upstream surveillance. Wikimedia's international contacts include foreign telecommunications companies, foreign government

officials, political and business leaders, universities, Wikimedia users and their legal counsel, Wikimedia trustees and international contractors, Wikimedia's international outside legal counsel, project partners, grantees, and volunteers—some of whom are likely targets. Wikimedia's communications with these contacts sometimes concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Wikimedia communicates both with and about these likely targets. Wikimedia's international communications contain, among other things, information about its foreign contacts, including the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to Wikimedia's work.

105. Moreover, more than one trillion of Wikimedia's international communications each year—its HTTP and HTTPS transmissions as well as its internal logs of user activity—contain details such as website addresses and IP addresses. Whenever a Wikimedia user abroad edits or contributes to a Project webpage that happens to reference one of the NSA's selectors, Wikimedia engages in an international communication containing that selector. The same is often true when a Wikimedia user abroad simply reads such a Project webpage. Some of these communications are likely retained, read, and disseminated in the course of Upstream surveillance.

106. Because Wikipedia is a comprehensive encyclopedic resource, it includes entries related to virtually any foreign organization or company the U.S. government might target for Upstream surveillance. Many of these entries contain website addresses and domain names associated with those likely targets. Notably, website addresses or domain names associated with organizations on the U.S. State Department's Foreign Terrorist Organization list appear over 700 times on Project webpages—including those describing organizations, like

Uzbekistan's Islamic Jihad Union, whose communications the U.S. government has targeted using FAA surveillance.

107. The NSA has expressed interest in surveilling Wikimedia's communications. An NSA slide disclosed by the media asks, "Why are we interested in HTTP?" It then answers its own question: "Because nearly everything a typical user does on the Internet uses HTTP." This statement is surrounded by the logos of major internet companies and websites, including Facebook, Yahoo, Twitter, CNN.com, and Wikipedia. The slide indicates that, by monitoring HTTP communications, the NSA can observe "nearly everything a typical user does" online—including individuals' online reading habits and other internet activities. This information is queried and reviewed by analysts using a search tool that allows NSA analysts to examine data intercepted pursuant to the FAA and other authorities.



108. Upstream surveillance undermines Wikimedia's ability to conduct its work. Wikimedia depends on its ability to ensure anonymity for individuals abroad who view, edit, or otherwise use Wikimedia Projects and related webpages. The ability to read, research, and write anonymously is essential to the freedoms of expression and inquiry. In addition, Wikimedia's staff depend on the confidentiality of their communications, including in some cases their ability to ensure that their contacts' identities will not be revealed. Because of these twin needs for anonymity and confidentiality, Upstream surveillance harms the ability of Wikimedia's staff to engage in communications essential to their work and compromises Wikimedia's organizational mission by making online access to knowledge a vehicle for U.S. government monitoring.

109. Due in part to NSA surveillance, including Upstream surveillance, Wikimedia has undertaken burdensome and costly measures to protect its communications, including adopting more secure methods of electronic communication, and in some instances self-censoring communications or forgoing electronic communications altogether. These measures divert Wikimedia's time and monetary resources as a non-profit entity from other important organizational work.

110. Despite these precautions, Wikimedia believes that Upstream surveillance has resulted and will result in some foreign readers, editors, contributors, and volunteers being less willing to read, contribute to, or otherwise engage with Wikimedia's Projects. For instance, some Wikimedia users have expressed reluctance to continue participating in the Wikimedia movement because of U.S. government surveillance, including FAA surveillance. The loss of these foreign users is a direct detriment to Wikimedia, its ability to receive information and associate with its community members, and its organizational goal of increasing global access

to knowledge. It also harms Wikimedia's domestic users, who do not have access to information and opinions that Wikipedia's foreign contributors would otherwise have provided. Similarly, Wikimedia believes that Upstream surveillance reduces the likelihood that Wikimedia's foreign volunteers, grantees, and other contacts will communicate with staff members, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

111. Because Wikimedia's community members are so numerous, because they are dispersed across the globe, and because millions of them choose to interact with Wikimedia anonymously, their rights are likely to be impaired if Wikimedia is unable to assert claims on their behalf. That is especially so because Wikimedia is uniquely capable of presenting the aggregate effects that Upstream surveillance has on community members' ability to contribute to the Projects and to receive information from others.

National Association of Criminal Defense Lawyers

112. The National Association of Criminal Defense Lawyers ("NACDL") is a membership organization based in Washington, D.C. NACDL's mission is to foster the integrity, independence, and expertise of the criminal defense profession, and to promote the proper and fair administration of justice. NACDL has approximately 9,200 members as well as 90 local, state, and international affiliate organizations with approximately 40,000 members. NACDL's interest in challenging the lawfulness of Upstream surveillance is germane to the organization's mission and purpose, and to its relationship with its members. As explained below, because unlawful U.S. government surveillance profoundly affects the ability of

criminal defense attorneys to ensure that accused persons receive effective counsel, such surveillance interferes with the proper and fair administration of justice.

113. As defense attorneys, NACDL's members engage in international and domestic internet communications that are essential to the effective representation of their clients. Among other things, NACDL's members routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad as part of their representations.

114. The communications of NACDL's members are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of members' communications and it violates their right to control their communications and the information they contain.

115. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates international communications of NACDL's members because they are communicating with or about persons the government has targeted for Upstream surveillance. In the course of their representations, NACDL members communicate internationally with clients, clients' families, witnesses, journalists, human rights organizations, experts, investigators, and foreign government officials, some of whom are likely targets. Their communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." NACDL members communicate both with and about these likely targets. Members' international communications contain, among other things, details about their foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to their work.

116. One group of NACDL members is especially likely to have their communications retained, read, and disseminated in the course of Upstream surveillance: defense attorneys who represent individuals in criminal prosecutions in which the government has acknowledged its use FAA surveillance. In these cases, the government's prosecution of the defendant is based on evidence obtained from an FAA target. As a result, defense attorneys are especially likely to engage in communications to, from, or about FAA targets in the course of investigating the government's allegations, contacting witnesses, and collecting their own evidence. Indeed, in several of these cases, the targeted selector—*e.g.*, the targeted email address—has been identified in press reports or may be ascertained from congressional testimony and court filings. NACDL defense attorneys who communicate internationally with or about that targeted selector will have their communications retained by the government, much as their clients' communications were warrantlessly intercepted and retained.

117. NACDL members have an ethical obligation to protect the confidentiality of their clients' information, including information covered by the attorney-client privilege.

118. Upstream surveillance compromises NACDL members' ability to comply with their ethical obligations and undermines their effective representation of their clients. Members' defense work depends on the confidentiality of their communications, including their ability to assure contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, NACDL's members have undertaken burdensome and costly measures to protect their communications, including adopting more secure methods of electronic communication, traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, NACDL believes that

Upstream surveillance reduces the likelihood that potential sources, witnesses, experts, and foreign government officials will share sensitive information with NACDL's members, because those contacts fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

*NACDL Member Joshua L. Dratel*

119. Joshua L. Dratel is a nationally recognized criminal defense lawyer in New York City who has been a member of NACDL since 1985. He is Chair of NACDL's National Security Committee, co-Chair of NACDL's Select Committee on Military Tribunals, and Co-Chair of its Amicus Curiae Committee. From 2003 to 2009, he served as a member of the Board of Directors of NACDL. He is also co-editor of *The Torture Papers: The Legal Road to Abu Ghraib* (Cambridge University Press 2005).

120. Mr. Dratel's litigation experience encompasses all aspects of criminal defense, and among other clients, he represents individuals accused of internet- and terrorism-related crimes. For example, he defended Wadith El Hage in *United States v. Usama Bin Laden*, the prosecution resulting from the 1998 bombings of the U.S. embassies in Kenya and Tanzania. Mr. Dratel also represented David Hicks—who was detained at Guantánamo Bay for six years—in U.S. military commission proceedings. The U.S. Court of Military Commission Review recently overturned Mr. Hicks's conviction for material support for terrorism. Mr. Dratel's current clients include Baasaly Moalin, who is appealing from a conviction of charges of material support for terrorism.

121. Mr. Dratel's law practice also includes a client who has received notice of FAA surveillance, and he previously represented a client in another case where officials have told

Congress that the government used FAA surveillance in the course of its investigation. He has defended other individuals in prosecutions where there is reason to believe the government relied on such surveillance.

122. In connection with his defense work and confidential consultations with defense attorneys in other national security-related cases, Mr. Dratel routinely engages in both domestic and international communications via the internet. Many of the individuals with whom he exchanges information are located abroad, and are neither U.S. citizens nor permanent residents. Their communications occur via email, instant messenger, and text messaging.

123. The vast majority of Mr. Dratel's international communications as a defense attorney are sensitive, and many of them are privileged or otherwise protected from disclosure by the attorney work-product doctrine.

124. Mr. Dratel's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of his communications and it violates his right to control his communications and the information they contain.

125. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Mr. Dratel's international communications because he is communicating with persons the government has targeted for Upstream surveillance. In the course of his representations, Mr. Dratel communicates internationally with clients, clients' families, lawyers, witnesses, journalists, human rights organizations, experts, investigators, and foreign government officials, some of whom are likely targets. Most notably, his international contacts include individuals the U.S. government has targeted for prosecution for terrorism-related crimes, as well as their families, friends, and associates, including their attorneys overseas. For example, Mr. Dratel communicates via the internet with his former client, Mr. Hicks, who lives

in Australia following his release from Guantánamo Bay. In addition, Mr. Dratel's communications with his international contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Mr. Dratel also communicates with likely FAA targets when he visits websites hosted overseas on the internet. This internet browsing involves communications with selectors—such as domain names and IP addresses—that the NSA has likely targeted for FAA surveillance. In his representation of defendants charged with terrorism-related crimes, it is often necessary for him to review websites maintained by terrorist organizations abroad, so that he can understand the facts related to certain investigations and prosecutions.

126. Similarly, there is a substantial likelihood that the NSA retains, reads, and disseminates Mr. Dratel's international communications because he is communicating *about* persons the government has targeted for Upstream surveillance. Mr. Dratel's international communications contain, among other things, details about his foreign contacts and other important sources of information—details such as the email addresses, phone numbers, social media identities, and website addresses of foreign individuals and organizations relevant to his work.

127. The fact that Mr. Dratel's clients have been subject to FAA surveillance themselves, or involved in investigations where others were subject to such surveillance, makes the NSA's retention and dissemination of Mr. Dratel's own communications especially likely. In representing these clients, Mr. Dratel is almost certain to engage in communications to, from, or about FAA targets in the course of investigating the government's allegations, contacting witnesses, and collecting evidence abroad via the internet. When Mr. Dratel

communicates with or about persons and selectors targeted under the FAA, he is subject to FAA surveillance just like his clients.

128. Due in part to U.S. government surveillance, including Upstream surveillance, Mr. Dratel has had to undertake burdensome and costly measures to protect his international communications, and in certain instances has forgone those communications altogether. For example, Mr. Dratel has had to and will have to travel abroad to gather information in-person that he would otherwise have gathered by electronic communication. Such travel is time-consuming and costly. He has also paid for and will have to pay for investigators abroad to travel to the United States to meet with him in-person to discuss their cases. In addition, Mr. Dratel routinely relies on time-consuming security measures, such as Pidgin Encryption and PGP, to encrypt his domestic and international instant messages and emails, in an effort to protect especially sensitive privileged communications and work product. Mr. Dratel also routinely censors his own speech (and asks his international contacts to do the same) in electronic communications. These precautions and security measures are not voluntary; they are the result of Upstream surveillance and the rules of professional responsibility that apply to Mr. Dratel as an attorney.

129. As a general matter, Upstream surveillance compromises Mr. Dratel's ability to communicate with his clients overseas and to gather information relevant and necessary to his work. This surveillance makes it difficult, expensive, and sometimes impossible to obtain information from individuals outside of the United States. In some instances, the increased awareness of U.S. government surveillance has resulted and will result in clients, lawyers, and potential witnesses limiting the information that they share with Mr. Dratel and that he shares with them. Indeed, some witnesses abroad have not and will not communicate with Mr. Dratel

at all electronically, because they believe that by sharing information with him, they are also sharing information with the U.S. government. At times, Mr. Dratel must forgo these communications altogether. The cost of traveling to certain remote areas of the globe to interview a potential witness in-person can be too high to justify the travel, and some regions are simply too dangerous or inaccessible to permit in-person visits.

Human Rights Watch

130. HRW is a non-profit, non-governmental human rights organization based in New York City. It employs approximately 400 staff members located across offices around the world. Formed in 1978, HRW's mission is to defend the rights of people worldwide. HRW conducts fact-finding investigations into human rights abuses by governments and non-state actors in all regions of the world.

131. HRW engages in international and domestic internet communications that are essential to its mission. Among other things, HRW's U.S.-based staff routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out HRW's research, reporting, and advocacy work.

132. HRW's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of HRW's communications and it violates HRW's right to control those communications and the information they contain.

133. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates HRW's international communications because HRW is communicating with or about persons the government has targeted for Upstream surveillance. HRW's international contacts include foreign government officials, humanitarian agencies, think tanks, military officials, human rights defenders, politicians, dissidents, victims of human rights abuses,

perpetrators of human rights abuses, religious groups, media, and scholars, some of whom are likely targets. HRW's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." HRW communicates both with and about these likely targets. HRW's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to HRW's work.

134. Upstream surveillance undermines HRW's ability to conduct its work. HRW's research, reporting, and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, HRW has undertaken burdensome and costly measures to secure and protect its communications, including adopting more secure methods of electronic communication, traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, HRW believes that Upstream surveillance reduces the likelihood that sources, witnesses, experts, foreign government officials, and victims of human rights abuses will share sensitive information with HRW's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

Amnesty International USA

135. AIUSA, headquartered in New York City, is one of Amnesty International's largest national sections, with hundreds of thousands of members and supporters. Through its

advocacy campaigns, AIUSA seeks to expose and stop human rights abuses in the United States and throughout the world.

136. AIUSA engages in international and domestic internet communications that are essential to its mission. Among other things, some of AIUSA's U.S.-based staff—as well as some AIUSA members who serve as volunteer specialists on particular countries and thematic issues—routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out AIUSA's reporting and advocacy work.

137. AIUSA's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of AIUSA's communications and it violates AIUSA's right to control those communications and the information they contain.

138. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates AIUSA's international communications because AIUSA is communicating with or about persons the government has targeted for Upstream surveillance. AIUSA's international contacts include Amnesty International researchers who are documenting and witnessing human rights violations in the field, human rights defenders, victims of violations and their families, eyewitnesses to violations, political dissidents, government officials, journalists, and lawyers, some of whom are likely targets. AIUSA's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." AIUSA communicates both with and about these likely targets. AIUSA's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to AIUSA's work.

139. Upstream surveillance undermines AIUSA's ability to conduct its work. AIUSA's reporting and advocacy depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, some AIUSA staff strive to communicate particularly sensitive matters in-person, and must sometimes avoid sensitive topics or forgo exchanging information about these matters altogether. Despite these precautions, AIUSA believes that Upstream surveillance reduces the likelihood that sources, witnesses, experts, foreign government officials, and victims of human rights abuses will share sensitive information with AIUSA's staff and members, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

PEN American Center

140. PEN is an association based in New York City of approximately 4,000 novelists, journalists, editors, poets, essayists, playwrights, publishers, translators, agents, and other professionals, and an even larger network of readers and supporters. It is the largest of the organizations within PEN International. For the last 90 years, PEN has worked to ensure that people all over the world are at liberty to create literature, to convey ideas freely, and to express their views unimpeded. One of PEN's core projects is to advocate on behalf of persecuted writers across the globe, so that they might be free to write and to express their ideas.

141. PEN engages in international and domestic internet communications that are essential to its mission. Among other things, PEN's U.S.-based staff routinely engage in

sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out PEN's research and advocacy work.

142. PEN's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of PEN's communications and it violates PEN's right to control those communications and the information they contain.

143. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates PEN's international communications because PEN is communicating with or about persons the government has targeted for Upstream surveillance. PEN's international contacts include writers whose work and experiences relate to political upheavals, human rights violations, freedom of the press, and government surveillance; those writers' families and legal representatives; human rights defenders; and other PEN partners in countries such as Syria, Cuba, China, Iran, and Ethiopia—some of whom are likely targets. PEN's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." PEN communicates both with and about these likely targets. PEN's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to PEN's work.

144. Upstream surveillance undermines PEN's ability to conduct its work. PEN's research and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, PEN staff have undertaken burdensome measures to secure and protect their

communications, including adopting more secure methods of electronic communication, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, PEN believes that Upstream surveillance reduces the likelihood that foreign writers and other contacts will share sensitive information with PEN's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

Global Fund for Women

145. GFW, based in San Francisco and New York City, is a grant-maker and a global advocate for women's human rights. GFW advances the movement for women's human rights by directing resources to and raising the voices of women worldwide. GFW invests in local, courageous women and women-led organizations, and creates digital advocacy campaigns on critical global issues for women and girls. Since its inception in 1986, GFW has awarded 9,921 grants totaling $120 million to 4,759 organizations in 175 countries.

146. GFW engages in international and domestic internet communications that are essential to its mission. Among other things, GFW's U.S.-based staff routinely engage in sensitive, confidential, and privileged internet communications with non-U.S. persons located abroad in carrying out GFW's grant-making and advocacy work.

147. GFW's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of GFW's communications and it violates GFW's right to control those communications and the information they contain.

148. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates GFW's international communications because GFW is communicating with or

about persons the government has targeted for Upstream surveillance. GFW's international contacts include foreign banks, foreign government agencies, funders, attorneys, and grantee and partner organizations working in conflict zones or on politically sensitive issues abroad, some of whom are likely targets. GFW's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." GFW communicates both with and about these likely targets. GFW's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to GFW's work.

149. Upstream surveillance undermines GFW's ability to conduct its work. GFW's grant-making depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, GFW's staff must exercise extreme caution when engaging in certain international communications, and in some instances avoid sensitive topics or forgo communications altogether. Some of GFW's international contacts will communicate with the organization only by phone or Skype, rather than email, because they believe that email is a less secure means of communication. Other of GFW's international contacts will communicate via email, but only if staff avoid using certain words in their communications that may result in further government scrutiny. Despite these precautions, GFW believes that Upstream surveillance reduces the likelihood that current and prospective grantees will share sensitive information with GFW's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the

other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Nation Magazine

150. The Nation is America's oldest weekly magazine of opinion, news, and culture. The Nation is also a digital media company, reporting daily on politics, social issues, and the arts. Its journalists report on a wide range of issues relating to international affairs, including the wars in Iraq and Afghanistan, the Israel–Palestine conflict, protest activities and politics in China and elsewhere in East Asia, and civil wars and other conflicts in Africa and Latin America.

151. The Nation engages in international and domestic internet communications that are essential to its mission. Among other things, The Nation's staff and contributing writers routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out The Nation's research, reporting, and editing.

152. The Nation's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of The Nation's communications and it violates The Nation's right to control those communications and the information they contain.

153. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates The Nation's international communications because The Nation is communicating with or about persons the government has targeted for Upstream surveillance. The Nation's international contacts include foreign journalists in conflict zones, foreign government officials, political dissidents, human rights activists, and members of guerrilla and insurgency movements, some of whom are likely targets. The Nation's communications with these

contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." The Nation communicates both with and about these likely targets. The Nation's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to The Nation's work.

154. Upstream surveillance undermines The Nation's ability to conduct its work. The Nation's research and reporting depends on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, The Nation has undertaken burdensome and costly measures to protect its communications, including adopting more secure methods of electronic communication, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, The Nation believes that Upstream surveillance reduces the likelihood that foreign journalists and sources will share sensitive information with The Nation, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Rutherford Institute

155. The Rutherford Institute, founded in 1982 and based in Virginia, is a civil liberties organization committed to protecting the constitutional freedoms of Americans and the human rights of all people. Rutherford provides free legal services in defense of civil liberties

and educates the public about constitutional and human rights issues. It also advocates on behalf of individuals abroad whose rights are threatened by foreign governments.

156. Rutherford engages in international and domestic internet communications that are essential to its mission. Among other things, Rutherford's staff, who are based in the U.S., routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out Rutherford's advocacy, legal, and educational activities.

157. Rutherford's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of Rutherford's communications, and it violates Rutherford's right to control those communications and the information they contain.

158. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates Rutherford's international communications because Rutherford is communicating with or about persons the government has targeted for Upstream surveillance. Rutherford's international contacts include human rights and civil liberties advocates, foreign government officials, and individuals whose rights are threatened by the U.S. or foreign governments, some of whom are likely targets. Rutherford's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." Rutherford communicates both with and about these likely targets. Rutherford's international communications, among other things, contain details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to Rutherford's work.

159. Upstream surveillance undermines Rutherford's ability to conduct its work. Rutherford's advocacy depends on its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, Rutherford in some instances avoids sensitive topics or forgoes communications altogether. Rutherford believes that Upstream surveillance reduces the likelihood that victims of human rights abuses, witnesses, foreign government officials, and other contacts will share sensitive information with Rutherford, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

The Washington Office on Latin America

160. WOLA is a non-profit, non-governmental organization based in Washington D.C. WOLA works to advance human rights and social justice in the Americas. WOLA is regularly called upon for its research and analysis by policymakers, the media, and academics in the U.S. and Latin America. To further this work, WOLA gathers and publishes information about U.S. policies concerning Latin America, U.S. assistance (military or otherwise) to Latin American countries, and U.S. immigration practices, among other things.

161. WOLA engages in international and domestic internet communications that are essential to its mission. Among other things, WOLA's U.S.-based staff routinely engage in sensitive and confidential internet communications with non-U.S. persons located abroad in carrying out WOLA's research, policy, and advocacy work.

162. WOLA's communications are intercepted, copied, and reviewed in the course of Upstream surveillance. This surveillance invades the privacy of WOLA's communications and it violates WOLA's right to control those communications and the information they contain.

163. Furthermore, there is a substantial likelihood that the NSA retains, reads, and disseminates WOLA's international communications because WOLA is communicating with or about persons the government has targeted for Upstream surveillance. For instance, WOLA communicates with foreign government officials located abroad—including at times presidents and foreign ministers. Similarly, it communicates with policymakers, academics, journalists, human rights defenders, victims of human rights abuses, and staff from multilateral institutions, such as the Organization of American States, the Inter-American Development Bank, and the United Nations, some of whom are also likely targets. WOLA's communications with these contacts frequently concern topics that fall within the FAA's expansive definition of "foreign intelligence information." WOLA communicates both with and about these likely targets. WOLA's international communications contain, among other things, details about its foreign contacts and other important sources of information—details such as the email addresses, phone numbers, and website addresses of foreign individuals and organizations relevant to WOLA's work.

164. Upstream surveillance undermines WOLA's ability to conduct its work. WOLA's research and advocacy depend on the confidentiality of its communications, including its ability to assure its contacts that their communications—and, in some cases, even their identities—will not be revealed. Due in part to NSA surveillance, including Upstream surveillance, WOLA has undertaken burdensome and costly measures to secure and protect its communications, including adopting more secure methods of electronic communication,

traveling to conduct in-person meetings, and in some instances avoiding sensitive topics or forgoing communications altogether. Despite these precautions, WOLA believes that Upstream surveillance reduces the likelihood that policymakers, foreign government officials, experts, witnesses, and victims of human rights abuses will share sensitive information with WOLA's staff, because they fear that their communications will be intercepted by the U.S. government and also shared with the other governments, intelligence services, and organizations with which the U.S. government cooperates.

## CAUSES OF ACTION

165. Upstream surveillance exceeds the authority granted by 50 U.S.C. § 1881a, and therefore violates 5 U.S.C. § 706.

166. Upstream surveillance violates the Fourth Amendment to the Constitution.

167. Upstream surveillance violates the First Amendment to the Constitution.

168. Upstream surveillance violates Article III of the Constitution.

## PRAYER FOR RELIEF

WHEREFORE Plaintiffs respectfully request that the Court:

1. Exercise jurisdiction over Plaintiffs' Complaint;

2. Declare that Upstream surveillance violates 50 U.S.C. § 1881a and 5 U.S.C. § 706;

3. Declare that Upstream surveillance is unconstitutional under the First and Fourth Amendments, and under Article III;

4. Permanently enjoin Defendants from continuing Upstream surveillance;

5. Order Defendants to purge all records of Plaintiffs' communications in their possession obtained pursuant to Upstream surveillance;

6. Award Plaintiffs fees and costs pursuant to 28 U.S.C. § 2412;

7. Grant such other and further relief as the Court deems just and proper.

Dated: June 19, 2015
Baltimore, Maryland

Respectfully submitted,

*/s/ Deborah A. Jeon*

Deborah A. Jeon
(Bar No. 06905)
jeon@aclu-md.org
David R. Rocah
(Bar No. 27315)
rocah@aclu-md.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838

*/s/ Patrick Toomey*

Patrick Toomey
(pro hac vice)
ptoomey@aclu.org
(*signed by Patrick Toomey with permission of Debbie A. Jeon*)
Jameel Jaffer
(pro hac vice)
jjaffer@aclu.org
Alex Abdo
(pro hac vice)
aabdo@aclu.org
Ashley Gorski
(pro hac vice)
agorski@aclu.org
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654

Charles S. Sims
(pro hac vice)

csims@proskauer.com
David A. Munkittrick
(pro hac vice)
dmunkittrick@proskauer.com
John M. Browning
(pro hac vice)
jbrowning@proskauer.com
PROSKAUER ROSE LLP
Eleven Times Square
New York, NY 10036
Phone: (212) 969-3000
Fax: (212) 969-2900

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

WIKIMEDIA FOUNDATION,

*Plaintiff*,

v.

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

*Defendants*.

Hon. T. S. Ellis, III

Civil Action No.
15-cv-00662-TSE

**DECLARATION OF PATRICK TOOMEY IN SUPPORT OF PLAINTIFF WIKIMEDIA FOUNDATION'S MOTION TO COMPEL**

I, Patrick Toomey, a member of the Bar of the State of New York and admitted *pro hac vice* to the Bar of this Court, declare under penalty of perjury as follows:

1. I am an attorney with the American Civil Liberties Union Foundation, and represent Plaintiff Wikimedia Foundation ("Wikimedia") in this matter. I submit this declaration in support of Plaintiff's Motion to Compel.

2. Attached hereto as **Exhibit 1** is a chart identifying Plaintiff's Requests for Admission, Interrogatories, and Requests for Production, as modified by Wikimedia following the parties' meet-and-confer discussions, that are at issue in this Motion to Compel.

3. Attached hereto as **Exhibit 2** is a true and correct copy of Plaintiff's First Set of Requests for Admission.

4. Attached hereto as **Exhibit 3** is a true and correct copy of Plaintiff's Second Set of Requests for Admission.

5. Attached hereto as **Exhibit 4** is a true and correct copy of Plaintiff's Third Set of Requests for Admission.

6. Attached hereto as **Exhibit 5** is true and correct copy of Plaintiff's First Set of Interrogatories.

7. Attached hereto as **Exhibit 6** is a true and correct copy of Plaintiff's Second Set of Interrogatories.

8. Attached hereto as **Exhibit 7** is a true and correct copy of Plaintiff's First Set of Requests for Production.

9. Attached hereto as **Exhibit 8** is a true and correct copy of Plaintiff's Second Set of Requests for Production.

10. Attached hereto as **Exhibit 9** is a true and correct copy of Defendant National Security Agency's ("NSA") Objections and Responses to Plaintiff's First and Second Sets of Requests for Admission.

11. Attached hereto as **Exhibit 10** is a true and correct copy of Defendant NSA's Objections to Plaintiff's Third Set of Requests for Admission.

12. Attached hereto as **Exhibit 11** is a true and correct copy of Defendant NSA's Objections and Responses to Plaintiff's First Set of Interrogatories.

13. Attached hereto as **Exhibit 12** is a true and correct copy of Defendant NSA's Objections to Plaintiff's Second Set of Interrogatories.

14. Attached hereto as **Exhibit 13** is a true and correct copy of Defendant NSA's Objections and Responses to Plaintiff's First and Second Sets of Requests for Production.

15. Attached hereto as **Exhibit 14** is a true and correct copy of Defendant Department of Justice's ("DOJ") Objections and Responses to Plaintiff's First and Second Sets of Requests for Admission.

16. Attached hereto as **Exhibit 15** is a true and correct copy of Defendant DOJ's Objections and Responses to Plaintiff's First Set of Interrogatories.

17. Attached hereto as **Exhibit 16** is a true and correct copy of Defendant DOJ's Objections and Responses to Plaintiff's First and Second Sets of Requests for Production.

18. Attached hereto as **Exhibit 17** is a true and correct copy of Defendant Office of the Director of National Intelligence's ("ODNI") Objections and Responses to Plaintiff's First and Second Sets of Requests for Admission.

19. Attached hereto as **Exhibit 18** is a true and correct copy of Defendant ODNI's Objections and Responses to Plaintiff's First Set of Interrogatories.

20. Attached hereto as **Exhibit 19** is a true and correct copy of Defendant ODNI's Revised Objections and Responses to Plaintiff's First and Second Sets of Requests for Production.

21. Attached hereto as **Exhibit 20** is a true and correct copy of Defendant NSA's Privilege Log.

22. Attached hereto as **Exhibit 21** is a true and correct copy of Defendant DOJ's Privilege Log.

23. Attached hereto as **Exhibit 22** is a true and correct copy of Defendant ODNI's Privilege Log.

24. Attached hereto as **Exhibit 23** is a true and correct copy of Plaintiff's Notice of Deposition Pursuant to Federal Rule of Civil Procedure 30(b)(6).

25. Attached hereto as **Exhibit 24** is a true and correct copy of a letter from James Gilligan, counsel for Defendant NSA, to Patrick Toomey, counsel for Plaintiff Wikimedia, regarding Defendant NSA's objections to Plaintiff's notice of deposition pursuant to Federal Rule of Civil Procedure 30(b)(6), dated March 22, 2018.

26. Attached hereto as **Exhibit 25** is a true and correct copy of a redacted FISC submission titled "Government's Response to the Court's Briefing Order of May 9, 2011," dated June 1, 2011, and labeled with Bates numbers NSA-WIKI 00234–77 ("June 1, 2011 FISC Submission"). It is available at: https://www.dni.gov/files/documents/icotr/NYT/Government's%20Response%20to%20May%209,%202011%20Briefing%20Order%20(June%201,%202011).pdf.

27. Attached hereto as **Exhibit 26** is a true and correct copy of a redacted FISC submission titled "Government's Response to the Court's Follow-Up Questions of June 17, 2011," dated June 28, 2011, and publicly released pursuant to the Freedom of Information Act ("June 28, 2011 FISC Submission"). It is available at: https://www.documentcloud.org/documents/4064819-Savage-NYT-FOIA-2011-Bates-MCT-third-tranche.html#document/p176.[1]

28. Attached hereto as **Exhibit 27** is a true and correct copy of a redacted FISC Memorandum Opinion, dated October 3, 2011, and labeled with Bates numbers NSA-WIKI 00149–229. It is available at: https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

29. Attached hereto as **Exhibit 28** is a true and correct copy of a redacted FISC Memorandum Opinion, dated September 20, 2012, and publicly released pursuant to the

[1] Although Defendants have stated that FISC opinions and FISC submissions released via FOIA are readily accessible at "various locations" on Defendant ODNI's public website, *see, e.g.*, NSA Resp. to Pl. Requests for Production No. 21, Plaintiff has been unable to locate a functioning web-link to this document and others on ODNI's website.

Freedom of Information Act. It is available at: https://www.aclu.org/sites/default/files/field_document/fisc-opinion-and-order-re-1809-dated09.20.2012-ocrd_2.pdf.

30. Attached hereto as **Exhibit 29** is a true and correct copy of a redacted FISC Memorandum Opinion and Order, dated April 26, 2017. It is available at: https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

31. Attached hereto as **Exhibit 30** is a true and correct copy of a document titled "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended," dated July 25, 2014. It is available at: https://www.dni.gov/files/documents/icotr/702/Bates%20365-373.pdf .

* * *

I declare under penalty of perjury that the foregoing is true and correct.

Patrick Toomey

Date: March 26, 2018
New York, New York

# Exhibit 1

***Wikimedia Foundation v. National Security Agency, et. al.***
No. 15-cv-00662-TSE

**Plaintiff Wikimedia's Discovery Requests at Issue, as Narrowed by Plaintiff**

**DEFINITIONS**

Notwithstanding any definition set forth below, each word, term, or phrase used in [each] Request is intended to have the broadest meaning permitted under the Federal Rules of Civil Procedure. As used in [each] Request, the following terms are to be interpreted in accordance with these definitions:

*Answer*: The term "ANSWER" means Defendants' Answer to Plaintiff's First Amended Complaint in this action, filed on October 16, 2017.

*Bulk*: To COPY or REVIEW INTERNET COMMUNICATIONS in "BULK" means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

*Circuit*: The term "CIRCUIT" has the ordinary meaning of that term within the telecommunications industry as understood by YOU in the context of Upstream surveillance.

*Communication*: The term "COMMUNICATION" means information transmitted by any means, whether orally, electronically, by document, or otherwise.

*Concern or Concerning*: The terms "CONCERN" and "CONCERNING" mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

*Copy*: The term "COPY" means to duplicate a piece of data (for any duration, no matter how brief).

*Describe*: The term "DESCRIBE" means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events, agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

*Document*: The term "DOCUMENT" shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way to a requested document. A draft or non-identical copy is a separate document within the meaning of the term "DOCUMENT."

*Identify (with respect to PERSONS)*: When referring to a PERSON, to "IDENTIFY" means to state the PERSON's full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

*Identify (with respect to documents)*: When referring to documents, to "IDENTIFY" means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

*Interacted With* **[as modified]**: The term "INTERACTED WITH" means to have used a device to COPY, filter, or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication or transaction in the ordinary course of its transmission or storage.

*International Communication*: The term "INTERNATIONAL COMMUNICATION" means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

*Internet Backbone*: The term "INTERNET BACKBONE" means the set of high capacity cables, switches, and routers that facilitates both domestic and international Internet communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

*Internet Communication*: The term "INTERNET COMMUNICATION" means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

*Internet Packet*: The term "INTERNET PACKET" means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol ("IP") address and some payload.

*Internet Transaction*: The term "INTERNET TRANSACTION" has the same meaning as "Internet transaction" within the PCLOB Report at pages 39 and 125 and note 517.

*NSA*: The terms "National Security Agency" and "NSA" include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA's direction.

*Parties*: The terms "PLAINTIFF" and "DEFENDANT," as well as a party's full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors,

employees, agents, representatives, attorneys, consultants, and contractors. This definition is not intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court's jurisdiction to enter any appropriate order.

*Person*: The term "PERSON" is defined as any natural person or any business, legal or governmental entity, or association.

*Process*: The term "PROCESS" has the same meaning as "process," "process[ed]," or "process[ing]" within the July 2014 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, *available at* https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf ("2014 NSA Minimization Procedures").

*Retain*: The term "RETAIN" has the same meaning as "retain," "retained," or "retention" within the 2014 NSA Minimization Procedures.

*Review* **[as modified]**: The term "REVIEW" means to examine, scan, screen, monitor, analyze, or gather information about the contents of.

*Selector*: The term "SELECTOR" has the same meaning as "selector" within the 2014 NSA Minimization Procedures.

*Target*: The term "TARGET" means the subjects who are "targeted" pursuant to 50 U.S.C. § 1881a.

*United States*: When used as a term of geographic location, "UNITED STATES" means all areas under the territorial sovereignty of the United States.

*Wholly Domestic Communication*: The term "WHOLLY DOMESTIC COMMUNICATION" means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

*You/Your*: The terms "YOU" or "YOUR" include the defendant agency, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. "All" means "any and all"; "any" means "any and all." "Including" means "including but not limited to." "And" and "or" encompass both "and" and "or." Words in the masculine, feminine, or neutral form shall include each of the other genders.

**REQUESTS AT ISSUE**

| No. | Request | Modified Request |
|---|---|---|
| **Requests for Admission** | | |
| **RFA 6** | Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are in transit on the INTERNET BACKBONE, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR. | |
| **RFA 7** | Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE. | |
| **RFA 8** | Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE. | |
| **RFA 9** | Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR. | |
| **RFA 10** | Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR. | |

| No. | Request | Modified Request |
|---|---|---|
| **RFA 13** | Admit that the NSA conducts Upstream surveillance on multiple INTERNET BACKBONE CIRCUITS. | |
| **RFA 14** | Admit that the NSA conducts Upstream surveillance on multiple "international Internet link[s]," as that term is used by the government in its submission to the Foreign Intelligence Surveillance Court, titled "Government's Response to the Court's Briefing Order of May 9, 2011," and filed on June 1, 2011, *see* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). | Admit that the NSA conducts Upstream surveillance on multiple "international Internet link[s]," as that term is used by the Foreign Intelligence Surveillance Court in describing Upstream surveillance, *see* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). |
| **RFA 15** | Admit that the NSA conducts Upstream surveillance at multiple INTERNET BACKBONE "chokepoints" or "choke points" (as that term is used by YOU). | Admit that the NSA conducts Upstream surveillance at multiple INTERNET BACKBONE "chokepoints" or "choke points." |
| **RFA 16** | Admit that the document attached hereto as Exhibit A, titled "Why are we interested in HTTP?," is a true and correct excerpted copy of a genuine document. | Admit that the document attached hereto as Exhibit A, titled "Why are we interested in HTTP?," is a true and correct excerpted copy of a genuine NSA document. |
| **RFA 17** | Admit that the statements within the document attached hereto as Exhibit A were made by YOUR employees on matters within the scope of their employment during the course of their employment. | |
| **RFA 18** | Admit that statements within the document attached hereto as Exhibit A were made by persons YOU authorized to make statements on the subjects of the statements within the document. | |
| **RFA 19** | Admit that the document attached hereto as Exhibit B, titled "Fingerprints and Appids," and "Fingerprints and Appids (more)," is a true and correct excerpted copy of a genuine document. | Admit that the document attached hereto as Exhibit B, titled "Fingerprints and Appids," and "Fingerprints and Appids (more)," is a true and correct excerpted copy of a genuine NSA document. |

| No. | Request | Modified Request |
|---|---|---|
| **RFA 20** | Admit that the statements within the document attached hereto as Exhibit B were made by YOUR employees on matters within the scope of their employment during the course of their employment. | |
| **RFA 21** | Admit that statements within the document attached hereto as Exhibit B were made by persons YOU authorized to make statements on the subjects of the statements within the document. | |
| **RFA 25** | Admit that the document attached hereto as Exhibit D, titled "SSO's Support to the FBI for Implementation of their Cyber FISA Orders," is a true and correct copy of a genuine document. | Admit that the document attached hereto as Exhibit D, titled "SSO's Support to the FBI for Implementation of their Cyber FISA Orders," is a true and correct copy of a genuine NSA document. |
| **RFA 26** | Admit that the statements within the document attached hereto as Exhibit D were made by YOUR employees on matters within the scope of their employment during the course of their employment. | |
| **RFA 27** | Admit that statements within the document attached hereto as Exhibit D were made by persons YOU authorized to make statements on the subjects of the statements within the document. | |
| **RFA 28** | Admit that the document attached hereto as Exhibit E, titled "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" and dated July 28, 2009 (the "NSA Targeting Procedures") is a true and correct copy of a genuine document. | Admit that the document attached hereto as Exhibit E, titled "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" and dated July 28, 2009 (the "NSA Targeting Procedures") is a true and correct copy of a genuine DOJ document. |

| No. | Request | Modified Request |
|---|---|---|
| **RFA 29** | Admit that the statements within the document attached hereto as Exhibit E were made by YOUR employees on matters within the scope of their employment during the course of their employment. | |
| **RFA 30** | Admit that statements within the document attached hereto as Exhibit E were made by persons YOU authorized to make statements on the subjects of the statements within the document. | |
| **RFA 34** | Admit that, in conducting Upstream surveillance, the NSA has COPIED at least one WIKIMEDIA INTERNET COMMUNICATION. | |
| **RFA 35** | Admit that, in conducting Upstream surveillance, the NSA has REVIEWED the content of at least one WIKIMEDIA INTERNET COMMUNICATION. | |
| **RFA 36** | Admit that, in conducting Upstream surveillance, the NSA has RETAINED at least one WIKIMEDIA INTERNET COMMUNICATION. | |
| **RFA 37** | Admit that, in conducting Upstream surveillance on or before June 22, 2015, the NSA screened the contents of Internet web traffic (that is, the application layer of HTTP and HTTPS communications). | |
| **RFA 38** | Admit that, in conducting Upstream surveillance as of the date of the service of this request, the NSA screens the contents of Internet web traffic (that is, the application layer of HTTP and HTTPS communications). | |

| No. | Request | Modified Request |
|---|---|---|
| **RFA 39** | Admit that the document attached hereto as Exhibit A, which describes the monitoring of hundreds of CIRCUITS at one international cable site, is a true and correct excerpted copy of a genuine NSA document. | |
| **RFA 40** | If YOU contend, for the purpose of contesting jurisdiction in this matter, that encryption bears in any way on the interception, accessing, COPYING, filtering, REVIEWING, ingestion, or RETENTION of WIKIMEDIA'S COMMUNICATIONS in the course of Upstream surveillance, admit that YOU have the ability to decrypt, decipher, or render intelligible the contents of some HTTPS communications subject to Upstream surveillance. | |
| **Interrogatories** | | |
| **ROG 1** | DESCRIBE YOUR understanding of the definition of the term "international Internet link" as used by the government in its submission to the Foreign Intelligence Surveillance Court— titled "Government's Response to the Court's Briefing Order of May 9, 2011," and filed on June 1, 2011, *see [Redacted]*, 2011 WL 10945618, at *15 (FISC Oct. 3, 2011)—and provide all information supporting that understanding. | DESCRIBE YOUR understanding of the definition of the term "international Internet link" as used by the Foreign Intelligence Surveillance Court in describing Upstream surveillance, *see [Redacted]*, 2011 WL 10945618, at *15 (FISC Oct. 3, 2011), and provide all information supporting that understanding. |

| No. | Request | Modified Request |
|---|---|---|
| **ROG 2** | DESCRIBE YOUR understanding of the definition of the term "circuit" as used at pages 36 to 37 of the PCLOB Report, and provide all information supporting that understanding, including but not limited to all information furnished by DEFENDANTS to the Privacy and Civil Liberties Oversight Board concerning this term. | |
| **ROG 3** | DESCRIBE YOUR understanding of the definition of the term "filtering mechanism" as used at pages 10 and 47–48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding. | |
| **ROG 4** | DESCRIBE YOUR understanding of the definition of the term "scanned" as used at page 10 of the Memorandum in Support of Defendants' Motion to Dismiss the First Amended Complaint, *Wikimedia Foundation v. NSA*, No. 15-cv-662-TSE (D. Md. Aug. 6, 2015), and provide all information supporting that understanding. | |
| **ROG 5** | DESCRIBE YOUR understanding of the definition of the term "screen" as used at page 48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding. | |
| **ROG 6** | DESCRIBE YOUR understanding of the definition of the term "discrete communication" as used in the 2014 NSA Minimization Procedures, and provide all information supporting that understanding. | |

| No. | Request | Modified Request |
|---|---|---|
| **ROG 7** | DESCRIBE YOUR understanding of all features that a series of INTERNET PACKETS comprising an "Internet transaction" has in common, as the term "Internet transaction" is used in at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding. For example, the INTERNET PACKETS comprising an "Internet transaction" might share source and destination IP addresses, source and destination ports, and protocol type (albeit with the source and destination IP addresses and ports reversed for packets flowing in the opposite direction). | |
| **ROG 8** | DESCRIBE YOUR understanding of the definitions of the terms "single communication transaction" and "multi-communication transaction" as used by the government in its submission to the Foreign Intelligence Surveillance Court, filed on August 16, 2011, and provide all information supporting that understanding. *See* [*Redacted*], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011). | |
| **ROG 9** | DESCRIBE YOUR understanding of the definitions of the terms "access" and "larger body of international communications" as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding. | |

| No. | Request | Modified Request |
|---|---|---|
| **ROG 14** | DESCRIBE the entire process by which, pursuant to Upstream surveillance, the contents of INTERNET COMMUNICATIONS are INTERACTED WITH. | |
| **ROG 15** | DESCRIBE any and all statements or facts YOU contend are inaccurate concerning Upstream surveillance in pages 7-10, 22, 32-33, 35-41 & n.157, 79, 111 n.476, 119-26, and 143-45 of the Privacy and Civil Liberties Oversight Board's *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), based on Upstream surveillance as it was conducted on the date the report was publicly released. | |
| **ROG 16** | DESCRIBE the approximate percentage of CIRCUITS carrying Internet communications into or out of the United States (not CIRCUITS carrying solely telephonic or private network communications) that were monitored in the course of Upstream surveillance in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available. | |

| No. | Request | Modified Request |
|---|---|---|
| **ROG 17** | DESCRIBE the approximate percentage of international submarine cables carrying Internet communications into or out of the United States (not international submarine cables carrying solely telephonic or private network communications) that were monitored in the course of Upstream surveillance in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available. | |
| **ROG 18** | DESCRIBE, by any metric commonly used in the telecommunications industry, such as bytes or packets, the approximate amount of Internet traffic that was subject to filtering in the course of Upstream surveillance, prior to retaining Internet communications that contain a selector, in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available. | |
| **ROG 19** | DESCRIBE, by any metric commonly used in the telecommunications industry, such as bytes or packets, the approximate amount of Internet traffic that was screened in the course of Upstream surveillance, prior to retaining Internet communications that contain a selector, in each of the years 2015, 2016, and 2017. If insufficient information is available for these three years, please provide sufficient information for the three most recent years available. | |

| No. | Request | Modified Request |
|---|---|---|
| **ROG 20** | If YOU contend, for the purpose of contesting jurisdiction in this matter, that encryption bears in any way on the interception, accessing, COPYING, filtering, REVIEWING, ingestion, or RETENTION of WIKIMEDIA'S COMMUNICATIONS in the course of Upstream surveillance, DESCRIBE the protocols used to encrypt INTERNET COMMUNICATIONS or INTERNET TRANSACTIONS subject to Upstream surveillance for which the NSA has the ability to decrypt, decipher, or render intelligible the contents of those COMMUNICATIONS. | |
| **Requests for Production** | | |
| **RFP 10** | DOCUMENTS sufficient to show or estimate the number of INTERNET COMMUNICATIONS and/or INTERNET TRANSACTIONS RETAINED using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017. | |
| **RFP 13** | DOCUMENTS sufficient to show or estimate the number of CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017. | |
| **RFP 14** | DOCUMENTS sufficient to show or estimate the combined bandwidth of the CIRCUITS on which the NSA conducted Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017. | |

| No. | Request | Modified Request |
|---|---|---|
| **RFP 15** | DOCUMENTS sufficient to show or estimate the number of "international Internet link[s]"— as that term was used by the government in its submission to the Foreign Intelligence Surveillance Court, titled "Government's Response to the Court's Briefing Order of May 9, 2011," and filed on June 1, 2011, *see [Redacted]*, 2011 WL10945618, at *15 (FISC Oct. 3, 2011)—monitored using Upstream surveillance in each of the years 2010, 2011, 2012, 2013, 2014, 2015, 2016, and the first six months of 2017. | |
| **RFP 16** | DOCUMENTS sufficient to show or estimate the number of Internet "chokepoints" or "choke points" (as that term is used by YOU) inside the UNITED STATES through which INTERNATIONAL COMMUNICATIONS enter and leave the UNITED STATES and where the NSA has established Upstream surveillance collection or PROCESSING capabilities. | |
| **RFP 18** | All Foreign Intelligence Surveillance Court–approved targeting procedures relevant at any time to DEFENDANTS' implementation of Upstream surveillance. | Foreign Intelligence Surveillance Court-approved targeting procedures relevant to DEFENDANTS' implementation of Upstream surveillance in 2009, 2015, 2016, and 2017. |

| No. | Request | Modified Request |
|---|---|---|
| **RFP 21** | All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court orders and opinions CONCERNING Upstream surveillance. | All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court orders and opinions CONCERNING Upstream surveillance that:<br>a. Describe the ways in which the NSA intercepts, COPIES, filters, or REVIEWS INTERNET COMMUNICATIONS or INTERNET TRANSACTIONS in the course of Upstream surveillance in order to identify COMMUNICATIONS associated with its SELECTORS;<br>b. Describe the points or places at which Upstream surveillance is conducted in relation to the Internet backbone and its components, including but not limited to CIRCUITS, links, or chokepoints; or<br>c. Describe the types or categories of INTERNET COMMUNICATIONS subject to Upstream surveillance, including but not limited to COMMUNICATIONS associated with web activity or email. |

| No. | Request | Modified Request |
|---|---|---|
| **RFP 22** | All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court submissions CONCERNING Upstream surveillance. | All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court submissions CONCERNING Upstream surveillance that:<br>a. Describe the ways in which the NSA intercepts, COPIES, filters, or REVIEWS INTERNET COMMUNICATIONS or INTERNET TRANSACTIONS in the course of Upstream surveillance in order to identify COMMUNICATIONS associated with its SELECTORS;<br>b. Describe the points or places at which Upstream surveillance is conducted in relation to the Internet backbone and its components, including but not limited to CIRCUITS, links, or chokepoints; or<br>c. Describe the types or categories of INTERNET COMMUNICATIONS subject to Upstream surveillance, including but not limited to COMMUNICATIONS associated with web activity or email. |
| **RFP 23** | Any INTERNET COMMUNICATION of WIKIMEDIA that any DEFENDANT INTERACTED WITH in connection with Upstream surveillance. | |
| **RFP 24** | All DOCUMENTS CONCERNING any INTERACTION WITH the INTERNET COMMUNICATIONS of WIKIMEDIA in connection with Upstream surveillance. | |

# Exhibit 2

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | | |
|---|---|---|
| **WIKIMEDIA FOUNDATION,** | * | |
| **Plaintiff,** | * | |
| **v.** | * | **Civil Action No.: 15-cv-00662-TSE** |
| **NATIONAL SECURITY AGENCY, *et al.*,** | * | |
| **Defendants.** | * | |

* * * * * * * * * * *

## REQUESTS FOR ADMISSION

Pursuant to Federal Rule of Civil Procedure 36, Local Rule 104, and Appendix A to the Local Rules, the Wikimedia Foundation ("WIKIMEDIA" or "PLAINTIFF"), by its undersigned attorneys, serves these Requests for Admission on defendants National Security Agency ("NSA"); the Office of the Director of National Intelligence ("ODNI"); the United States Department of Justice ("DOJ"); Admiral Michael S. Rogers, in his official capacity as the Director of the NSA; Daniel Coats, in his official capacity as the Director of National Intelligence ("DNI"); and Jefferson B. Sessions, III, in his official capacity as Attorney General (collectively, the "DEFENDANTS"), and demands that DEFENDANTS answer each Request for Admission herein in writing and under oath and within thirty (30) days of the date of service of the Requests for Admission, in accordance with the Definitions and Instructions set forth below.

## DEFINITIONS

Notwithstanding any definition set forth below, each word, term, or phrase used in this Request is intended to have the broadest meaning permitted under the Federal Rules of Civil

Procedure. As used in this Request, the following terms are to be interpreted in accordance with these definitions:

*Answer:* The term "ANSWER" means Defendants' Answer to Plaintiff's First Amended Complaint in this action, filed on October 16, 2017.

*Bulk:* To COPY or REVIEW INTERNET COMMUNICATIONS in "BULK" means to COPY or REVIEW INTERNET COMMUNICATIONS in large quantity without prior application of SELECTORS, or other identifiers associated with specific targets of Upstream surveillance.

*Circuit:* The term "CIRCUIT" has the same meaning as "circuit" in the Privacy and Civil Liberties Oversight Board's "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," dated July 2, 2014 ("PCLOB Report"), at pages 36 to 37.

*Communication:* The term "COMMUNICATION" means information transmitted by any means, whether orally, electronically, by document, or otherwise.

*Concern or Concerning:* The terms "CONCERN" and "CONCERNING" mean relating to, referring to, describing, evidencing, constituting, reflecting, memorializing, identifying, embodying, pertaining to, commenting on, discussing, analyzing, considering, containing, consisting of, indicating, supporting, refuting, or connected to.

*Copy:* The term "COPY" means to duplicate a piece of data (for any duration, no matter how brief).

*Describe:* The term "DESCRIBE" means to provide a narrative statement or description of the specific facts or matters to which an Interrogatory refers, including, but not limited to, an identification of all persons, communications, acts, transactions, events,

agreements, recommendations, and DOCUMENTS used, necessary, or desirable to support such statement or make the description complete.

*Document:* The term "DOCUMENT" shall have the broadest meaning ascribed to that term in Federal Rule of Civil Procedure 34 and Federal Rule of Evidence 1001. The term also includes any parent or child attachment or other documents embedded or linked in any way to a requested document. A draft or non-identical copy is a separate document within the meaning of the term "DOCUMENT."

*Identify (with respect to PERSONS):* When referring to a PERSON, to "IDENTIFY" means to state the PERSON's full name, present or last known address, and, when referring to a natural person, the present or last known place of employment. If the business and home telephone numbers are known to the answering party, and if the PERSON is not a party or present employee of a party, said telephone numbers shall be provided. Once a PERSON has been identified in accordance with this subparagraph, only the name of the PERSON need be listed in response to subsequent discovery requesting the identification of that PERSON.

*Identify (with respect to documents):* When referring to documents, to "IDENTIFY" means to state the: (i) type of document; (ii) general subject matter; (iii) date of the document; and (iv) author(s), addressee(s), and recipient(s); or, alternatively, to produce the document.

*Interacted with:* "INTERACTED WITH" means to have used a device to COPY or REVIEW an INTERNET COMMUNICATION or INTERNET TRANSACTION while such communication or transaction is being transmitted or while the communication or transaction is being stored, other than as necessary to transmit or store the communication.

*International Communication:* The term "INTERNATIONAL COMMUNICATION" means an INTERNET COMMUNICATION between at least one party in the UNITED STATES and at least one party outside the UNITED STATES.

*Internet Backbone:* The term "INTERNET BACKBONE" means the set of high-capacity cables, switches, and routers that facilitates both domestic and international Internet communication by parties connected to it. The INTERNET BACKBONE includes, but is not limited to, the international submarine cables that carry INTERNET COMMUNICATIONS.

*Internet Communication:* The term "INTERNET COMMUNICATION" means a series of related packets that are sent from a particular source to a particular destination that together constitute a message of some sort, including but not limited to an email message, an HTTP request, or an HTTP response.

*Internet Packet:* The term "INTERNET PACKET" means a discrete chunk of information transmitted across the Internet. All INTERNET COMMUNICATIONS are split into one or more INTERNET PACKETS. Each INTERNET PACKET contains a source and destination Internet Protocol ("IP") address and some payload.

*Internet Transaction:* The term "INTERNET TRANSACTION" has the same meaning as "Internet transaction" within the PCLOB Report at pages 39 and 125 and note 517.

*NSA:* The terms "National Security Agency" and "NSA" include any department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof, as well as telecommunication providers acting at the NSA's direction.

*Parties:* The terms "PLAINTIFF" and "DEFENDANT," as well as a party's full or abbreviated name or a pronoun referring to a party, mean that party and its officers, directors, employees, agents, representatives, attorneys, consultants, and contractors. This definition is not

intended to impose a discovery obligation on any PERSON who is not a party to the litigation or to limit the Court's jurisdiction to enter any appropriate order.

*Person*: The term "PERSON" is defined as any natural person or any business, legal or governmental entity, or association.

*Process:* The term "PROCESS" has the same meaning as "process," "process[ed]," or "process[ing]" within the July 2014 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, *available at* https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf ("2014 NSA Minimization Procedures").

*Retain:* The term "RETAIN" has the same meaning as "retain," "retained," or "retention" within the 2014 NSA Minimization Procedures.

*Review:* The term "REVIEW" means to scan, search, screen, capture, monitor, analyze, redirect, divert, or gather information about the contents of.

*Selector:* The term "SELECTOR" has the same meaning as "selector" within the 2014 NSA Minimization Procedures.

*Target:* The term "TARGET" means the subjects who are "targeted" pursuant to 50 U.S.C. § 1881a.

*United States:* When used as a term of geographic location, "UNITED STATES" means all areas under the territorial sovereignty of the United States.

*Wholly Domestic Communication:* The term "WHOLLY DOMESTIC COMMUNICATION" means an INTERNET COMMUNICATION whose origin and final destination are both located within the UNITED STATES.

*You/Your:* The terms "YOU" or "YOUR" include the defendant agency, and department, office, entity, officer, employee, agent, representative, attorney, consultant, or contractor thereof.

The present tense includes the past and future tenses. The singular includes the plural, and the plural includes the singular. "All" means "any and all"; "any" means "any and all." "Including" means "including but not limited to." "And" and "or" encompass both "and" and "or." Words in the masculine, feminine, or neutral form shall include each of the other genders.

## INSTRUCTIONS

1. YOU are requested to answer each Request for Admission set forth below separately and completely in writing under oath. In answering these Requests for Admission, respond truthfully and in good faith on the basis of all information that is known or readily obtainable by YOU.

2. As required by Federal Rule of Civil Procedure 36(a)(4), if good faith requires that YOU deny only a portion of any matter as to which an admission is requested, or that YOU qualify any response as to any given Request for Admission, specify and admit so much of the Request as is true and deny or qualify only that portion of the Request as to which good faith requires a denial or qualification.

3. Each Request for Admission shall be answered fully unless it is objected to in good faith, in which event the reasons for YOUR objection shall be stated in detail. If an objection pertains to only a portion of a Request for Admission, or a word, phrase, or clause contained within it, YOU are required to state YOUR objection to that portion only and to respond to the remainder of the Request for Admission, using YOUR best efforts to do so.

4. If YOU assert that any information responsive to any Request for Admission is privileged or otherwise protected from discovery, YOU are requested to expressly make a claim of privilege and to describe the nature of the information not disclosed, in a manner that, without revealing information itself privileged or protected, will enable PLAINTIFF to assess the claim of privilege. For any DOCUMENT or information withheld on the grounds that it is privileged or otherwise claimed to be excludable from discovery, identify the information or DOCUMENT, describe its subject matter and date, identify all authors and all recipients (including copied and blind copied recipients), and specify the basis for the claimed privilege or other grounds of exclusion.

5. YOUR responses to these Requests should be based upon information known to YOU CONCERNING facts or events that occurred, in whole or in part, as of June 22, 2015.

6. These Requests for Admission are continuing in nature and YOUR responses to them are to be promptly supplemented or amended if, after the time of YOUR initial responses, YOU learn that any response is or has become in some material respect incomplete or incorrect, to the full extent provided for by Federal Rule of Civil Procedure 26(e).

## REQUESTS FOR ADMISSION

**REQUEST FOR ADMISSION NO. 1:**

Admit that there are between 45 and 55 international submarine cables that carry INTERNET COMMUNICATIONS directly into or directly out of the UNITED STATES.

**REQUEST FOR ADMISSION NO. 2:**

Admit that the international submarine cables that carry INTERNET COMMUNICATIONS directly into or directly out of the UNITED STATES make landfall at approximately 40 to 45 different landing points within the UNITED STATES.

**REQUEST FOR ADMISSION NO. 3:**

Admit that the INTERNET BACKBONE includes international submarine cables that carry INTERNET COMMUNICATIONS into and out of the UNITED STATES.

**REQUEST FOR ADMISSION NO. 4:**

Admit that the INTERNET BACKBONE includes high-capacity terrestrial cables that carry traffic within the UNITED STATES.

**REQUEST FOR ADMISSION NO. 5:**

Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS that are in transit on the INTERNET BACKBONE, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

**REQUEST FOR ADMISSION NO. 6:**

Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are in transit on the INTERNET BACKBONE, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

**REQUEST FOR ADMISSION NO. 7:**

Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.

**REQUEST FOR ADMISSION NO. 8:**

Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS in BULK that are in transit on the INTERNET BACKBONE.

**REQUEST FOR ADMISSION NO. 9:**

Admit that, in conducting Upstream surveillance, the NSA COPIES INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

**REQUEST FOR ADMISSION NO. 10:**

Admit that, in conducting Upstream surveillance, the NSA REVIEWS the contents of INTERNET COMMUNICATIONS that are neither to nor from TARGETS, prior to RETAINING INTERNET COMMUNICATIONS that contain a SELECTOR.

**REQUEST FOR ADMISSION NO. 11:**

Admit that the NSA does not consider an INTERNET COMMUNICATION "collected," within the meaning of the 2014 NSA Minimization Procedures, until after it has REVIEWED the contents of the communication and has selected it for RETENTION.

**REQUEST FOR ADMISSION NO. 12:**

Admit that, in the course of Upstream surveillance, the NSA RETAINS WHOLLY DOMESTIC COMMUNICATIONS.

**REQUEST FOR ADMISSION NO. 13:**

Admit that the NSA conducts Upstream surveillance on multiple INTERNET BACKBONE CIRCUITS.

**REQUEST FOR ADMISSION NO. 14:**

Admit that the NSA conducts Upstream surveillance on multiple "international Internet link[s]," as that term is used by the government in its submission to the Foreign Intelligence Surveillance Court, titled "Government's Response to the Court's Briefing Order of May 9,

2011," and filed on June 1, 2011, *see* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011).

**REQUEST FOR ADMISSION NO. 15:**

Admit that the NSA conducts Upstream surveillance at multiple INTERNET BACKBONE "chokepoints" or "choke points" (as that term is used by YOU).

**REQUEST FOR ADMISSION NO. 16:**

Admit that the document attached hereto as Exhibit A, titled "Why are we interested in HTTP?," is a true and correct excerpted copy of a genuine document.

**REQUEST FOR ADMISSION NO. 17:**

Admit that the statements within the document attached hereto as Exhibit A were made by YOUR employees on matters within the scope of their employment during the course of their employment.

**REQUEST FOR ADMISSION NO. 18:**

Admit that statements within the document attached hereto as Exhibit A were made by persons YOU authorized to make statements on the subjects of the statements within the document.

**REQUEST FOR ADMISSION NO. 19:**

Admit that the document attached hereto as Exhibit B, titled "Fingerprints and Appids," and "Fingerprints and Appids (more)," is a true and correct excerpted copy of a genuine document.

**REQUEST FOR ADMISSION NO. 20:**

Admit that the statements within the document attached hereto as Exhibit B were made by YOUR employees on matters within the scope of their employment during the course of their employment.

**REQUEST FOR ADMISSION NO. 21:**

Admit that statements within the document attached hereto as Exhibit B were made by persons YOU authorized to make statements on the subjects of the statements within the document.

**REQUEST FOR ADMISSION NO. 22:**

Admit that the document attached hereto as Exhibit C, "Seven Access Sites—International 'Choke Points'," is a true and correct excerpted copy of a genuine document.

**REQUEST FOR ADMISSION NO. 23:**

Admit that the statements within the document attached hereto as Exhibit C were made by YOUR employees on matters within the scope of their employment during the course of their employment.

**REQUEST FOR ADMISSION NO. 24:**

Admit that statements within the document attached hereto as Exhibit C were made by persons YOU authorized to make statements on the subjects of the statements within the document.

**REQUEST FOR ADMISSION NO. 25:**

Admit that the document attached hereto as Exhibit D, titled "SSO's Support to the FBI for Implementation of their Cyber FISA Orders," is a true and correct copy of a genuine document.

**REQUEST FOR ADMISSION NO. 26:**

Admit that the statements within the document attached hereto as Exhibit D were made by YOUR employees on matters within the scope of their employment during the course of their employment.

**REQUEST FOR ADMISSION NO. 27:**

Admit that statements within the document attached hereto as Exhibit D were made by persons YOU authorized to make statements on the subjects of the statements within the document.

**REQUEST FOR ADMISSION NO. 28:**

Admit that the document attached hereto as Exhibit E, titled "Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" and dated July 28, 2009 (the "NSA Targeting Procedures") is a true and correct copy of a genuine document.

**REQUEST FOR ADMISSION NO. 29:**

Admit that the statements within the document attached hereto as Exhibit E were made by YOUR employees on matters within the scope of their employment during the course of their employment.

**REQUEST FOR ADMISSION NO. 30:**

Admit that statements within the document attached hereto as Exhibit E were made by persons YOU authorized to make statements on the subjects of the statements within the document.

**REQUEST FOR ADMISSION NO. 31:**

Admit that the document attached hereto as Exhibit F, titled "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," dated July 2014, and available at https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf, is a true and correct copy of a genuine document.

**REQUEST FOR ADMISSION NO. 32:**

Admit that the statements within the document attached hereto as Exhibit F were made by YOUR employees on matters within the scope of their employment during the course of their employment.

**REQUEST FOR ADMISSION NO. 33:**

Admit that statements within the document attached hereto as Exhibit F were made by persons YOU authorized to make statements on the subjects of the statements within the document.

Dated: November 7, 2017

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

*Counsel for Plaintiff*

# Exhibit A

# Why are we interested in HTTP?

facebook

YAHOO!

twitter

myspace.com
a place for friends

Because nearly everything a typical user does on the Internet uses HTTP

CNN.com

Google Earth

@mail.ru

WIKIPEDIA
The Free Encyclopedia

Gmail by Google BETA

# Exhibit B

# 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)

# 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

# Exhibit C

TOP SECRET // COMINT // NOFORN//20291130

# STORMBREW At a Glance




TOP SECRET // COMINT // NOFORN//20291130

# Exhibit D

SECRET//REL TO USA, FVEY

SECURITY CLASSIFICATION

# NSA STAFF PROCESSING FORM

| TO | EXREG CONTROL NUMBER | KCC CONTROL NUMBER |
|---|---|---|
| SIGINT DIR | 2012-704 | S353-113-11 |

| THRU | ACTION | EXREG SUSPENSE |
|---|---|---|
| | [X] APPROVAL | |
| SUBJECT | [ ] SIGNATURE | KCC SUSPENSE |
| (S//REL) SSO's Support to the FBI for Implementation of their Cyber FISA Orders | [ ] INFORMATION | ELEMENT SUSPENSE |

DISTRIBUTION
V2, V3, V07

SUMMARY

**RECOMMENDATION:** (U//FOUO) Approve the provision of the assistance to FBI, with the proviso that the FBI remains responsible for any additional expenses incurred.

**PURPOSE:** (S//REL) To obtain the SIGINT Director's approval for the Office of Special Source Operations (SSO) to provide ongoing technical assistance to the Federal Bureau of Investigation (FBI) for the implementation of the various orders they have obtained, and will obtain, from the Foreign Intelligence Surveillance Court (FISC) in certain Cyber cases involving agents of foreign powers (e.g. - [redacted] soon, [redacted]). The preparation of this Staff Processing Form was a collaborative effort between SSO and the NSA Office of General Counsel (OGC).

**BACKGROUND:** (S//REL) On December 20, 2011, NSA received a request for technical assistance from the FBI seeking access to infrastructure established by NSA for collection of foreign intelligence from U.S. telecommunications providers. The FISC has issued a number of orders at the request of the FBI authorizing electronic surveillance directed at communications related to computer intrusions being conducted by foreign powers. The orders include some that are limited to pen register/trap and trace (PRTT) information as well as others that authorize collection of content. The first of these for which NSA assistance has been requested is directed at communications related to intrusions conducted by the [redacted] (Docket Number 11-91), regarding what FBI refers to as STYGIAN FLOW.

(S//REL) In mid-2011, prior to receipt of the request for technical assistance, SSO became aware of FBI's plans to seek these orders and has been in discussions with FBI throughout the latter half of the year, in the belief that use of NSA's collection/processing infrastructure would allow the FBI to

Continued...

COORDINATION/APPROVAL

| OFFICE | NAME AND DATE | SECURE PHONE | OFFICE | NAME AND DATE | SECURE PHONE |
|---|---|---|---|---|---|
| OGC | [redacted] /email/ 30 Jan. | | | | |
| F1B | [redacted] /email/ 9 Feb. | | S3 | [redacted] /s/ 3-20-12 | |
| S1 | [redacted] /s/ | | S35 | [redacted] | |
| NTOC | [redacted] /s/ | | SV | [redacted] /s/ 31 Jan. | |
| T | [redacted] /s/ 6 Feb | | POC | [redacted] | [redacted] |

| ORIGINATOR | ORG. | PHONE (Secure) | DATE PREPARED |
|---|---|---|---|
| [redacted] Digitally signed by [redacted] DN: c=US, [redacted] ou=NSA, ou=D002, [redacted] Date: 2011.12.21 07:42:01 -05'00' | S353 | [redacted] | 20111221 |

FORM A6796DE REV NOV 2008(Supersedes A6796 FEB 05 which is obsolete)
NSN: 7540-FM-001-5465
Derived From: NSA/CSS Manual 1-52
Dated: 8 January 2007
Declassify On: 20320108

SECURITY CLASSIFICATION
SECRET//REL TO USA, FVEY

maximize the value of the collection without incurring the expenses associated with duplication of that infrastructure. Although FBI conducts numerous electronic surveillances without NSA's assistance, the vast majority of them are directed against targets located inside the United States, and U.S. providers served with FISC orders are ordinarily able to identify and deliver to the FBI most, if not all, of the targets' communications that they carry. That is because such electronic surveillance is typically effected at a point or points in the provider's infrastructure in physical proximity to the target's location. In the case of computer intrusions being conducted by foreign powers, the providers may be carrying a target's communications, but it is much more difficult to identify and locate them, because the communications in question will enter and leave the United States via any convenient path, and their path may be obscured to avoid detection. In other words, in these cases, because the target's location is outside the United Statues and not well-characterized, effecting the surveillance via FBI's traditional means is not effective.

(S//REL) However, in support of FAA and in anticipation of the need to conduct similar collection activities for computer network defense purposes, over the last decade, NSA has expended a significant amount of resources to create collection/processing capabilities at many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States. Collection at such chokepoints is much better suited to electronic surveillance directed at targets located outside the United States than FBI's traditional means of collection. In theory, FBI could rely on the orders it has obtained to direct U.S. providers to conduct surveillance at these chokepoints without relying on NSA capabilities, but it would take a considerable amount of time to do so, and FBI would have to reimburse the providers to recreate (i.e., duplicate) what NSA has already put in place. The cost alone would be prohibitive, and the time lost in doing so would necessarily result in a loss of foreign intelligence.

(S//REL) The assistance being sought by the FBI is limited in nature. The U.S. providers served with Secondary Orders in this matter will assume full responsibility for the provisioning of PR/TT and content collection to the FBI. Since all of the authorized "facilities" (typically known as "targeted selectors" in NSA parlance) to date are Internet Protocol (IP) addresses used by the targets, there is no question as to the providers' abilities to employ devices under their control (e.g., routers) to provision fully-compliant, authorized intercept.

(S//REL) Neither the providers nor the FBI will require NSA's Government off the Shelf (GOTS) Digital Network Intelligence (DNI) collection and processing solutions (e.g., TURMOIL, XKEYSCORE). Instead, metadata and full content derived from the authorized intercept will be produced using Commercial off the Shelf (COTS) processing solutions. If these COTS processing solutions involve components developed at NSA's expense and used, primarily, for NSA's Cyber survey purposes, the SSO will make careful and informed decisions prior to authorizing use of these components.

**Page 3 of 4: CATS 2012-704 (S//REL TO USA, FVEY) SSO's Support to the FBI for Implementation of their Cyber FISA Orders**

(S//REL) Prior to authorizing use of the extensive secure Wide Area Networks established at the two primary providers (cover terms, LITHIUM and ARTIFICE, respectively) as the end-to-end data delivery infrastructure to connect intercept and processing locations with the FBI's designated Cyber data repository at the Engineering Research Facility, Quantico, VA, SSO will make careful and informed decisions to ensure this capability is undertaken on a 100% non-interference basis with NSA's current and future data backhaul needs on these same networks.

(S//REL) All data (metadata and/or content) collected under the auspices of these FISC orders will be forwarded securely and directly to the designated FBI repository. The FISC orders do contain a provision, as follows: "NCIJTF personnel participating in this joint investigation may have access to raw data prior to minimization." However, access to raw data by NTOC members of the NCIJTF will be facilitated under the purview of the FBI and not through any actions that SSO might take as the collected data passes through NSA's secure Wide Area Networks. Should the FBI's cyber orders from the FISC be modified in the future to authorize raw data retention by NSA, SSO will coordinate with all cognizant NSA offices (e.g., Data Governance, OGC, SV) to ensure the proper data delivery mechanism is put in place.

(S//REL) Should the FBI require a sustained and high-level of dedicated analytical resources (i.e., cleared, technical manpower) at the providers in order to optimize the collection effectiveness of their PR/TT and content orders, they will contract for those services directly with the providers. If, on the other hand, the FBI's requirement for provider analytical support is more ad hoc and aperiodic in nature during the period of time these orders remain in effect, SSO will make careful and informed decisions prior to authorizing labor charges against the relevant SSO contracts with the providers for these services on behalf of the FBI. Any charges that cannot be justified as necessary for NSA purposes will not be made unless/until FBI agrees to reimburse NSA.

**DISCUSSION:** (S//REL) If SID decides to approve the requested assistance, SSO will assist the FBI in effecting any cyber orders submitted to it after the NSA/OGC has verified that each of them contains language permitting NSA's involvement. As stated in Attachment 1, NSA will have the opportunity to review and respond to any proposed use of FISA-derived information from these collections prior to the Attorney General authorizing the use of such information in any criminal proceedings.

(S//REL) The assistance SSO is being asked to provide to the FBI will not preclude NSA's SIGINT targeting of these same fully-qualified, overseas IP addresses under the auspices of the FISA

Continued...

(S//REL) The assistance SSO is being asked to provide to the FBI will not preclude NSA's SIGINT targeting of these same fully-qualified, overseas IP addresses under the auspices of the FISA Amendments Act (FAA) of 2008. To the contrary, the relatively recent discovery of these FBI Cyber FISA orders and the countless pages of SIGINT-derived evidence that was cited in the respective Applications to the FISC have already formed the basis for a dialog between NSA's OGC and the Department of Justice's National Security Division.

**(C) DIRECTOR, SIGNALS INTELLIGENCE DECISION:**

CONCUR: Teresa H. Shea DATE: 3-827-12

NON-CONCUR:_____ DATE:_____

# Exhibit E

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2009 JUL 29 PM 3:14

CLERK OF COURT

# EXHIBIT A

## PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED

(S) These procedures address: (I) the manner in which the National Security Agency/Central Security Service (NSA) will determine that a person targeted under section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended ("the Act"), is a non-United States person reasonably believed to be located outside the United States ("foreignness determination"); (II) the post-targeting analysis done by NSA to ensure that the targeting of such person does not intentionally target a person known at the time of acquisition to be located in the United States and does not result in 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; (III) the documentation of NSA's foreignness determination; (IV) compliance and oversight; and (V) departures from these procedures.

### I. (U) DETERMINATION OF WHETHER THE ACQUISITION TARGETS NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES

(S) NSA determines whether a person is a non-United States person reasonably believed to be outside the United States in light of the totality of the circumstances based on the information available with respect to that person, including information concerning the communications facility or facilities used by that person.

(S) NSA analysts examine the following three categories of information, as appropriate under the circumstances, to make the above determination: (1) they examine the lead information they have received regarding the potential target or the facility that has generated interest in conducting surveillance to determine what that lead information discloses about the person's location; (2) they conduct research in NSA databases, available reports and collateral information (i.e., information to which NSA has access but did not originate, such as reports from other agencies and publicly available information) to determine whether NSA knows the location of the person, or knows information that would provide evidence concerning that location; and (3) they conduct technical analyses of the facility or facilities to determine or verify information about the person's location. NSA may use information from any one or a combination of these categories of information in evaluating the totality of the circumstances to determine that the potential target is located outside the United States.

(TS//SI) In addition, in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

overseas, or it will target Internet links that terminate in a foreign country. In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.

**(S) Lead Information**

(S) When NSA proposes to direct surveillance at a target, it does so because NSA has already learned something about the target or the facility or facilities the target uses to communicate. Accordingly, NSA will examine the lead information to determine what it reveals about the physical location of the target, including the location of the facility or facilities being used by the potential target.

(S) The following are examples of the types of lead information that NSA may examine:

a) Has the target stated that he is located outside the United States? For example, has NSA or another intelligence agency collected a statement or statements made by the target indicating that he is located outside the United States?

b) Has a human intelligence source or other source of lead information indicated that the target is located outside the United States?

c) Does the lead information provided by an intelligence or law enforcement agency of the United States government or an intelligence or law enforcement service of a foreign government indicate that the target is located outside the United States?

d) Was the lead information about the target found on a hard drive or other medium that was seized in a foreign country?

e) With whom has the target had direct contact, and what do we know about the location of such persons? For example, if lead information indicates the target is in direct contact with several members of a foreign-based terrorist organization or foreign-based political organization who themselves are located overseas, that may suggest, depending on the totality of the circumstances, that the target is also located overseas.

**(S) Information NSA Has About the Target's Location and/or Facility or Facilities Used by the Target**

(S) NSA may also review information in its databases, including repositories of information collected by NSA and by other intelligence agencies, as well as publicly available information, to determine if the person's location, or information providing evidence about the person's location, is already known. The NSA databases that would be used for this purpose contain information culled from signals intelligence, human intelligence, law enforcement information, and other sources. For example, NSA databases may include a report produced by the Central Intelligence Agency (CIA) with the fact that a known terrorist is using a telephone with a particular number, or detailed information on worldwide telephony numbering plans for wire and wireless telephone systems.

**(S) NSA Technical Analysis of the Facility**

(S) NSA may also apply technical analysis concerning the facility from which it intends to acquire foreign intelligence information to assist it in making determinations concerning the location of the person at whom NSA intends to direct surveillance. For example, NSA may examine the following types of information:

(S) For telephone numbers:

a) Identify the country code of the telephone number, and determine what it indicates about the person's location.

b) Review commercially available and NSA telephone numbering databases for indications of the type of telephone being used (e.g. landline, wireless mobile, satellite, etc.), information that may provide an understanding of the location of the target.

(S) For electronic communications accounts/addresses/identifiers:

Review NSA content repositories and Internet communications data repositories (which contain, among other things, Internet communications metadata) for previous Internet activity. This information may contain network layer (e.g., Internet Protocol addresses) or machine identifier (e.g., Media Access Control addresses) information, which NSA compares to information contained in NSA's communication network databases and commercially available Internet Protocol address registration information in order to determine the location of the target.

**(S) Assessment of the Non-United States Person Status of the Target**

(S) In many cases, the information that NSA examines in order to determine whether a target is reasonably believed to be located outside the United States may also bear upon the non-United States person status of that target. For example, lead information provided by an intelligence or law enforcement service of a foreign government may indicate not only that the target is located in a foreign country, but that the target is a citizen of that or another foreign country. Similarly, information contained in NSA databases, including repositories of information collected by NSA and by other intelligence agencies, may indicate that the target is a non-United States person.

(S) Furthermore, in order to prevent the inadvertent targeting of a United States person, NSA maintains records of telephone numbers and electronic communications accounts/addresses/identifiers that NSA has reason to believe are being used by United States persons. Prior to targeting, a particular telephone number or electronic communications account/address/identifier will be compared against those records in order to ascertain whether NSA has reason to believe that telephone number or electronic communications account/address/identifier is being used by a United States person.

(S) In the absence of specific information regarding whether a target is a United States person, a person reasonably believed to be located outside the United States or whose location is not known will be presumed to be a non-United States person unless such person can be positively identified as a United States person, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person.

**(S) Assessment of the Foreign Intelligence Purpose of the Targeting**

(S) In assessing whether the target possesses and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory, NSA considers, among other things, the following factors:

a. With respect to telephone communications:

- Information indicates that the telephone number has been used to communicate directly with another telephone number reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
- Information indicates that a user of the telephone number has communicated directly with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Information indicates that the telephone number is listed in the telephone directory of a telephone used by an individual associated with a foreign power or foreign territory;
- Information indicates that the telephone number has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Publicly available sources of information (e.g., telephone listings) match the telephone number to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Information contained in various NSA-maintained knowledge databases containing foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register and trap or trace device, or other information, reveals that the telephone number has been previously used by an individual associated with a foreign power or foreign territory;[1] or

[1] (TS//SI//NF) The NSA knowledge databases that would be used to satisfy this factor contain fused intelligence information concerning international terrorism culled from signals intelligence, human intelligence, law enforcement information, and other sources. The information compiled in these databases is information that assists the signals intelligence system in effecting collection on intelligence targets. For example, a report produced by the CIA may include the fact that a known terrorist is using a telephone with a particular number. NSA would include that information in its knowledge databases.

- Information made available to NSA analysts as a result of processing telephony metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the telephone number is used by an individual associated with a foreign power or foreign territory.

b. With respect to Internet communications:

- Information indicates that the electronic communications account/address/identifier has been used to communicate directly with an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;

- Information indicates that a user of the electronic communications account/address/identifier has communicated directly with an individual reasonably believed to be associated with a foreign power or foreign territory;

- Information indicates that the electronic communications account/address/identifier is included in the "buddy list" or address book of an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;

- Information indicates that the electronic communications account/address/identifier has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;

- Public Internet postings match the electronic communications account/address/identifier to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;

- Information contained in various NSA-maintained knowledge databases of foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, the use of a pen register or trap and trace device, or other information, reveals that electronic communications account/address/identifier has been previously used by an individual associated with a foreign power or foreign territory;

- Information made available to NSA analysts as a result of processing metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the electronic communications account/address/identifier is used by an individual associated with a foreign power or foreign territory; or

- Information indicates that Internet Protocol ranges and/or specific electronic identifiers or signatures (e.g., specific types of cryptology or steganography) are used almost exclusively by individuals associated with a foreign power or foreign territory,

or are extensively used by individuals associated with a foreign power or foreign territory.

## II. (S) POST-TARGETING ANALYSIS BY NSA

(S//SI) After a person has been targeted for acquisition by NSA, NSA will conduct post-targeting analysis. Such analysis is designed to detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States, and will enable NSA to take steps 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, or the intentional targeting of a person who is inside the United States. Such analysis may include:

For telephone numbers:

- Routinely comparing telephone numbers tasked pursuant to these procedures against information that has been incidentally collected from the Global System for Mobiles (GSM) Home Location Registers (HLR). These registers receive updates whenever a GSM phone moves into a new service area. Analysis of this HLR information provides a primary indicator of a foreign user of a mobile telephone entering the United States.

- NSA analysts may analyze content for indications that a foreign target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

For electronic communications accounts/addresses/identifiers:

- Routinely checking all electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against available databases that contain Internet communications data (including metadata) to determine if an electronic communications account/address/identifier was accessed from overseas. Such databases contain communications contact information and summaries of communications activity from NSA signals intelligence collection. The foreign access determination is made based on comparing the Internet Protocol address associated with the account activity to other information NSA possesses about geographical area(s) serviced by particular Internet Protocol addresses. If the IP address associated with the target activity is identified as a U.S.-based network gateway (e.g., a Hotmail server) or a private Internet Protocol address, then NSA analysts will be required to perform additional research to determine if the access was in a foreign country using additional criteria such as machine identifier or case notation (NSA circuit identifier) of a communications link known to be foreign. Such databases normally maintain information about such activity for a 12-month period. This data will be used in an attempt to rule out false positives from U.S.-based network gateways. If the account access is determined to be from a U.S.-based machine, further analytic checks will be performed using content collection to determine if the target has moved into the United States.

- Routinely comparing electronic communications accounts/addresses/identifiers tasked pursuant to these procedures against a list of electronic communications accounts/ addresses/identifiers already identified by NSA as being accessed from inside the United States. This will help ensure that no target has been recognized to be located in the United States.

- NSA analysts may analyze content for indications that a target has entered or intends to enter the United States. Such content analysis will be conducted according to analytic and intelligence requirements and priorities.

(S) If NSA determines that a target has entered the United States, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay. In cases where NSA cannot resolve an apparent conflict between information indicating that the target has entered the United States and information indicating that the target remains located outside the United States, NSA will presume that the target has entered the United States and will terminate the acquisition from that target. If at a later time NSA determines that the target is in fact located outside the United States, NSA may re-initiate the acquisition in accordance with these procedures.

(S) If NSA determines that a target who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will follow the procedures set forth in section IV of this document, including the termination of the acquisition from the target without delay.

## III. (U) DOCUMENTATION

(S) Analysts who request tasking will document in the tasking database a citation or citations to the information that led them to reasonably believe that a targeted person is located outside the United States. Before tasking is approved, the database entry for that tasking will be reviewed in order to verify that the database entry contains the necessary citations.

(S) A citation is a reference that identifies the source of the information, such as a report number or communications intercept identifier, which NSA will maintain. The citation will enable those responsible for conducting oversight to locate and review the information that led NSA analysts to conclude that a target is reasonably believed to be located outside the United States.

(S) Analysts also will identify the foreign power or foreign territory about which they expect to obtain foreign intelligence information pursuant to the proposed targeting.

## IV. (U) OVERSIGHT AND COMPLIANCE

(S) NSA's Signals Intelligence Directorate (SID) Oversight and Compliance, with NSA's Office of General Counsel (OGC), will develop and deliver training regarding the applicable procedures to ensure intelligence personnel responsible for approving the targeting of persons under these procedures, as well as analysts with access to the acquired foreign intelligence information understand their responsibilities and the procedures that apply to this acquisition. SID Oversight and Compliance has established processes for ensuring that raw traffic is labeled and stored only in authorized repositories, and is accessible only to those who have had the proper training. SID

Oversight and Compliance will conduct ongoing oversight activities and will make any necessary reports, including those relating to incidents of noncompliance, to the NSA Inspector General and OGC, in accordance with its NSA charter. SID Oversight and Compliance will also ensure that necessary corrective actions are taken to address any identified deficiencies. To that end, SID Oversight and Compliance will conduct periodic spot checks of targeting decisions and intelligence disseminations to ensure compliance with established procedures, and conduct periodic spot checks of queries in data repositories.

(S) The Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) will conduct oversight of NSA's exercise of the authority under section 702 of the Act, which will include periodic reviews by DOJ and ODNI personnel to evaluate the implementation of the procedures. Such reviews will occur at least once every sixty days.

(S) NSA will report to DOJ, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer any incidents of noncompliance with these procedures by NSA personnel that result in the intentional targeting of a person reasonably believed to be located in the United States, the intentional targeting of a United States person, or the intentional acquisition of any communication in which the sender and all intended recipients are known at the time of acquisition to be located within the United States. NSA will provide such reports within five business days of learning of the incident. Any information acquired by intentionally targeting a United States person or a person not reasonably believed to be outside the United States at the time of such targeting will be purged from NSA databases.

(S) NSA will report to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer, any incidents of noncompliance (including overcollection) by any electronic communication service provider to whom the Attorney General and Director of National Intelligence issued a directive under section 702. Such report will be made within five business days after determining that the electronic communication service provider has not complied or does not intend to comply with a directive.

(S) In the event that NSA concludes that a person is reasonably believed to be located outside the United States and after targeting this person learns that the person is inside the United States, or if NSA concludes that a person who at the time of targeting was believed to be a non-United States person was in fact a United States person, it will take the following steps:

1) Terminate the acquisition without delay and determine whether to seek a Court order under another section of the Act. If NSA inadvertently acquires a communication sent to or from the target while the target is or was located inside the United States, including any communication where the sender and all intended recipients are reasonably believed to be located inside the United States at the time of acquisition, such communication will be treated in accordance with the applicable minimization procedures.

2) Report the incident to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer within five business days.

## V. (U) DEPARTURE FROM PROCEDURES

(S) If, in order to protect against an immediate threat to the national security, NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures and that it is not feasible to obtain a timely modification of these procedures from the Attorney General and Director of National Intelligence, NSA may take such action and will report that activity promptly to DOJ through the Deputy Assistant Attorney General in the National Security Division with responsibility for intelligence operations and oversight, to the ODNI Office of General Counsel, and to the ODNI Civil Liberties Protection Officer. Under such circumstances, the Government will continue to adhere to all of the statutory limitations set forth in subsection 702(b) of the Act.

7-28-09
Date

Eric H. Holder, Jr.
Attorney General of the United States

# Exhibit F

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2011 OCT 31 P 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

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | | |
|---|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | ) | Civil Action No. 1:15-cv-00662-TSE |

# EXHIBIT B

**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

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

**PUBLIC DECLARATION OF DANIEL R. COATS,**
**DIRECTOR OF NATIONAL INTELLIGENCE**

I, DANIEL R. COATS, do hereby state and declare as follows:

## INTRODUCTION

1. I am the Director of National Intelligence ("DNI") and have held this position since March 16, 2017. As the DNI, I oversee the United States Intelligence Community ("IC") and serve as the principal intelligence advisor to the President. Prior to commencing my role as the DNI, I held various positions within the United States Congress. Specifically, from 1981 to 1999, I served in the U.S. House of Representatives and then in the U.S. Senate. During this tenure, I served on the Senate Armed Services Committee and the Senate Select Committee on Intelligence where I worked to strengthen our nation's defense and security. Following my time in Congress, I was named U.S. Ambassador to the Federal Republic of Germany, where I served as the Ambassador from 2001 to 2005. As a U.S. Ambassador and Chief of Mission, I was responsible for leading the embassy's charge to ensure that U.S. foreign policy goals were advanced; the embassy served American interests and values, and all executive branch agencies attached to the embassy did likewise; and executive, legislative, and judicial responsibilities were

carried out. Further, in my role as Chief of Mission, I was directly responsible for the security of the mission, including security from terrorism and protection of all U.S. Government personnel on official duty. After my tenure as U.S. Ambassador to the Federal Republic of Germany, I returned to the U.S. Senate in 2011 and again served on the Senate Select Committee on Intelligence, where I was charged with overseeing intelligence activities and programs of the U.S. Government.

2. The position of the DNI was created by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, §§ 1011(a) and 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending sections 102 through 104 of Title I of the National Security Act of 1947). Subject to the authority, direction, and control of the President, the DNI serves as the head of the IC and as the principal adviser to the President and the National Security Council for intelligence matters related to national security. *See* 50 U.S.C. § 3023(b)(1)-(2).

3. The IC includes the Office of the Director of National Intelligence; the National Security Agency ("NSA"); the Central Intelligence Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Office of Intelligence and Analysis of the Department of the Treasury; the Office of Intelligence and Analysis of the Department of Homeland Security; and such other elements of any other department or agency as may be designated by the President, or jointly

designated by the DNI and heads of the department or agency concerned, as an element of the IC. *See* 50 U.S.C. § 3003(4); *see also* Executive Order 12333 § 3.5.

4. The National Security Act of 1947, as amended, provides that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 3024(i)(1). By this language, Congress expressed its determination that disclosure of intelligence sources or methods is potentially harmful to national security and directed the DNI to protect them.

5. By virtue of my position as the DNI, unless otherwise directed by the President, I have access to all intelligence related to the national security that is collected by any department, agency, or other entity of the United States. 50 U.S.C. § 3024(b).

6. I make the following statements based on my personal knowledge and on information made available to me in my official capacity. Moreover, I have read and personally considered the information contained in the *In Camera, Ex Parte* Declaration of George C. Barnes, Deputy Director, NSA, executed on April 24, 2018 (hereinafter "Classified NSA Declaration").

7. In the course of my official duties, I have been advised of the above-captioned lawsuit and the allegations by the plaintiff, Wikimedia Foundation ("Wikimedia"), concerning NSA's "Upstream" surveillance, a technique employed by the NSA to gather foreign intelligence information under section 702 of the Foreign Intelligence Surveillance Act ("FISA"). I have also been advised of Wikimedia's motion to compel the Government to disclose certain documents and information responsive to Wikimedia's discovery requests ("Motion to Compel"). The purpose of this declaration is to formally assert, in my capacity as DNI and head of the IC, the state secrets privilege and my statutory privilege under the National Security Act in order to

protect intelligence information, sources, and methods that are at risk of disclosure in this case as a result of Wikimedia's Motion to Compel. *See* 50 U.S.C. § 3024(i)(1). This assertion of privilege is over highly sensitive and classified national security information concerning NSA's Upstream surveillance and falling within the categories described herein. This information must be protected because its disclosure reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

## SUMMARY

8. As detailed in this declaration and in the Classified NSA Declaration, disclosure of the documents and information that Wikimedia seeks to compel the Government to disclose reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States. This information should be protected from disclosure to Wikimedia and excluded from any use in this case.

9. Accordingly, as set forth further below, I am asserting the state secrets privilege and the DNI's statutory authority to protect intelligence sources and methods pursuant to 50 U.S.C. § 3024(i)(1) to protect against the disclosure of highly classified and important intelligence information, sources, and methods regarding Upstream surveillance that Wikimedia has sought to compel the Government to disclose in response to Wikimedia's discovery requests (and certain deposition questions) and in response to any further discovery requests Wikimedia may serve in this case, or as otherwise may be necessary to litigate Wikimedia's claims or the Government's defenses in this case. Such information is vital to the national security of the United States and covers the following seven categories: (A) information that would tend to confirm what individuals or entities are subject to Upstream surveillance activities; (B) information concerning the operational details of the Upstream collection process; (C) the

location(s) at which Upstream surveillance is conducted; (D) the categories of Internet-based communications collected through Upstream surveillance activities; (E) information concerning the scope and scale of Upstream surveillance; (F) NSA cryptanalytic capabilities; and (G) additional categories of classified information regarding Upstream surveillance contained in opinions and orders issued by, and submissions made to, the Foreign Intelligence Surveillance Court ("FISC").

10. I make these assertions of privilege mindful of the public disclosures—both authorized and unauthorized—of information about classified NSA intelligence programs, including the IC's declassification and public release of certain materials concerning NSA's Upstream surveillance, which is the program that is challenged in this lawsuit. However, it has remained necessary to withhold considerable details about Upstream surveillance, even from publicly released documents, to protect highly sensitive intelligence information, sources and methods, such as particular subjects of surveillance and methods of collecting and analyzing intelligence information. Therefore, notwithstanding prior disclosures, it is my judgment that additional disclosure of the highly sensitive and still-classified documents and information that Wikimedia has sought to compel the Government to disclose in this case would cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

11. Furthermore, my assertions of privilege have not been made to conceal a violation of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency of the Government; to restrain competition; or to prevent or delay the release of information that does not require protection in the interests of national security.

12. For these reasons, as set forth further below, I request that the Court uphold the state secrets and statutory privilege assertions that I make herein, as well as the statutory privilege assertion made by the NSA pursuant to Section 6 of the National Security Agency Act (50 U.S.C. § 3605(a)), and protect from disclosure the information that Wikimedia now seeks to compel the Government to disclose.

## BACKGROUND OF THE CHALLENGED UPSTREAM PROGRAM

13. In July 2008, Congress enacted the Foreign Intelligence Surveillance Act Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436. This Act added a new section 702 to FISA, 50 U.S.C. § 1881a ("Section 702"), which created new statutory authority permitting the targeting of non-United States persons reasonably believed to be outside of the United States to acquire foreign intelligence information, without individualized orders or warrants from the FISC. More specifically, Section 702 provides that, upon the FISC's approval of a "certification" submitted by the Government, the Attorney General and the DNI may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a), (h). Although the statute does not require the IC to identify the specific facilities, places, premises, or property at which an authorized acquisition will be directed, the Government must certify that an acquisition involves obtaining foreign intelligence information "from or with the assistance of an electronic communication service provider." *Id.* § 1881a(h)(2)(A)(vi).

14. Under Section 702, the Attorney General and the DNI submit annual certifications to the FISC for its approval, as required under the statute, to authorize the targeting of non-U.S. persons reasonably believed to be located outside of the United States to acquire foreign

intelligence information. These certifications identify categories of foreign intelligence information authorized for acquisition but do not identify the particular non-U.S. persons who will be targeted. Instead, the certifications include targeting procedures, approved by the Attorney General in consultation with the DNI, which must, among other things, be reasonably designed to ensure that any Section 702 acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of wholly domestic communications. In addition, the targeting procedures specify the manner in which the IC determines whether a person is a non-U.S. person reasonably believed to be located outside the United States who is likely to possess or receive foreign intelligence information authorized for acquisition by a certification.[1]

15. There are two types of Section 702 acquisition: what has been publicly referred to as "PRISM" collection and "Upstream" collection. I understand that this case involves a legal challenge to Upstream collection. In unclassified terms, in the course of the Upstream collection process, certain Internet transactions transiting the Internet backbone network(s) of certain electronic communication service provider(s) are filtered for the purpose of excluding wholly domestic communications and are then scanned to identify for acquisition those transactions that

1. Four requirements must be met for FISC approval of a Section 702 certification. First, the Attorney General and the DNI must certify, among other things, that a significant purpose of the acquisitions is to obtain foreign intelligence information, as that term is defined under FISA, and the FISC must find that the Attorney General and DNI's certification contains all of the required statutory elements. 50 U.S.C. § 1881a(h)(2)(A)(v), (j)(2)(A). Second, the FISC must find that the Government's targeting procedures are reasonably designed to ensure that acquisitions conducted under the authorization (a) are limited to targeting non-U.S. persons reasonably believed to be located outside the United States, and (b) will not intentionally acquire communications known at the time of acquisition to be purely domestic. *Id.* § 1881a(j)(2)(B). Third, the FISC must find that the Government's minimization procedures meet FISA's requirements. *Id.* §§ 1801(h), 1821(4), 1881a(j)(2)(C). And fourth, the FISC must find that the Government's targeting and minimization procedures are consistent, not only with FISA, but also with the requirements of the Fourth Amendment. *Id.* § 1881a(j)(3)(A). Following passage of the FISA Amendments Reauthorization Act of 2017, the FISC must now also find that the Government's querying procedures meet the statutory requirements and are consistent with the Fourth Amendment. *Id.* § 1881a(j)(2)(D); (j)(3)(A).

are to or from (or, prior to early 2017, to, from, or "about") persons[2] targeted in accordance with the applicable NSA targeting procedures; only those transactions that pass through both the filtering and the scanning are ingested into Government databases. While the Upstream collection process has been described in general terms in this declaration and in declassified documents and unclassified reports, certain operational details of Upstream collection remain highly classified as described in the Classified NSA Declaration.

## ASSERTION OF THE STATE SECRETS PRIVILEGE

16. After careful and actual personal consideration of the matter, based upon my own knowledge and on information obtained in the course of my official duties, including the information contained in the Classified NSA Declaration, I have determined that Wikimedia's Motion to Compel implicates highly sensitive and classified state secrets concerning intelligence information, sources, and methods. Disclosure of such information—as set forth herein and described in more detail in the Classified NSA Declaration—reasonably could be expected to cause serious damage, and in many cases exceptionally grave damage, to the national security of the United States. This information must be protected from disclosure and excluded from use in this case. Therefore, as to the information Wikimedia seeks to compel the Government to disclose, I formally assert the state secrets privilege.

## ASSERTION OF STATUTORY PRIVILEGE UNDER NATIONAL SECURITY ACT

17. Through this declaration, I also hereby invoke and assert a statutory privilege held by the DNI under the National Security Act of 1947, as amended, to protect the information described herein and in the Classified NSA Declaration, *see* 50 U.S.C. § 3024(i)(1). My

2. When the NSA targets a non-U.S. person under Section 702, it must identify a specific communications identifier, known as a "selector." A selector cannot be the name of the individual or a keyword.

assertion of this statutory privilege for intelligence sources and methods is coextensive with my state secrets privilege assertion.

## INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE

18. In general and unclassified terms, documents and information responsive to Wikimedia's discovery requests that Wikimedia has sought to compel the Government to disclose are subject to my state secrets and statutory privilege assertions because they contain the following seven categories of classified information:

A. *Individuals or Entities Subject to Upstream Surveillance Activities:* Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that indicate or may tend to indicate whether communications of Wikimedia, and/or of other individuals and entities, have been subject to Upstream surveillance activities;

B. *Operational Details of the Upstream Collection Process:* Documents and information (not already encompassed by other categories herein) responsive to Wikimedia's pending discovery requests or to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still-classified technical details concerning the methods, processes, and devices employed (including the design, operation, and capabilities of the devices employed) to conduct Upstream surveillance;

C. *Location(s) at Which Upstream Surveillance is Conducted:* Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still-classified information about any specific location(s), or the nature of the location(s), on the Internet backbone network(s) of U.S. electronic communication service provider(s) at which Upstream surveillance is conducted;

D. *Categories of Internet-Based Communications Subject to Upstream Surveillance Activities:* Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still-classified information about the specific types or categories of communications either subject to or acquired in the course of the Upstream collection process;

E. *Scope and Scale on Which Upstream Surveillance Is or Has Been Conducted:* Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still-classified information about (i) the volume or proportion of Internet communications traffic, including international Internet communications, either subject to or acquired in the course of the Upstream collection process, (ii) the number, proportion, and/or bandwidth of any circuit, international submarine or terrestrial cable, or other Internet backbone link, on which Upstream surveillance is or has been conducted; and (iii) any other measure of the scope or scale on which Upstream surveillance is or has been conducted;

F. *NSA Cryptanalytic Capabilities (or Lack Thereof)*: Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still-classified information about the NSA's capability, or lack thereof, to decrypt, circumvent, or defeat specific types of communications security protocols; and

G. *Additional Categories of Classified Information Contained in Opinions and Orders issued by, and submissions made to, the FISC Concerning Upstream:* The additional categories of classified information contained in the documents responsive to Wikimedia's discovery Requests for Production numbered 21 and 22 (and not already encompassed by categories A-F, above) as set forth in the privilege log served by Defendant United States Department of Justice on March 19, 2018.

## HARM OF DISCLOSING INFORMATION SUBJECT TO PRIVILEGE

19. As discussed in detail in the Classified NSA Declaration, protection of these categories of information is key to the NSA's ability to produce foreign intelligence information, which depends on its access to foreign and international electronic communications. Foreign intelligence information produced by communications intelligence activities, such as Upstream surveillance, is an extremely important part of the overall foreign intelligence information available to the United States. Indeed, communications intelligence is often the only means by which the United States can learn the existence of particular threats or the identities of particular individuals who are involved in hostile activities. Communications intelligence is thus essential to the ability of the IC to identify adversaries and to detect and disrupt their plans for attacks and other hostile acts against the United States. Against that backdrop, the risks of disclosing the specific categories of information described herein are especially grave.

20. Below, I describe each of these categories, and the harm that reasonably could be expected to result from disclosure, in unclassified terms. Much of the harm, however, necessarily must be described in classified terms, and, as such, is set forth in the Classified NSA Declaration.

### A. Information That May Tend to Confirm or Deny Whether or Not the Communications of Wikimedia or Other Individuals or Entities Have Been Subjected to Upstream Surveillance Activities.

21. The first category of information over which I am asserting privilege is information that would tend to reveal whether particular individuals or entities, including Wikimedia, have been subjected to Upstream surveillance activities. Disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

22. My privilege assertion over information that may tend to confirm or deny whether or not the communications of Wikimedia, or other individuals or entities, have been subject to Upstream surveillance includes, for example, Wikimedia's attempt to compel the Government to confirm or deny whether or not NSA has copied, reviewed the content of, and/or retained at least one Wikimedia communication in the course of Upstream surveillance, and Wikimedia's attempt to compel the Government to confirm or deny the authenticity of purportedly classified documents which Wikimedia believes indicate that the NSA targets its communications for Upstream surveillance.

23. The Government cannot publicly confirm or deny whether any particular individual or entity is subject to intelligence-gathering activities, no matter how likely or unlikely it might appear that the individual or entity would be subject to surveillance. If the Government were to reveal that an individual or entity is the target or a subject of intelligence-gathering, the collection capability relating to that individual or entity would certainly be compromised. On the other hand, if the Government were to reveal that an individual or entity is not the target or subject of intelligence-gathering, adversaries would know that a particular individual has avoided scrutiny and is a secure source for communicating. Moreover, providing assurances to those individuals who (or entities which) are not targets or subjects quickly becomes unworkable when faced with a situation in which an individual (or entity) has in fact been a target or subject. If the Government were to confirm that any specific individual or entity is not a target or subject of intelligence-gathering, but later refuse to confirm or deny that fact in a situation involving an actual target or subject, it would be apparent that intelligence-gathering was occurring in the latter case. The only recourse for the Government is to neither confirm nor deny whether someone (or some entity) has been targeted by or subject to NSA intelligence-gathering

activities, regardless of whether the individual or entity has been a target or subject or not. To say otherwise when challenged in litigation would result in the frequent, routine exposure of intelligence information, sources, and methods, and would severely undermine surveillance activities in general.

24. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**B. Operational Details of the Upstream Collection Process.**

25. The second category of information over which I am asserting privilege is still-classified information concerning the operational details of the Upstream collection process, as discussed in greater detail in the Classified NSA Declaration (and where such information is not already encompassed by other categories of privileged information described elsewhere in this declaration). Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

26. My privilege assertion over the operational details of the Upstream collection process includes, for example, Wikimedia's request for additional technical details concerning "filtering mechanisms" employed by NSA and the "scanning," "screening," and content review of communications during Upstream surveillance. Although the IC has publicly acknowledged the existence of the Upstream surveillance program and has publicly released a limited amount of information describing, at a high level of generality, how Upstream operates, additional technical details about the Upstream collection process remain classified.

27. As discussed in greater detail in the Classified NSA Declaration, disclosure of still-classified operational details regarding Upstream surveillance, either directly or indirectly, would reveal to our adversaries the extent of the ability of the United States to monitor and track their activities and communications, thereby helping our adversaries evade detection, which would seriously compromise, if not destroy, important and vital ongoing intelligence operations.

28. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**C. The Location(s) Where Upstream Surveillance is Conducted.**

29. The third category of information over which I am asserting privilege is information that would, directly or indirectly, tend to reveal the location(s) on the Internet backbone where Upstream surveillance is conducted. Public disclosure of such information, even at a general level, reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

30. My privilege assertion over the location(s) on the Internet backbone where Upstream surveillance is conducted includes information regarding the number and nature of such Upstream surveillance point(s). For example, Wikimedia has sought disclosure of information sufficient to show the "number of circuits" and "number of Internet chokepoints" at which Upstream surveillance is conducted. Although the IC has publicly acknowledged that Upstream surveillance is conducted on one or more points on the Internet backbone, we have not acknowledged any further details regarding the location of these one or more points or any information about the nature or number of these one or more points.

31. As discussed in greater detail in the Classified NSA Declaration, disclosing information on the location(s) where Upstream surveillance is conducted would assist foreign adversaries in trying to evade particular channels of communications that are being monitored, exploit any particular channels of communications that are not being monitored, and target location(s) where the NSA obtains critical foreign intelligence information for hostile action.

32. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration), either directly or indirectly, would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**D. Categories of Internet-Based Communications Subject to Upstream Surveillance Activities.**

33. The fourth category of information over which I am asserting privilege is information that would tend to reveal categories of Internet-based communications subject to and not subject to Upstream surveillance activities. Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

34. My privilege assertion over information that would tend to reveal the types of communications collected through Upstream surveillance includes, for example, information sought by Wikimedia in deposition questions it asked NSA's designated witness concerning whether NSA collection devices are configured to exclude various types of encrypted communications. However, as discussed in greater detail in the Classified NSA Declaration, disclosing information on the types of communications collected through Upstream surveillance would induce our foreign adversaries to avoid those forms of online communications in order to defeat NSA's attempts to capture their communications.

35. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**E. Information Concerning the Scope and Scale of Upstream Surveillance.**

36. The fifth category of information over which I am asserting privilege is information concerning the scope and scale of Upstream surveillance. Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

37. My privilege assertion over the scope and scale of Upstream surveillance includes, for example, Wikimedia's requests that the Government describe the approximate amount of Internet traffic subject to each stage of the Upstream collection process and that the Government admit that the NSA conducts Upstream surveillance on "multiple international Internet links." The IC has publicly acknowledged that (a) NSA is monitoring at least one circuit carrying international Internet communications and (b) the Upstream process necessarily involves the NSA having access to a larger body of communications than those that contain the targeted selectors in order to filter and scan that larger body to ingest into NSA repositories only those communications containing the selectors. However, any additional facts about the scope and scale of the Upstream surveillance program remain classified.

38. As discussed in greater detail in the Classified NSA Declaration, disclosing information regarding the scope and scale of Upstream surveillance would inform foreign adversaries whether they should increase or decrease their efforts to avoid such surveillance.

39. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**F. NSA Cryptanalytic Capabilities (or Lack Thereof).**

40. The sixth category of information over which I am asserting privilege is information concerning NSA's capabilities, or lack thereof, to decrypt, circumvent, or defeat communications security protocols. Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

41. My privilege assertion over the NSA's cryptanalytic capabilities includes, for example, Wikimedia's request that the Government describe any Internet Protocols subject to Upstream surveillance that NSA is able to decrypt, as well as Wikimedia's request that the Government admit whether NSA has the ability to decrypt any portion of HTTPS (HyperText Transfer Protocol Secure) communications that may be subject to Upstream surveillance.

42. As discussed in greater detail in the Classified NSA Declaration, NSA's capabilities against communications security protocols are exceptionally fragile. Public disclosure of information concerning NSA's capabilities, or lack thereof, to decrypt, circumvent, or defeat communications security protocols would cause adversaries to shift their communications to less susceptible protocols. NSA's resulting loss of foreign intelligence information would cause irreparable damage to national security.

43. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would

compromise important and critical information, sources, and methods, causing exceptionally grave damage to the national security of the United States.

**G. Additional Categories of Classified Information Contained in Opinions and Orders Issued by, and Submissions Made to, the FISC Concerning Upstream Surveillance.**

44. Finally, the seventh category of information over which I am asserting privilege is information contained in opinions and orders issued by, and submissions made to, the FISC concerning Upstream surveillance (where such information is not already encompassed by other categories of privileged information described elsewhere in this declaration). Public disclosure of such information reasonably could be expected to cause exceptionally grave damage to the national security of the United States.

45. My privilege assertion over information contained within opinions and orders issued by, and submissions made to, the FISC concerning Upstream surveillance stems from Wikimedia's request that the Government produce every such opinion, order, or submission concerning Upstream surveillance in its entirety. Although the IC has already publicly released some of these documents in redacted form—including a release of significant FISC opinions concerning FISA Section 702—additional information in these documents remains classified.

46. Because Wikimedia has nonetheless sought disclosure of every opinion, order, and submission concerning Upstream, its expansive request necessarily implicates multiple categories of information, which cannot be described further on the public record but are set forth in the Classified NSA Declaration. The release of this information would be devastating to NSA's mission and collection efforts pursuant to Upstream surveillance, as described in the Classified NSA Declaration.

47. After personal consideration of the matter, it is my judgment that disclosing the information described herein (and in further detail in the Classified NSA Declaration) would

compromise important and critical information, sources, and methods, causing serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

## CONCLUSION

48. In sum, I am asserting the state secrets privilege and the DNI's statutory privilege set forth in 50 U.S.C. § 3024(i)(1) to protect classified documents and information regarding Upstream surveillance that Wikimedia has sought to compel the Government to disclose in response to Wikimedia's discovery requests (and certain deposition questions), as well as in response to any further discovery requests Wikimedia may serve in this case, or as otherwise may be necessary to litigate Wikimedia's claims or the Government's defenses in this case. I have set forth, in general and unclassified terms, as much as I can say on the public record concerning the highly sensitive and classified intelligence information, sources, and methods covered by my privilege assertions and the harm that would result from their disclosure; for a more detailed, classified description of such information, I respectfully refer the Court to the Classified NSA Declaration.

49. I respectfully request that the Court take all steps necessary to protect the intelligence information, sources, and methods described herein in order to prevent serious damage, and in many cases exceptionally grave damage, to the national security of the United States.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: April 25, 2018



DANIEL R. COATS
Director of National Intelligence

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE |

# EXHIBIT C

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No.<br><br>1:15-cv-00662-TSE |

**DECLARATION OF LAUREN L. BERNICK**

I, Lauren L. Bernick, do hereby state and declare as follows:

## I. Introduction

1. I am a Senior Associate Civil Liberties Protection Officer in the Office of Civil Liberties, Privacy, and Transparency ("CLPT") at the Office of the Director of National Intelligence ("ODNI"). I have held this supervisory position since August 8, 2017. Prior to my current position, I was assigned to the ODNI's CLPT office as an Associate, and then a Senior Associate, Civil Liberties Protection Officer on a temporary "detail" assignment from the National Security Division of the Department of Justice ("DOJ"). At DOJ, I served as an attorney-advisor in the Office of Intelligence handling issues related to the Foreign Intelligence Surveillance Act ("FISA"), including the drafting of FISA applications and litigating before the Foreign Intelligence Surveillance Court ("FISC"), from February 2004 until my detail assignment to ODNI in June 2013.

2. CLPT's mission is, among other things, to ensure that the Intelligence Community ("IC")[1] carries out its national security mission in a manner that protects privacy and

1. The IC is comprised of ODNI; the Central Intelligence Agency; the National Security Agency; the Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National Reconnaissance Office; other

civil liberties and provides appropriate transparency to the public in accordance with the *Principles of Intelligence Transparency for the Intelligence Community* (hereinafter, "*Transparency Principles*").[2] *See* ODNI, *Intelligence Community Directive 107* (2018), https://www.dni.gov/files/documents/ICD/ICD-107.pdf. The Chief of the CLPT office also serves as the ODNI's Chief Transparency Officer. *Id*. To fulfill its transparency mission, CLPT's subject matter expertise includes national security laws (e.g., FISA); classification of national security information; and the processes required to effectuate classification and the authorized released of unclassified information.

3. As part of my current and past duties with CLPT, I am responsible for participating in the oversight of the IC's implementation of Section 702 of FISA.[3] Specifically, the Director of National Intelligence ("DNI") has a statutory duty to assess the IC elements' compliance with procedures and guidelines promulgated pursuant to Section 702. *See* 50 U.S.C. § 1881a(m)(1). The IC elements that currently implement Section 702 are the National Security Agency ("NSA"); Central Intelligence Agency ("CIA"); Federal Bureau of Investigation ("FBI"); and ODNI's National Counterterrorism Center ("NCTC"). I am also responsible for promoting the authorized release of FISA information as it comports with the *Transparency*

---

offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs; the intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy; the Bureau of Intelligence and Research of the Department of State; the Office of Intelligence and Analysis of the Department of the Treasury; the Office of Intelligence and Analysis of the Department of Homeland Security; and such other elements of any other department or agency as may be designated by the President, or jointly designated by the DNI and heads of the department or agency concerned, as an element of the IC. *See* 50 U.S.C. § 3003(4).

2. The IC's *Transparency Principles* are intended to facilitate IC decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security. *See* ODNI, *Transparency Principles* (2015), https://www.dni.gov/files/documents/ppd-28/FINAL%20Transparency_poster%20v1.pdf.

3. Under Section 702, the Director of National Intelligence and the Attorney General may jointly authorize, for up to one year, the targeting of non-United States person reasonably believed to be located outside the United States to acquire foreign intelligence information. *See* 50 U.S.C. § 1881a.

*Principles* and the USA FREEDOM Act (*see* 50 U.S.C. § 1872),[4] as well as the protection of national security information as required by Executive Order 13526.

4. My subject matter expertise focuses on FISA, in particular Section 702. I have developed this expertise through my participation in the following tasks while working at ODNI and DOJ: drafting the joint DNI and Attorney General report assessing the IC elements' compliance with procedures and guidelines promulgated pursuant to Section 702; facilitating review of FISA materials, both within ODNI and among the relevant IC elements, in preparation for authorized release to the public pursuant to the IC's *Transparency Principles*; participating in the interagency classification review process of certain decisions, orders, and opinions issued by the FISC on or after the 2015 enactment of the USA FREEDOM Act; the public reporting of certain statistics relating to national security authorities, such as FISA; processing of FISA materials (including Section 702 materials) through Freedom of Information Act ("FOIA") requests and litigation; intra- and inter-agency coordination of public statements and other public education documents associated with the authorized release of FISA documents, including documents related to Section 702. As a result of these efforts, I developed expertise concerning what aspects of FISA information, and in particular Section 702 information, are and are not classified.

5. In the course of my official duties, I have been advised of the above-captioned lawsuit and the allegations by the plaintiff, Wikimedia Foundation, challenging the NSA's "Upstream" surveillance program conducted pursuant to Section 702 of FISA. I have also been advised of plaintiff's motion to compel the Government to disclose documents, including documents responsive to the following two discovery requests:

---

4. The USA FREEDOM Act added section 602 to FISA, which required the DNI, in consultation with the Attorney General, to conduct a declassification review of each decision, order, or opinion issued by the FISC that includes a significant construction or interpretation of any provision of law. *See* 50 U.S.C. § 1872.

**REQUEST FOR PRODUCTION NO. 21:** All Foreign Intelligence Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court orders and opinions CONCERNING Upstream surveillance.

**REQUEST FOR PRODUCTION NO. 22:** All Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court of Review, and Supreme Court submissions CONCERNING Upstream surveillance.

6. I make the following statements based on my personal knowledge and on information made available to me in my official capacity. The purpose of this declaration is to advise the Court of the time, effort, and resources that would be required if the Court were to direct the IC to conduct a classification review for authorized release of all of the documents responsive to these two discovery requests.

## II. Summary

7. Ordering the IC to process all of the documents responsive to these two discovery requests would require the IC to undergo a time-consuming and resource-intensive classification review process of classified FISC orders and opinions, as well as classified submissions to that court, which are estimated to total more than 10,000 pages. While it is extremely difficult to predict how long such a process would take, I can state that, in a recent FOIA case, it took the IC one year to complete the processing of approximately 80 FISC orders, opinions, and decisions, which contained less than 800 pages. *See Elec. Frontier Found. v. DOJ*, 16-cv-2041 (N.D. Cal.) ("*EFF* FOIA case"). The processing of all documents responsive to these two discovery requests is likely to take much longer given that the number of pages of classified information at issue here is more than twelve times the number involved in the *EFF* FOIA case.

## III. The Requirements That Would Be Placed on the IC to Process These Two Discovery Requests

8. In the event the Court orders the Government to produce the unclassified portions of the classified documents responsive to the two discovery requests, the IC would need to conduct a classification review of more than 10,000 pages. The classification review of classified documents is extremely time consuming and resource intensive.

9. This is so for several reasons. First, the classification review will not be a generalized "pass/fail" review to determine whether a document as a whole is classified or not; instead, such a review will involve a line-by-line and word-by-word analysis to determine whether the information in each document must remain classified in accordance with applicable classification guidance and, consequently, be withheld from the public. Such a classification review will require comprehensive and consistent analysis of the sensitivities of the information, accurate application of classification guidance, and the precise use of redactions to protect all currently classified information. This process is complex and time-consuming because each redaction applied to classified information must correspond to the applicable classification guidance based on the topic and context of the individual information as well as consideration of whether the information is classified when combined with already officially released information.

10. Second, the classification review of all responsive documents will also entail determining whether any of the documents have previously been officially released in part. If any responsive document has previously been officially released in redacted form, the IC will have to determine whether those redactions remain appropriate in light of any official disclosures that may have occurred since the document was released. And, if the document itself has not been previously officially released in any form, the IC will have to determine whether any information contained in the document nevertheless already has been officially disclosed

through, for example, FOIA document productions, transparency disclosures, disclosures mandated by the USA FREEDOM Act, or various Government reports such as those issued by the NSA's Civil Liberties and Privacy Office or the Privacy and Civil Liberties Oversight Board.

11. Third, the classification review will involve multi-layered review by each applicable IC element. Each IC element has multiple internal stakeholders, such as FISA compliance officers, General Counsel offices, privacy and civil liberties offices, and classification offices, each of which may need to be consulted as part of the internal review of any particular document.

12. Finally, for each document, the classification review process will need to be coordinated among each IC element identified as possessing an equity in that document. This consultation necessarily takes time. As I stated above, the IC elements that currently implement Section 702 of FISA are the NSA, the CIA, the FBI, and NCTC. This means that, for any particular document, one or more of these equity holders will need to review every responsive document line-by-line. And, for submissions made by DOJ to the FISC, DOJ officials will also need to review those documents. Coordination between and among all of these equity holders takes time to ensure internal consistency within a document, consistency within a set of responsive documents, and consistency with documents and information previously officially disclosed.

13. If the Court orders the Government to produce the unclassified portions of the classified documents responsive to the two discovery requests, this extremely time-consuming and resource-intensive classification review process would be imposed upon a limited number of subject matter experts who have the necessary and appropriate training and experience to conduct such a review. Classification review for most of these subject matter experts is a collateral duty. These experts have significant competing priorities and responsibilities in their

respective IC elements that include, for example, supporting the operational and mission needs of their respective IC element; preparing statutorily mandated reports to Congress and transparency reports; supporting criminal and military commission cases; and handling FOIA requests and FOIA litigation. The most important of these responsibilities—supporting operational work— takes precedence over other duties. Therefore, imposing the additional duty of an onerous classification review of more than 10,000 pages will necessarily require the IC to reallocate resources from these competing priorities to the classification review, adversely affecting operational and other mission needs.

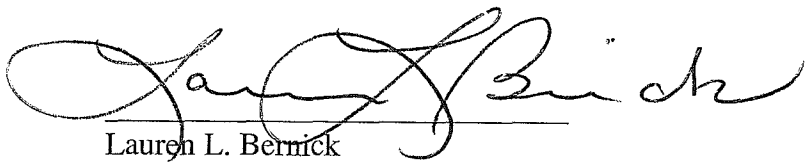
14. For all of the reasons described above, it is extremely difficult to predict the exact amount of time needed to conduct a classification review. Typically, it is not until the process has run its course that an accurate determination can be made as to the difficulty of a review. Nevertheless, I have recent experience with a similar kind of classification process that should serve as a guidepost for the Court as to the time likely required to complete the review Plaintiff seeks here. In the *EFF* FOIA case, the IC conducted a review of approximately 80 FISC orders, opinions, and decisions; about half of the documents were released in redacted form while the remainder were withheld in full. That process took one year. Less than 800 pages were at issue in that review, which is far less than the over 10,000 pages sought by plaintiff in the two discovery requests discussed herein. While it is unlikely that the review sought here would take more than a decade, a twelve-fold increase in the pages at issue means that, at the very least, the classification review Plaintiff seeks here would take more than one year, and possibly several years, to complete. The only way to reduce processing time would be for each respective IC element to divert significant resources away from operational tasks and other mission needs to process these documents.

15. While my understanding is that the Plaintiff has not narrowed its two discovery requests to seek only those documents that have not been previously subject to classification review, I can state that if such a narrowing of the requests were to be made, it would not significantly affect the processing time for all responsive documents. This is primarily because the bulk of documents responsive to these two requests are submissions to the FISC, the vast majority of which have not been previously subject to classification review. If Plaintiff were to withdraw Request for Production No. 22, and narrow Request for Production No. 21 by limiting it to solely those orders and opinions that have not been previously subject to classification review, only then would the drain on IC resources be significantly eased.

16. In sum, based on my experience in conducting classification reviews in the context of FOIA cases, transparency initiatives, and as part of the mandatory classification process established by the USA FREEDOM Act, I estimate that a court order requiring the IC to conduct a classification review of more than 10,000 pages of classified materials would take at least one year and could take several years to complete.

17. Pursuant to 28 U.S.C. § 1746, I certify under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 27th day of April, 2018.



Lauren L. Bernick
Senior Associate Civil Liberties Protection Officer
Office of the Director of National Intelligence

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No.<br>1:15-cv-00662-TSE |

**NOTICE OF FILING OF UNCLASSIFIED (REDACTED) VERSION OF CLASSIFIED DECLARATION LODGED WITH THE COURT *IN CAMERA* AND *EX PARTE* ON APRIL 27, 2018, IN SUPPORT OF THE GOVERNMENT'S ASSERTION OF THE STATE SECRETS PRIVILEGE AND RELATED STATUTORY PRIVILEGES**

Defendants National Security Agency ("NSA"); the United States Department of Justice; the Office of the Director of National Intelligence; General Paul M. Nakasone, in his official capacity as Director of the NSA; Jefferson B. Sessions, III, in his official capacity as Attorney General of the United States; and the Honorable Daniel Coats, in his official capacity as Director of National Intelligence, hereby give notice that they are filing, as an attachment hereto, a redacted, unclassified version of the Classified Declaration of George C. Barnes, Deputy Director of the NSA, which was lodged with the Court Information Security Officer on April 27, 2018, for the Court's *in camera*, *ex parte* consideration in support of the Government's assertion in this matter of the state secrets privilege and the statutory privileges established under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a). *See* ECF No. 137 (notice of lodging of Classified Declaration of George C. Barnes, Deputy Director of the NSA).

Dated: May 11, 2018

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

*/s/ James J. Gilligan*
JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Trial Counsel

JULIA A. BERMAN
TIMOTHY A. JOHNSON
OLIVIA HUSSEY-SCOTT
Trial Attorneys

U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
james.gilligan@usdoj.gov

*Counsel for Defendants*

# ATTACHMENT

~~TOP SECRET//SI//ORCON/NOFORN~~

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

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

**CLASSIFIED DECLARATION OF GEORGE C. BARNES,**
**DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY**

(U) TABLE OF CONTENTS

I. (U) INTRODUCTION ..... 1

II. (U) CLASSIFICATION OF DECLARATION ..... 2

III. (U) SUMMARY ..... 3

IV. (U) BACKGROUND ..... 8

A. (U) The National Security Agency and Its Signals Intelligence Mission ..... 8

B. (U) External Threats to the National Security of the United States ..... 10

C. (U) Collection of Communications Content Pursuant to FISA Section 702 ..... 13

D. (U) Upstream Collection ..... 17

E. (U) The Wikimedia Discovery Requests ..... 22

V. (U) INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE ..... 27

VI. (U) HARM OF DISCLOSURE OF PRIVILEGED INFORMATION ..... 30

A. (U) Information Concerning Whether Communications of Wikimedia or of Other Entities or Individuals Have Been Subjected to Upstream Surveillance Activities ..... 30

B. (U) Operational Details of the Upstream Collection Process ..... 37

C. (U) Location(s) on the Internet Backbone Where Upstream Surveillance Is Conducted .. 44

D. (U) Categories of Internet-Based Communications Subject to Upstream Surveillance Activities ..... 51

E. (U) Scope and Scale of Upstream Surveillance ..... 54

F. (~~S//NF~~) NSA's Capabilities, or Lack Thereof, to Decrypt, Circumvent, or Defeat Communications Security Protocols ..... 58

G. (U) Additional Categories of Classified Information Contained in Opinions, Orders, and Court Submissions Concerning Upstream Surveillance ..... 60

VII. (U) CONCLUSION ..... 65

**(U)** I, George C. Barnes, for my declaration pursuant to 28 U.S.C. § 1746, depose and say as follows:

## I. (U) INTRODUCTION

1. **(U)** I am the Deputy Director of the National Security Agency ("NSA"), an intelligence agency within the Department of Defense. I have held this position since May 1, 2017. Prior to serving as Deputy Director, I served as the Director, Workforce Support Activities Directorate, and have been an NSA employee since 1987. I have served in a variety of roles at the Agency, including as NSA's Special United States Liaison Officer in London, where I supported our cryptologic partnership with the United Kingdom and interacted regularly with key U.K. intelligence and cybersecurity leadership, as well as the Chief of Data Acquisition, overseeing NSA's signals intelligence access, collection, and exploitation. I have been designated an original TOP SECRET classification authority under Executive Order No. 13526, 75 Fed. Reg. 707 (Jan. 5, 2010), and Department of Defense Manual No. 5200.1, Vol. 1, Information and Security Program (Feb. 24, 2012).

2. **(U)** The purpose of this declaration is to support an assertion of the military and state secrets privilege (hereinafter, "state secrets privilege") by the Director of National Intelligence ("DNI") in his capacity as head of the Intelligence Community, as well as the DNI's assertion of a statutory privilege under the National Security Act of 1947, *see* 50 U.S.C. § 3024(i)(1), to protect the information described below. The information in question is sought in discovery by the Plaintiff in the above-captioned case, Wikimedia Foundation ("Wikimedia"), and concerns critical NSA intelligence-gathering activities and capabilities. This information is classified, extraordinarily sensitive, and its disclosure reasonably could be expected to cause exceptionally grave damage to the national security of the United States. Through this declaration, I also

hereby invoke and assert the NSA's statutory privilege set forth in Section 6 of the National Security Agency Act of 1959, Public Law No. 86-36 (codified at 50 U.S.C. § 3605(a)), to protect information related to NSA intelligence activities as described herein.

3. **(U)** The statements made herein are based on my personal knowledge of NSA activities and operations, and on information made available to me in my official capacity as the Deputy Director of NSA.

## II. (U) CLASSIFICATION OF DECLARATION

4. **(U)**This declaration is classified TOP SECRET//SI//ORCON/NOFORN pursuant to the standards in Executive Order No. 13526. *See* 75 Fed. Reg. 707 (Dec. 29, 2009). Under Executive Order No. 13526, information is classified "TOP SECRET" if unauthorized disclosure of the information reasonably could be expected to cause exceptionally grave damage to the national security of the United States; "SECRET" if unauthorized disclosure of the information reasonably could be expected to cause serious damage to national security; and "CONFIDENTIAL" if unauthorized disclosure of the information reasonably could be expected to cause identifiable damage to national security. At the beginning of each paragraph of this declaration, the letter or letters in parentheses designate(s) the level of classification of the information the paragraph contains. When used for this purpose, the letters "U," "C," "S," and "TS" indicate respectively that the information is either UNCLASSIFIED, or is classified CONFIDENTIAL, SECRET, or TOP SECRET.

5. **(U)** Additionally, this declaration contains Sensitive Compartmented Information (SCI), which is "information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods." 28

C.F.R. § 17.18(a). Because of the exceptional sensitivity and vulnerability of such information, these safeguards and access requirements exceed the access standards that are normally required for information of the same classification level. Specifically, this declaration references communications intelligence ("COMINT"), also referred to as special intelligence ("SI"), which is a subcategory of SCI. COMINT or SI identifies SCI that was derived from exploiting cryptographic systems or other protected sources by applying methods or techniques, or from foreign communications.

6. **(U)** Finally, the "ORCON" designator means that the originator of the information controls to whom it is released. In addition to the fact that classified information contained herein and that is contained within the accompanying documents may not be revealed to any person without authorization pursuant to Executive Order 13526, this declaration and many of the accompanying documents contain information that may not be released to foreign governments, foreign nationals, or non-U.S. citizens without permission of the originator and in accordance with DNI policy. This information is labeled "NOFORN."

7. **(U)** Accordingly, none of the information in this declaration can be removed from classified channels without prior classification review by NSA.

## III. (U) SUMMARY

8. **(U)** I have been informed that Wikimedia alleges that a technique employed by the NSA to gather foreign intelligence information under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), known as Upstream surveillance,[1] exceeds the Government's

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

authority under FISA, violates the Constitution, and should be permanently enjoined. It is my understanding that the question now before the Court for resolution is whether Wikimedia has legal standing to assert these claims. In an effort to prove its standing, Wikimedia has served a total of 84 discovery requests on the Government, including interrogatories, requests for admission, and document requests. Wikimedia has also taken the deposition of a designated NSA official under Federal Rule of Civil Procedure 30(b)(6). Wikimedia's discovery requests and deposition questions are apparently intended to uncover direct and indirect evidence to support Wikimedia's standing to challenge Upstream surveillance.

9. **(U)** It is my understanding that although the NSA and the other Defendant Government agencies responded to many of Wikimedia's discovery requests, the Government also objected in whole or in part to certain requests based, *inter alia*, on the classified, privileged, and extraordinarily sensitive nature of the national security information Wikimedia sought. The Government also objected to and refused to answer certain deposition questions because they, too, called for classified, privileged, and extraordinarily sensitive national security information. In particular, the Government has objected to any discovery requests or deposition questions that would tend to reveal whether Wikimedia's communications have been subject to Upstream surveillance; operational details of Upstream surveillance; the locations on the Internet backbone where Upstream surveillance is or has been conducted; the types of communications collected through Upstream surveillance; the scope of Upstream surveillance; NSA's cryptanalytic capabilities; and certain additional categories of classified information contained in opinions by, orders from, and submissions to, the Foreign Intelligence Surveillance Court ("FISC") regarding

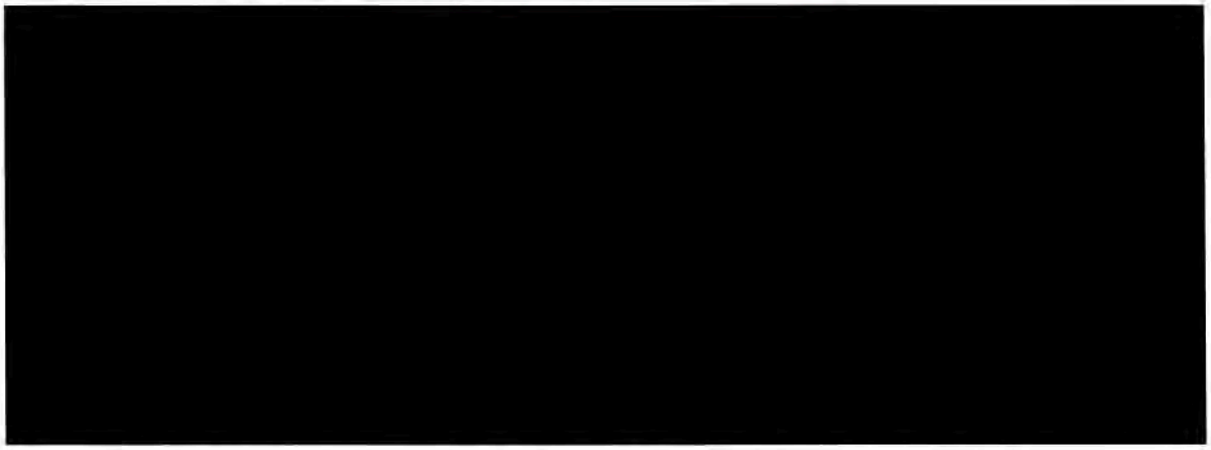
Upstream surveillance. Wikimedia has now moved to compel the disclosure of this classified, privileged, and extraordinarily sensitive national security information.

10. **(U)** This declaration supports the assertion of the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1) by the DNI over the classified information that Wikimedia seeks, whether in response to Wikimedia's pending discovery requests, in response to any further discovery requests Wikimedia may serve in this case, or as otherwise may be necessary to litigate Wikimedia's claims or the Government's defenses in this case. I also assert herein the NSA's statutory privilege under 50 U.S.C. § 3605(a) over the same categories of information. As set forth in the accompanying public declaration of the DNI, and explained in classified detail below, the disclosure of the information and documents that Wikimedia seeks could reasonably be expected to cause exceptionally grave damage to the national security of the United States, and therefore must be protected from disclosure and excluded from this case.

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

[redacted]

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



12. **(U)** The facts at issue include, first, whether or not any of Wikimedia's communications, or of other individuals and entities, have been subject to Upstream surveillance. As a matter of course, the Government cannot publicly confirm or deny whether any individual or organization is or has been subject to NSA intelligence-gathering activities, because to do so would tend to reveal to our adversaries who are the NSA's actual targets of surveillance and who are not, which channels of communication are free from NSA surveillance and which are not, and other sensitive intelligence methods and sources, thereby helping our adversaries evade detection and capitalize on limitations in the NSA's surveillance capabilities.

13. **(U)** As further explained below, it is also essential to protect information concerning the operational details of Upstream surveillance, as well as the location(s) on the Internet "backbone" where Upstream surveillance is conducted; the types of communications collected through Upstream surveillance; the scale and scope of Upstream surveillance; NSA's cryptanalytic capabilities; and additional categories of classified information contained in opinions, orders, and submissions to the FISC concerning Upstream surveillance that Wikimedia seeks in discovery. Notwithstanding the Government's disclosure of certain facts, in order to promote transparency and public understanding about the Upstream program, the additional

disclosure of the information Wikimedia seeks to compel could reasonably be expected to cause exceptionally grave damage to national security.

14. **(U)** Most obviously, the disclosure of the information Wikimedia seeks would reveal to foreign adversaries the NSA's operational methods and capabilities (or lack thereof), and specific channels of communication from which the NSA has in the past and continues today to obtain intelligence information, thus enabling them to evade particular channels that are being monitored, to exploit channels that are not subject to NSA collection, to target for hostile action the facilities where the NSA obtains critical foreign intelligence, and to exploit the NSA's sources and methods of surveillance for their own purposes. In addition, the information that Wikimedia seeks would also tend to reveal the identities of specific foreign targets of foreign intelligence surveillance that NSA conducts pursuant to Section 702, alerting them that their activities have been detected by the U.S. Intelligence Community. In all cases, these disclosures would risk exceptionally grave damage to national security.

15. **(U)** For all of these reasons and others explained below, I support the DNI's assertion of the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1) to prevent the disclosure of information falling within the categories described herein. I also assert the NSA's statutory privilege under Section 6 of the National Security Agency Act, 50 U.S.C. § 3605(a), over the same information, which concerns NSA intelligence functions. The information Wikimedia seeks must be protected from disclosure and excluded from this case to avoid risking exceptionally grave damage to the national security of the United States

## IV. (U) BACKGROUND

### A. (U) The National Security Agency and Its Signals Intelligence Mission

16. **(U)** The NSA was established by Presidential Directive in 1952 as a separately organized agency within the Department of Defense. The NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate signals intelligence ("SIGINT") information, of which COMINT is a significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations. *See* Executive Order 12333, § 1.7(c), as amended.[3]

17. **(U)** SIGINT consists of three subcategories: (1) COMINT; (2) electronic intelligence ("ELINT"); and (3) foreign instrumentation signals intelligence ("FISINT"). COMINT is defined as "all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients." 18 U.S.C. § 798. COMINT includes information derived from the interception of foreign and international communications, such as voice, facsimile, and computer-to-computer information conveyed via a number of means (*e.g.*, microwave, satellite links, high frequency/very high frequency ("HF/VHF") broadcast). ELINT is technical intelligence information derived from foreign non-communications electromagnetic radiations except atomic detonation or radioactive sources—in essence, radar systems affiliated with military weapons platforms (*e.g.*, anti-ship) and civilian systems (*e.g.*, shipboard and air traffic control radars). FISINT is derived from the

[3] **(U)** Executive Order 12333, reprinted as amended in 50 U.S.C § 3001 note, generally describes the NSA's authority to collect foreign intelligence not subject to FISA's definition of electronic surveillance, including activities undertaken abroad. Section 1.7(c) of E.O. 12333, as amended, specifically authorizes the NSA to "[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information for foreign-intelligence and counterintelligence purposes to support national and departmental missions."

intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-U.S. aerospace, surface, and subsurface systems.

18. **(U)** The NSA's SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities set forth in E.O. 12333, § 1.7(c)(2), as amended, and 50 U.S.C. § 3038(b)(1). In performing its SIGINT mission, the NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications and related information. The technological infrastructure that supports the NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated electronic data collection and processing technology.

19. **(U)** There are two primary reasons for gathering and analyzing foreign intelligence information. The first, and most important, is to gain information required to direct U.S. resources as necessary to counter external threats and in support of military operations. The second reason is to obtain information necessary to the formulation and promotion of U.S. foreign policy. Foreign intelligence information provided by the NSA is thus relevant to a wide range of important issues, including military order of battle; threat warnings and readiness; cybersecurity; arms proliferation; international terrorism; counterintelligence; and foreign aspects of international narcotics trafficking.

20. **(U)** The NSA's ability to produce foreign intelligence information depends on its access to foreign and international electronic communications. Foreign intelligence produced by COMINT activities, of which NSA's acquisition of foreign communications pursuant to FISA (to include Upstream 702 collection) is a subset, is an extremely important part of the overall foreign intelligence information available to the United States and is often unobtainable by other

means. Public disclosure of either the capability to collect specific communications or the substance of the information derived from such collection itself can easily alert targets to the vulnerability of their communications. Disclosure of even a single communication holds the potential of revealing intelligence collection techniques that are applied against targets around the world. Once alerted, targets can frustrate COMINT collection by using different or new encryption techniques, by disseminating disinformation, or by utilizing a different communications link. Such evasion techniques may inhibit access to the target's communications and therefore deny the United States access to information crucial to the defense of the United States both at home and abroad. COMINT is provided special statutory protection under 18 U.S.C. § 798, which makes it a crime to knowingly disclose to an unauthorized person classified information "concerning the communication intelligence activities of the United States or any foreign government." Disclosure of the NSA's Upstream collection techniques would also negatively impact the Agency's ability to execute COMINT activities pursuant to E.O. 12333, given the overlap in the technical and operational details of both sets of collection activities.

**B. (U) External Threats to the National Security of the United States**

21. **(U)** The threat of international terrorism originally gave rise to the NSA intelligence activities challenged in this lawsuit. As a result of the unprecedented attacks of September 11, 2001, the United States found itself immediately propelled into a conflict with al Qaeda and its associated forces, and later their successors, groups that still possess the evolving capability and intention of inflicting further attacks on the United States.

22. **(~~S//NF~~)** [redacted]

[redacted]

[redacted]

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

[redacted]

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

[redacted]



25. **(U)** Protecting U.S. national security against our foreign adversaries therefore presents critical challenges for the Nation's communications intelligence capabilities. One advantage enjoyed by the NSA in meeting these challenges stems from the fact that the United States long has been and remains a critical hub for the transmission and routing of electronic

[4] **(~~S//NF~~)**

communications traveling on the global telecommunications network. Because of the United States' position as a global communications hub, hostile foreign actors often communicate using providers or services based in the United States, but, even when the NSA's foreign intelligence targets use foreign-based providers or services, their communications are often routed through the United States regardless of their country of origin or their ultimate destination. NSA SIGINT activities in the United States seek to exploit this "home field" advantage to discover and intercept our adversaries' communications in order to provide the timely, insightful, and precise intelligence needed to take decisive action against these external threats to our security.

26. (~~S//NF~~) [redacted]

[redacted]

**C. (U) Collection of Communications Content Pursuant to FISA Section 702**

27. **(U)** In July 2008, Congress enacted the Foreign Intelligence Surveillance Act Amendments Act of 2008 (the "FAA"), Pub. L. 110-261, 122 Stat. 2436. The FAA added a new section 702 to FISA, 50 U.S.C. § 1881a ("Section 702"), which created new statutory authority permitting the targeting of non-United States persons reasonably believed to be outside of the United States to acquire foreign intelligence information without individualized orders or warrants from the FISC. More specifically, Section 702 generally provides that, upon the FISC's

approval of a "certification" submitted by the Government, the Attorney General and the DNI may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a), (h).[5] Although the statute does not require the government to identify the specific facilities, places, premises, or property at which an authorized acquisition will be directed, the government must certify that an acquisition involves obtaining foreign intelligence information "from or with the assistance of an electronic communication service provider." *Id.* § 1881a(h)(2)(A)(vi).

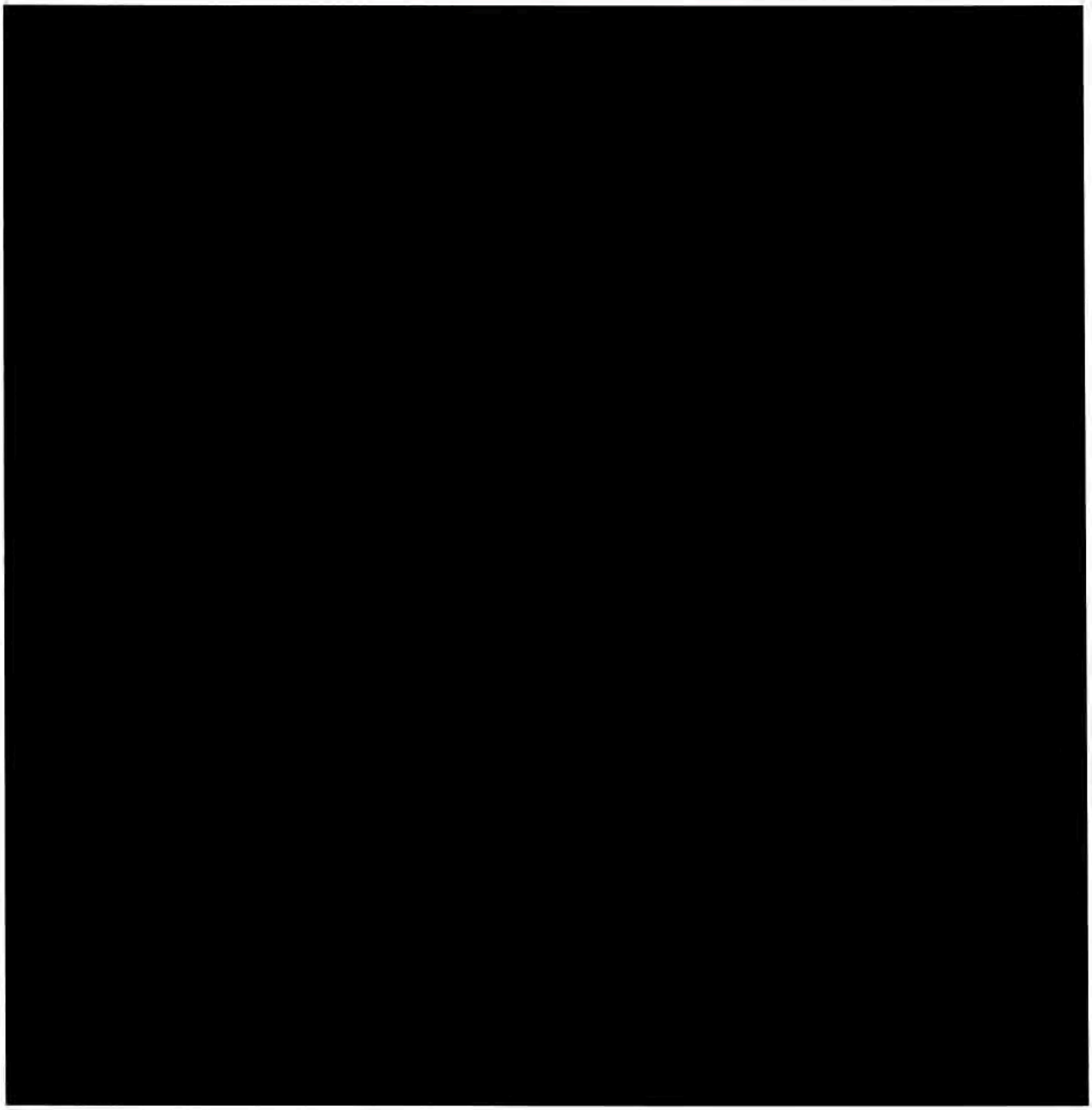
28. **(U)** Accordingly, under Section 702, the Attorney General and the DNI submit annual certifications to the FISC for its approval, as required under the statute, to authorize the targeting of non-U.S. persons reasonably believed to be located outside of the United States to acquire foreign intelligence information. These certifications identify categories of foreign intelligence information authorized for acquisition, but do not identify the particular non-U.S. persons who will be targeted. Instead, the certifications include targeting procedures, approved

[5] **(U)** Section 702 has always imposed four requirements that must be met for FISC approval of a Section 702 certification. First, the Attorney General and the DNI must certify, *inter alia*, that a significant purpose of the acquisitions is to obtain foreign-intelligence information, as that term is defined under FISA, and the FISC must find that the Attorney General and DNI's certification contains all of the required statutory elements. 50 U.S.C. § 1881a(h)(2)(A)(iv), (j)(2)(A). Second, the FISC must find that the Government's targeting procedures are reasonably designed to ensure that acquisitions conducted under the authorization are limited to targeting non-U.S. persons reasonably believed to be located outside the United States, and will not intentionally acquire communications known at the time of acquisition to be purely domestic. *Id.* § 1881a(j)(2)(B). Third, the FISC must find that the Government's minimization procedures meet FISA's requirements. *Id.* §§ 1801(h), 1821(4), 1881a(j)(2)(C). And fourth, the FISC must find that the Government's targeting and minimization procedures are consistent, not only with FISA, but also with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A). Following passage of the FISA Amendments Reauthorization Act of 2017 earlier this year, the FISC must now also find that the Government's querying procedures meet the statutory requirements and are consistent with the Fourth Amendment. *Id.* § 1881a(j)(2)(D); (j)(3)(A).

by the Attorney General, which must, among other things, be reasonably designed to ensure that any Section 702 acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of wholly domestic communications. In addition, the targeting procedures specify the manner in which the Intelligence Community determines whether a person is a non-U.S. person reasonably believed to be located outside the United States who is likely to possess, receive, or communicate foreign intelligence information authorized for acquisition by a certification.

29. ~~(S//NF)~~ [redacted]

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



[6] **(U)** Generally speaking, the Internet "backbone" refers to the interconnected networks of providers' long-haul terrestrial, fiber-optic cables that carry large volumes of Internet communications over long distances, usually between large metropolitan areas, and interchange communications traffic around the world. The Internet backbone also includes the high-capacity submarine telecommunications cables that carry Internet communications between different parts of the globe.

31. (~~S//NF~~) [redacted]

[redacted]

**D. (U) Upstream Collection**

32. (~~S//NF~~) [redacted]

[redacted]

33. (U) Over the past several years, the Government has declassified and publicly released thousands of pages of materials pertaining to Section 702 collection activities, including

Upstream surveillance, such as redacted memorandum opinions and orders issued by the FISC and certain of NSA's Section 702 targeting and minimization procedures. In addition, two Government reports have been issued that address Section 702 activities, including Upstream surveillance. In April 2014, the NSA's Civil Liberties and Privacy Office released a report on the NSA's implementation of FISA Section 702, which included a high-level unclassified description of Upstream. A short time later, in July 2014, the Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent Executive Branch agency established pursuant to statute, 42 U.S.C. section 2000ee, issued its report on the Government's implementation of Section 702, which also included an unclassified description of the Upstream program. *See* PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("PCLOB Section 702 Report").

34. **(U)** While these declassified documents and unclassified reports describe the Upstream acquisition process in general terms, they are necessarily incomplete because certain operational details of Upstream acquisition remain highly classified.

35. **(~~TS//SI//NF~~)** [redacted]

[redacted]

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

[redacted]

[redacted]

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

[redacted]

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

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

[redacted]

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

[redacted]

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

[redacted]

[10] **(U)** IP addresses identify devices on the Internet or other computer networks, and are used to route packets between destinations on a computer network. Public IP addresses are allocated to organizations (*e.g.*, companies, governments, universities, etc.), who register the basic ownership details (to include country) with a regional registry. The organizations that are allocated IP addresses may have network devices outside of the country listed in regional registry entry, thereby enabling IP addresses to be associated with network devices outside of the registered country. IP filtering refers to blocking or selecting communications to or from particular groups of IP addresses (which may include single IP addresses).

[redacted]

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

[redacted]

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

[redacted]

[redacted]

41. **(U)** It is against this backdrop that the risks of disclosing the information that Wikimedia seeks to compel the Government to reveal should be assessed.

**E. (U) The Wikimedia Discovery Requests**

42. **(U)** As discussed above, Wikimedia, seeking evidence with which to establish its legal standing to bring a legal challenge to Upstream surveillance, served 84 separate discovery requests on the Government. I am advised that Wikimedia has moved to compel further responses by the Government to 53 of those requests, and that it divides them into three categories.

43. **(U)** The first category Wikimedia describes as "direct evidence" that it "has been surveilled" in the course of Upstream surveillance, i.e., that at least some of its communications have been copied, scanned, retained, or otherwise "interacted with" by the NSA. The Government has refused to confirm or deny, however, whether the NSA has copied, scanned, retained, or otherwise "interacted with" Wikimedia communications in the course of Upstream surveillance (see Wikimedia Requests for Admission ("RFA") Nos. 34-36); has refused to confirm or deny the authenticity of purported Power Point slides that, according to Wikimedia, express NSA interest in surveilling its communications (RFA Nos. 16-21); and has refused to confirm or deny whether the NSA possesses any communications of Wikimedia's acquired in the course of Upstream surveillance, or any other documents concerning interactions with Wikimedia communications during the Upstream collection process (Wikimedia Requests for Production ("RFP") Nos. 23-24). Disclosure of this information reasonably can be expected to cause exceptionally grave damage to the national security of the United States.

44. **(U)** The second category of information that Wikimedia seeks in its motion to compel is described therein as "[k]ey terms used in describing Upstream surveillance to the public." This category includes information responsive to interrogatories asking the Government to describe its understanding of the "definitions" of a list of terms and phrases used in unclassified public documents to discuss various aspects of Upstream surveillance. *See* Wikimedia Interrogatory Nos. 1-9. In response the Government set forth its understanding of most of these terms and phrases, so far as it could do so without revealing classified information regarding the sources and methods and technical operational details of Upstream surveillance.

45. **(U)** The Government was unable to provide any unclassified response, however, to Wikimedia's Interrogatory Nos. 1 and 7. Interrogatory No. 1 sought the Government's understanding of the term "international Internet link," as used by the FISC in an October 3, 2011, memorandum opinion concerning Upstream surveillance. "International Internet link" is not a term commonly used in the telecommunications industry. The Government has its own understanding of what the FISC meant when the FISC used that term, but, because that understanding is based on still-classified portions of the FISC's October 3, 2011, opinion, the Government cannot explain its understanding of what the FISC meant by the term "international Internet link" without revealing classified information.

46. **(U)** Interrogatory No. 7 asks the Government to state its understanding of the common features of Internet packets that comprise an "Internet transaction." "Internet transaction" is also not a term commonly used in the telecommunications industry, but a term defined in the NSA's Section 702 Minimization Procedures to help explain that the NSA's Upstream collection devices do not necessarily acquire just single communications but packets of communications data that may form either a single, discrete communication, or multiple

communications. The Government, however, was unable to state the common features of the packets of data constituting an Internet transaction, as Wikimedia requested, without revealing, or tending to reveal, classified information about the design and operation of the NSA's Upstream surveillance equipment.

47. **(U)** Wikimedia also includes in its second category of discovery RFP Nos. 21 and 22, which ask the Government to produce all FISC, Foreign Intelligence Surveillance Court of Review, and Supreme Court opinions and orders concerning Upstream surveillance, and all submissions to these courts concerning Upstream surveillance,[11] since the enactment of Section 702 in July 2008, regardless of whether they include any of the information otherwise sought by the requests in this category. The Government objected to producing these documents on the grounds that, among other reasons, their disclosure could reasonably be expected to cause exceptionally grave damage to the national security of the United States. In addition, I am told that the volume of documents called for by RFP Nos. 21 and 22 exceeds 10,000 pages, and thus the Government also objected to the burden of producing unclassified versions of such a large body of classified materials.

48. **(U)** The third and largest category of discovery requests to which Wikimedia seeks to compel responses is labeled in Wikimedia's motion to compel as "Evidence concerning the scope and breadth of Upstream surveillance." The requests in this wide-ranging category ask the Government (i) to state the percentage of international Internet circuits and submarine cables that were "monitored" in the course of Upstream surveillance during each of the years 2015-2017 (Interrogatory Nos. 16-17); (ii) to admit whether the NSA conducts Upstream surveillance

[11] **(U)** The Government has not made submissions to the FISC-R or the Supreme Court specifically concerning Upstream collection and nor has either Court issued an opinion or order specifically concerning Upstream collection.

on multiple Internet backbone circuits, chokepoints, and international Internet links (RFA Nos. 13-15); (iii) to admit the authenticity of documents that, according to Wikimedia, indicate locations on the Internet backbone where the NSA conducts Upstream surveillance (RFA Nos. 25-30, 39); (iv) to state the amount of Internet communications traffic that was "filtered" and "scanned" in the course of Upstream surveillance during each of the years 2015-2017 (Interrogatory Nos. 18-19); (v) to admit whether the contents of Internet web traffic (HTTP and HTTPS communications) are now and previously were scanned in the course of Upstream surveillance (RFA Nos. 37-38); (vi) to admit whether the NSA, in conducting Upstream surveillance, copies, and reviews in bulk the contents of Internet communications that are in transit and neither to nor from Upstream surveillance targets (RFA Nos. 6-10); (vii) to describe the entire process by which the contents of Internet communications are in any way "interacted with" during the Upstream process, including any inaccuracies in the description provided in the PCLOB Section 702 Report (Interrogatory Nos. 14-15); and (viii) to identify the protocols used to encrypt Internet communications that the NSA is capable of decrypting (Interrogatory No. 20; RFA No. 40).

49. **(U)** Wikimedia also includes in this third category eight separate requests for the production of documents, seeking (i) documents sufficient to show the total number of circuits on which Upstream surveillance was conducted, the total bandwidth of those circuits, and the total number of Internet transactions acquired, during each of the years 2010-2017 (RFP Nos. 10, 13, 14); (ii) documents sufficient to show the number of "international Internet links" that were "monitored" in the course of Upstream surveillance during each of the years 2015-2017 (RFP No. 15); (iii) documents sufficient to show the number of international Internet "chokepoints" at which the NSA has allegedly conducted Upstream surveillance at any time since Section 702

was enacted in July 2008 (RFA No. 16); and (iv) the targeting procedures applied for purposes of implementing Upstream surveillance in the years 2009, 2015, and 2017 (RFP No. 18). In addition, Wikimedia includes in this "scope and breadth" category RFP Nos. 21 and 22, which call for the production of more than 10,000 pages of classified orders and opinions issued by and submissions made to the FISC, regardless of whether they contain any of the information otherwise sought in category three.

50. **(U)** The Government was able to provide partial, unclassified responses to Wikimedia's RFA Nos. 6, 8, and 10 (concerning the review of communications during the Upstream collection process), and partial responses to several of the document requests in this category. But because of the highly classified and extraordinarily sensitive nature of the documents and information sought in Wikimedia's third category of discovery requests, it was otherwise necessary for the Government to object to producing the documents and information sought in this category in order to protect classified information whose disclosure could reasonably be expected to cause exceptionally grave damage to national security.

51. **(U)** In addition to the foregoing three categories of discovery requests, Wikimedia also seeks to compel further testimony from an NSA official who was deposed on April 16, 2018, who had been designated to testify on behalf of the NSA on the following topics: (i) the definitions and meaning, as understood by the NSA, of terms that have been used in official public disclosures to describe Upstream surveillance; (ii) the ways in which the NSA (or telecommunications service providers acting on the NSA's behalf) access or interact with Internet communications in the course of Upstream surveillance; (iii) the number and type of Internet communications or transactions intercepted, accessed, copied, filtered, reviewed, screened, scanned, ingested, and/or retained by the NSA in the course of Upstream surveillance;

(iv) the number of circuits, international Internet links, and Internet backbone checkpoints on or at which the NSA conducts and has conducted Upstream surveillance; and (v) the facts related to Upstream surveillance that the NSA has disclosed, or authorized disclosure of, to the FISC, the Foreign Intelligence Surveillance Court of Review, the Supreme Court, and/or the PCLOB, and that it has subsequently declassified.

52. **(U)** The designated deponent, Rebecca J. Richards, has served as the Director of Civil Liberties and Privacy at NSA since February 2014. As NSA's Chief Transparency Officer, Ms. Richards works to communicate with the public about the value of signals intelligence and the tools NSA needs to conduct its mission, while maintaining protection over NSA's vital sources and methods. These duties and responsibilities require that she maintain a high level of familiarity with the operational details of a wide range of NSA intelligence activities, including Upstream surveillance. I have been advised that Ms. Richards was questioned for approximately seven hours on the record on topics concerning Upstream surveillance that were largely coextensive with the subjects covered by Wikimedia's written discovery requests. I understand that because the questions posed by Wikimedia's counsel consistently called for classified details about the sources, methods and operational details of Upstream surveillance, it was necessary throughout the deposition for the Government to object to Wikimedia's questions, and to withhold information, in whole or in part, in response thereto, in order to protect classified information whose disclosure could reasonably be expected to cause exceptionally grave damage to the national security of the United States.

## V. (U) INFORMATION SUBJECT TO ASSERTIONS OF PRIVILEGE

53. **(U)** As discussed above, the Government has officially declassified and publicly disclosed certain information about the existence and nature of NSA Upstream surveillance.

However, the additional information that Wikimedia seeks to compel the Government to disclose in response to its discovery requests and certain deposition questions remains properly classified, and is subject to the DNI's assertions of the state secrets privilege, to the DNI's assertion of the statutory privilege under 50 U.S.C. § 3024(i)(1), and to my own assertion herein of the NSA's statutory privilege under 50 U.S.C. § 3605(a). Although, as discussed above, I have been advised that Wikimedia divides the classified information it seeks into the three categories discussed above, for purposes of understanding the exceptionally grave risks to national security that would flow from disclosing this information, the information sought is best understood as falling into the seven separate categories identified below. For the Court's ease of reference, I note below each of Wikimedia's written discovery requests that calls for, or implicates, classified information in each category. I have been informed that the classified information that Wikimedia sought to elicit during Ms. Richards's deposition falls into all seven categories. The information encompassed by these categories would remain classified, and privileged, regardless of whether it is sought in response to pending or future discovery requests served by Wikimedia, or may become necessary for any other purposes associated with the litigation of Wikimedia's claims or the Government's defenses in this case.

54. **(U)** Accordingly, in general and unclassified terms, the DNI's assertion of the state secrets privilege, of the statutory privilege under 50 U.S.C. § 3024(i)(1), and my assertion of the NSA's statutory privilege under 50 U.S.C. § 3605(a), encompass the following categories of still-classified information and properly protected national security information concerning NSA Upstream surveillance:

A. **(U) Entities subject to Upstream surveillance activities:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that indicate or may tend to indicate whether communications of Wikimedia, and/or of other individuals and entities, have been subject to Upstream surveillance activities [RFA Nos. 16-21, 34-36; RFP Nos. 21-24];

B. **(U) Operational details of the Upstream collection process:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified technical details concerning the methods, processes, and devices employed (including the design, operation, and capabilities of the devices employed) to conduct Upstream surveillance [Interrogatory Nos. 3-5, 14, 15; RFA Nos. 6-10, 37, 38; RFP Nos. 21, 22];

C. **(U) Locations at which Upstream surveillance is conducted:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about any specific location(s), or the nature of the location(s), on the Internet backbone network(s) of U.S. electronic communication service provider(s) at which Upstream surveillance is conducted [Interrogatory Nos. 1, 2; RFA Nos. 13-15, 25-30, 39; RFP Nos. 13, 15, 16, 18, 21, 22];

D. **(U) Categories of Internet-based communications subject to Upstream surveillance activities:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about the specific types or categories of communications either subject to or acquired in the course of the Upstream collection process [Interrogatory Nos. 6-8; RFA Nos. 16-18; RFP No. 22];

E. **(U) The scope and scale on which Upstream surveillance is or has been conducted:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about (i) the volume or proportion of Internet communications traffic, including international Internet communications, either subject to or acquired in the course of the Upstream collection process, (ii) the number, proportion, and/or bandwidth of any circuit, international submarine or terrestrial cable, or other Internet backbone link, on which Upstream surveillance

is or has been conducted; and (iii) any other measure of the scope or scale on which Upstream surveillance is or has been conducted [Interrogatory Nos. 9, 16-19; RFP Nos. 10, 14];

F. **(U) NSA's cryptanalytic capabilities:** Documents and information responsive to Wikimedia's pending discovery requests, to any future discovery that Wikimedia may seek, or that may otherwise be necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this litigation, that reveal or may tend to reveal still classified information about the NSA's capability, or lack thereof, to decrypt, circumvent, or defeat specific types of communications security protocols [Interrogatory No. 20; RFA No. 40]; and

G. **(U) Additional categories of classified information contained in opinions and orders issued by, and in submissions made to, the FISC:** The additional categories of classified information contained in the documents responsive to Wikimedia RFP Nos. 21 and 22, not already encompassed by categories A-F, above, as set forth in the privilege log served by Defendant U.S. Department of Justice on March 19, 2018 [RFP Nos. 21, 22]

## VI. (U) HARM OF DISCLOSURE OF PRIVILEGED INFORMATION

### A. (U) Information Concerning Whether Communications of Wikimedia or of Other Entities or Individuals Have Been Subjected to Upstream Surveillance Activities [RFA Nos. 16-21, 34-36; RFP Nos. 21-24]

55. **(U)** The first category of information as to which I am supporting the DNI's assertions of privilege, and asserting the NSA's statutory privilege, concerns documents and information that would reveal or tend to reveal whether communications of Wikimedia or of other entities or individuals have been subject to any stage of the Upstream collection process.

56. **(U)** As discussed above, Wikimedia seeks to compel the Government to admit or deny whether the NSA has copied, reviewed the content of, and/or retained at least one Wikimedia communication in the course of Upstream surveillance; to produce any Wikimedia communications the NSA has copied, reviewed, or otherwise interacted with; and to produce any documents concerning such NSA "interaction" with Wikimedia communications. See RFA Nos. 34-36, RFP Nos. 23-24. In addition, Wikimedia seeks to compel the Government to confirm or deny the authenticity of purportedly classified documents indicating, according to Wikimedia,

that the NSA targets its communications for Upstream surveillance. RFA Nos. 16-21. These matters were also the subjects of questions propounded by Wikimedia to the NSA's designated deposition witness, who was instructed for reasons of privilege that she should not answer. Documents responsive to Wikimedia RFP Nos. 21 and 22, regarding court orders, opinions, and submissions concerning Upstream surveillance, also include information about the nature or specific identities of individual Upstream surveillance targets, and of entities about which the NSA seeks to acquire intelligence information. See, e.g., Department of Justice Privilege Log dated March 19, 2018 ("DOJ Privilege Log") at Nos. 18, 23, 29, 31. For the reasons set forth below, disclosure of such information by the NSA reasonably could be expected to cause exceptionally grave damage to national security, because it would reveal information as to whether particular entities have been subject to surveillance, as well as the nature, scope, and extent of NSA Upstream surveillance activities.

57. **(U)** As a matter of course, the NSA cannot publicly confirm or deny whether particular individuals or entities are or have been subject to intelligence-gathering activities, because to do so would tend to reveal actual targets or subjects. The harm of revealing the identities of persons or organizations who are the actual targets or subjects of foreign-intelligence gathering is relatively straightforward. If individuals or organizations knew or suspected they are targets of subjects of U.S. intelligence activities, they would naturally tend to alter their behavior to take new precautions against such scrutiny. In addition, revealing which individuals or entities are not targets or subjects of intelligence gathering would indicate who has avoided surveillance or collection, and which channels of communication may be secure. Such information could allow actual or potential adversaries, secure in the knowledge that they are not under government scrutiny, to convey information necessary or useful to the execution of hostile

acts against the United States and its interests. Alternatively, such individuals or entities may be unwittingly utilized or even forced by foreign adversaries to convey information through secure channels. Revealing which channels are free from surveillance and which are not could also reveal sensitive intelligence methods, and thereby help an adversary evade detection and capitalize on limitations in the NSA's surveillance capabilities.

58. **(U)** Similar harms would result from confirming or denying whether the communications of particular persons or entities have been subject to collection, even where it may be assumed that they are law-abiding and not likely to be actual targets or subjects of such activity. This is so because, if the NSA were to confirm that specific individuals or entities have not been targets of or subject to collection (*i.e.*, that their communications have not been intercepted), but later refuse to comment (as it would have to) in situations involving actual targets or subjects, actual or potential adversaries of the United States could then easily deduce that the persons in the latter instances are or have been targets of or subject to surveillance. In addition, disclosing whether communications of particular persons or organizations have or have not been targeted, or intercepted through the targeting of third parties, would reveal whether particular channels of communication are secure, and also reveal to third-party targets whether their own communications may be secure. Moreover, each occasion where the Government confirms (even if compelled to confirm) that certain persons or organizations have or have not been subjects of surveillance makes it more difficult in the future to withhold information about the surveillance status of other individuals or entities. This could result in a cascading effect of disclosures.

59. **(U)** To appreciate the national security risks associated with disclosing whether the NSA, through Upstream surveillance, has copied, reviewed, retained, or otherwise interacted

with Wikimedia's communications, it is necessary to understand that Wikimedia has placed three types of its communications at issue in this case: (i) online communications between Wikimedia websites and individuals who read, contribute to, or edit the contents of those websites, using the HTTPS and HTTP protocols; (ii) Wikimedia's internal "logs" of such communications with its websites, whose logs are transmitted from its servers in Amsterdam to its servers in the United States; and (iii) electronic communications of Wikimedia's U.S. staff with Wikimedia staff, contractors, and volunteers located in other countries. Disclosing (be it through admission, or the production of documents) whether Wikimedia communications have been subject to copying, reviewing, or any other alleged form of "interaction" in the Upstream collection process, would entail confirmation of whether Wikimedia's HTTPS/HTTP communications, its "log" communications, and/or its staff communications have been subjected to Upstream surveillance.

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

[redacted]

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

62. **(U)** Revealing whether the NSA, in the course of Upstream surveillance, has collected or otherwise interacted with the online communications of Wikimedia's U.S. staff, or the personnel of any organization that communicates routinely over the Internet, could reveal to targeted individuals or entities in communication with that organization that they may be subject to NSA surveillance. That is especially the case were the Government actually to produce any communications with the subject organization that it has acquired, as has been demanded here. The presence or absence, among the disclosed communications, of exchanges with targets that

had been in contact with the subject organization could alert them to surveillance of which they had been unaware, or provide assurance that their communications are secure. In either event, national security could be imperiled. The presence or absence of communications to or from particular countries could also alert other potential targets within those countries to whether NSA seeks to collect communications to or from that country.

63. **(U)** In search of "direct evidence" that its communications have been subject to Upstream surveillance, Wikimedia also demands that the Government confirm or deny whether two purportedly classified Power Point slides (reproduced on page four of its motion to compel) are in fact genuine NSA documents indicating that the NSA targets Wikimedia communications (and HTTP communications generally) for Upstream surveillance. For the reasons just discussed, including the dangers of alerting our adversaries to the types of communications on which the NSA does or does not focus its surveillance efforts, the Government cannot confirm or deny the authenticity of the so-called "NSA slides" without damaging national security.

64. **(U)** Specifically, RFA Nos. 16-18 refer to a slide, entitled: "Why are we interested in HTTP?" while RFA Nos. 19-21 relate to a slide, entitled: "Fingerprints and Appids." Wikimedia requests the Government to admit that both documents are "genuine" NSA documents containing statements by NSA "employees on matters within the scope of their employment during the course of their employment," and that these NSA employees were "authorized to make statements on the subjects of the statements within the document."

65. **(~~TS//SI//NF~~)** [redacted]

[redacted]

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

[redacted]

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

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

[redacted]

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

70. **(U)** Finally, as reflected in the DOJ Privilege Log, a substantial number of the classified orders, opinions, and court submissions concerning Upstream surveillance that are responsive to Wikimedia's RFP Nos. 21 and 22 contain information about the nature or specific identities of individual Upstream surveillance targets, and of entities about which the NSA seeks to acquire intelligence information under Section 702. For the reasons discussed herein, the Government cannot disclose such information about the nature and identities of the NSA's actual surveillance targets without risking exceptionally grave damage to national security.

71. **(U)** For all of the above-noted reasons, disclosing information tending to confirm or deny whether communications of Wikimedia, or of other entities or individuals, have been subject to any stage of the Upstream collection process could reasonably be expected to cause exceptionally grave damage to the national security of the United States.

**B. (U) Operational Details of the Upstream Collection Process**
**[Interrogatory Nos. 3-5, 14-15; RFA Nos. 6-10, 37, 38; RFP Nos. 21, 22]**

72. (~~S//NF~~) [redacted]

[redacted]

73. **(U)** As discussed above, the Government has officially acknowledged the existence of Upstream surveillance and has publicly released a limited amount of information describing, at a high level of generality, how Upstream collection operates. The Government has produced this now-unclassified information about Upstream's operation in response to Wikimedia's discovery requests. Wikimedia now seeks additional technical details about the Upstream collection process, information that remains classified in the interests of national security.

74. **(U)** Specifically, Wikimedia's Interrogatory Nos. 3-5 ask the Government to describe its understanding of the terms "filtering mechanism," "scanned," and "screened" as used to describe aspects of the Upstream collection process in previous Government filings in this case. The Government did so in its responses to the extent possible without revealing classified operational details about the Upstream collection process. Similarly, Wikimedia's RFA Nos. 6, 8, and 10 ask the Government to admit or deny that the NSA "reviews the contents of Internet communications" in various ways during Upstream surveillance. The Government also responded to these requests to the extent possible without revealing classified information. Wikimedia now insists, however, on disclosures of additional technical details about the "filtering mechanism[s]" employed and the "scann[ing]," "screen[ing]" and content review of communications during Upstream surveillance.

~~TOP SECRET//SI//ORCON/NOFORN~~

75. **(U)** The Government could provide no response to Wikimedia's Interrogatory Nos. 14-15 and RFA Nos. 7, 9, and 37-38, because any response would have required the disclosure of classified operational details about Upstream surveillance. Interrogatory No. 14 asks the Government to describe the entirety of the process by which communications are allegedly copied, filtered, scanned, or otherwise "interacted with" during Upstream collection. Interrogatory No. 15 asks the Government to identify any inaccuracies in the PCLOB's unclassified description of the Upstream collection process, which also would have necessarily required the Government to provide highly technical and classified information about any changes in the sources and methods or operational details of Upstream surveillance since the PCLOB issued its report in July 2014.

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

[redacted]

[redacted]

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

[redacted]

78. (~~S//NF~~) [redacted]

[redacted]

[12] **(U)** As described at greater length in previous filings, *e.g.*, Mem. in Supp. of Defs.' Mot. to Compel, ECF No. 126-1, to send a communication via the Internet, the transmitting device first converts the communication into one or more "packets," relatively small bundles of

[redacted]

79. **(U)** Thus, Wikimedia seeks to compel disclosures concerning classified operational details about the entirety of the Upstream collection process that would reveal to foreign adversaries the NSA's operational methods and capabilities (or lack thereof), enabling them to evade particular types of surveillance and to exploit the NSA's sources and methods of surveillance for their own purposes, in both cases risking exceptionally grave damage to national security.

80. ~~(S//NF)~~ [redacted]

---

digital information. This process is governed by the use of standardized protocols, including, for web pages, the HTTP and HTTPS protocols. Each "packet" is configured with so-called "layers" containing different types of information, some of which provide the address and routing information necessary to send the packet from its origin to its destination over the Internet. The "application layer," by contrast, generally contains a portion of the content of the original communication.

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

[redacted]

84. (~~S//NF~~) [redacted]

[redacted]

85. (~~S//NF~~) [redacted]

[redacted]

**C. (U) Location(s) on the Internet Backbone Where Upstream Surveillance Is Conducted**
**[Interrogatory Nos. 1, 2; RFA Nos. 13-15, 25-30, 39; RFP Nos. 13, 15, 16, 18, 21, 22]**

86. **(U)** I am also supporting the DNI's assertions of privilege and asserting the NSA's statutory privilege over documents and information that would tend to reveal the nature and number of the location(s) on the Internet backbone where Upstream surveillance is conducted.

87. **(U)** As discussed above, the Government has publicly acknowledged that, as part of Upstream surveillance, the NSA collects communications from one or more circuits at one or more points on the Internet backbone. However, to protect sensitive sources and methods of Upstream surveillance, and the identities of assisting electronic communication service providers, the Government has not acknowledged any further details about the number, nature, or specific locations of the sites where Upstream surveillance is conducted.

88. **(~~TS//SI//NF~~)** [redacted]

[redacted]

89. **(U)** Wikimedia Interrogatory No. 2 asks for the Government's understanding of the definition of the term "circuit," as used by the PCLOB in its Section 702 Report. In response to Interrogatory No. 2, the Government has provided an accepted definition of "circuit" as that term is used by the telecommunications industry. The NSA's designated witness also testified that the NSA has no specialized understanding of the term "circuit" that it applies in the context of Upstream surveillance, other than its accepted meaning in the telecommunications industry. In responding, however, to this request for a definition of the term "circuit," the Government has objected to providing classified information about the specific type(s) and/or location(s) of the circuit(s) on which Upstream surveillance is now or in the past has been conducted.

90. **(U)** Wikimedia RFA Nos. 13-15 ask the Government to admit that the NSA conducts Upstream surveillance on "multiple Internet backbone circuits," "multiple international Internet links," and "multiple Internet backbone chokepoints." RFP Nos. 13, 15, and 16 seek documents sufficient to show or estimate the "number of circuits," "number of international Internet links" and the "number of Internet chokepoints" at which Upstream surveillance is conducted.

91. **(~~TS//SI//NF~~)** [redacted]

[redacted]

92. **(U)** Additionally, Wikimedia's request for tens of thousands of pages of classified court orders, opinions, and submissions concerning Upstream surveillance (RFP Nos. 21 and 22) include documents identifying certain telecommunications service providers that at one time or another have been compelled to assist the NSA in Upstream collection activities.

93. **(U)** For the reasons that follow, public release of the documents and information sought by the foregoing could reasonably be expected to cause exceptionally grave damage to national security.

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

[redacted]

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

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

[redacted]

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

[redacted]

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

[redacted]

[redacted]

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

[redacted]

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

**D. (U) Categories of Internet-Based Communications Subject to Upstream Surveillance Activities**
**[Interrogatory Nos. 6-8; RFA Nos. 16-18; RFP No. 22]**

101. **(U)** I am likewise supporting the DNI's assertions of privilege, and asserting the NSA's statutory privilege, over still-classified documents and information that would reveal or tend to reveal the types of Internet communications that are subject to any stage of the Upstream collection process, and those that are not.

102. **(U)** In this regard, Wikimedia seeks to compel the Government to describe at greater, and classified, length its understanding of the terms "discrete communication," "single communication transaction" and "multi-communication transaction," and of the common features of Internet packets comprising an "Internet transaction." Interrogatory Nos. 6-8. Wikimedia's request that the Government confirm or deny the authenticity of the so-called "NSA slide" headed "Why Are We Interested in HTTP?" also implicates information in this category, as do a significant number of the court submissions concerning Upstream surveillance that are responsive to RFP No. 22. In deposition, Wikimedia also propounded questions to the NSA's designated witness (which she was instructed for reasons of privilege not to answer) concerning the categories of Internet-based communications that are subject to Upstream collection activities, including whether the devices used are configured to exclude various types of encrypted communications.

103. **(~~TS//SI//NF~~)** [redacted]

[redacted]

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

105. **(U)** So far as Wikimedia's discovery requests in this category are concerned, the first, Interrogatory No. 6, seeks the NSA's understanding of the "definition" of the term "discrete communication" as used in the NSA's 2014 Section 702 Minimization Procedures. Given the innumerable, ever-increasing, and ever-changing means by which to convey information electronically, there is no single, commonly accepted technical definition of a "communication" in the telecommunications industry, and the NSA has not developed a particularized definition of

the term that it uses in connection with Upstream surveillance, or otherwise. Therefore, in responding to Interrogatory No. 6 that the term "discrete communication" means a single communication, the Government has already given the most complete answer to this interrogatory that it is reasonably capable of providing. (To respond in any further detail would require the NSA to reveal the types of communications it collects via Upstream, which inevitably would induce our foreign adversaries to avoid those forms of online communications in order to defeat the NSA's attempts to capture their communications.) So far as Interrogatory No. 8 is concerned, the Government has already responded, straightforwardly that a "single communication transaction" is an Internet transaction containing only a single, discrete communication, and that a "multi-communication transaction" is an Internet transaction that contains multiple discrete communications. (Again, any further response would require the NSA to disclose examples of the kinds of communications it collects today via Upstream—that information is currently and properly classified.) The root of Wikimedia's dissatisfaction with the Government's responses to Interrogatory Nos. 6-8 apparently lies, therefore, with the Government's refusal to provide its understanding, in response to Interrogatory No. 7, of the common features of the Internet "packets" that constitute a single Internet transaction (or communication) for purposes of Upstream surveillance.

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

[redacted]

[redacted]

107. (~~S//NF~~) [redacted]

[redacted]

108. **(U)** Accordingly, the Government cannot disclose classified information falling within this category, whether in response to Wikimedia's pending discovery requests or otherwise, without risking exceptionally grave damage to the national security of the United States.

**E. (U) Scope and Scale of Upstream Surveillance [Interrogatory Nos. 9, 16-19; RFP Nos. 10, 14]**

109. **(U)** I am also supporting the DNI's assertions of privilege and asserting the NSA's statutory privilege over still-classified facts concerning the scope and scale of Upstream

surveillance, the disclosure of which would likely motivate foreign adversaries and others to intensify their efforts to avoid such surveillance.

110. **(U)** As discussed above, Wikimedia seeks to compel the Government to reveal the scope of its Upstream surveillance by describing (i) the "body of international communications" that is subject to the surveillance (Interrogatory No. 9); (ii) the approximate percentage of circuits and international submarine cables carrying international Internet traffic into and out of the United States that the NSA is monitoring (Interrogatory Nos. 16-17); and (iii) the approximate amount of Internet traffic subject to each stage of the Upstream process (Interrogatory Nos. 18-19). Wikimedia also seeks the disclosure of documents showing the total bandwidth of the circuits on which Upstream surveillance was conducted, and number of Internet transactions acquired by the NSA, during each of the years 2010-2017 (RFP Nos. 10, 14). These matters were also the subjects of questions propounded by Wikimedia to the NSA's designated deposition witness, which on the basis of privilege the Agency declined to answer.

111. **(~~TS//SI//NF~~)** [redacted]

[redacted]

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

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

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

[redacted]

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

[redacted]

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

[redacted]

**F. (~~S//NF~~) NSA's Capabilities, or Lack Thereof, to Decrypt, Circumvent, or Defeat Communications Security Protocols**
**[Interrogatory No. 20; RFA No. 40]**

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

[redacted]

[redacted]

118. **(U)** In particular, Wikimedia's Interrogatory No. 20 asks the Government to describe any Internet Protocols subject to Upstream surveillance that the NSA is able to decrypt. RFA No. 40 asks a related but narrower question: whether the NSA has the ability to decrypt any portion of HTTPS communications that may be subject to Upstream surveillance. Wikimedia asked similar questions during the deposition of the NSA's designated witness.

119. **(~~TS//SI//NF~~)** [redacted]

120. **(~~TS//SI//NF~~)** [redacted]

[redacted]

**G. (U) Additional Categories of Classified Information Contained in Opinions, Orders, and Court Submissions Concerning Upstream Surveillance [RFP Nos. 21-22]**

121. **(U)** Finally, as discussed herein, Wikimedia RFP Nos. 21 and 22 ask the Government to produce all FISC, Foreign Intelligence Surveillance Court of Review, and Supreme Court opinions and orders concerning Upstream surveillance, and all submissions to these courts concerning Upstream surveillance, since the enactment of Section 702 in 2008.[13] I am also supporting the DNI's assertions of privilege, and asserting the NSA's statutory privilege, over the additional categories of classified information contained in the more than 10,000 pages of documents responsive to RFP Nos. 21 and 22.

122. **(~~TS//SI//NF~~)** [redacted]

[13] **(U)** As noted earlier, neither the Foreign Intelligence Court of Review, nor the Supreme Court, has issued any opinions or orders, nor has the Government made any filings in either court, concerning Upstream surveillance.

[redacted]

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

[redacted]

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

[redacted]

[redacted]

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

[redacted]

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

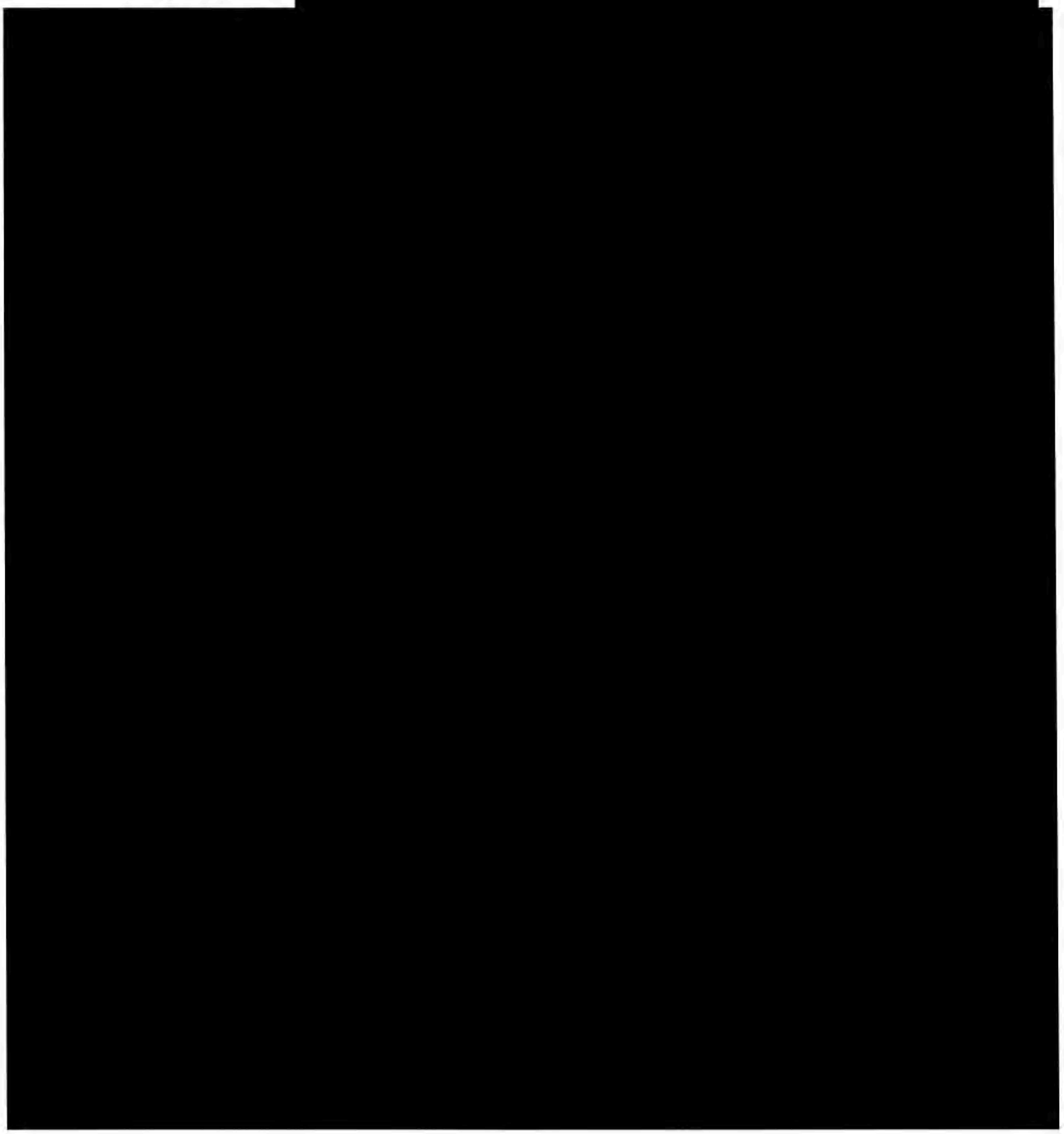
[redacted]

[redacted]

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

[redacted]

128. (~~S//OC//NF~~) [redacted]



129. (U) For the reasons discussed above, disclosure of the aforementioned categories of classified information contained in documents responsive to Wikimedia's RFP Nos. 21 and 22

could reasonably be expected to cause exceptionally grave harm to the national security of the United States.

## VII. (U) CONCLUSION

130. **(U)** Set forth in this declaration is the NSA's support for the assertion by the DNI of the state secrets privilege, of the statutory privilege under 50 U.S.C. § 3024(i)(1), and the NSA's assertion herein of the privilege under 50 U.S.C. § 3605(a), over the foregoing seven categories of classified information, whether sought in response to Wikimedia's pending discovery requests, in response to any future discovery requests Wikimedia may serve in this case, or as otherwise may become necessary for the purpose of litigating Wikimedia's claims or the Government's defenses in this case. The information contained in the above-described categories concerns critical NSA intelligence-gathering functions, is classified, and extraordinarily sensitive. Its disclosure could cause exceptionally grave damage to the national security of the United States. For the reasons explained above, I therefore support the assertion by the DNI of the state secrets privilege over this information, of the statutory privilege under 50 U.S.C. § 3024(i)(1), and I assert NSA's privilege under Section 6 of the National Security Agency Act, 50 U.S.C. § 3605(a).

~~TOP SECRET//SI//ORCON/NOFORN~~

I declare under penalty of perjury, pursuant to 28 U.S.C § 1746, that the foregoing is true and correct to the best of my knowledge and belief.

Executed on April 24, 2018

[redacted]

GEORGE C. BARNES, Deputy Director
National Security Agency

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

WIKIMEDIA FOUNDATION,

*Plaintiff*,

v.

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

*Defendants*.

Civil Action No.
15-cv-00662-TSE

**DECLARATION OF ASHLEY GORSKI IN SUPPORT OF PLAINTIFF WIKIMEDIA FOUNDATION'S MOTION TO COMPEL**

I, Ashley Gorski, a member of the Bar of the State of New York and admitted *pro hac vice* to the Bar of this Court, declare under penalty of perjury as follows:

1. I am an attorney with the American Civil Liberties Union Foundation, and represent Plaintiff Wikimedia Foundation in this matter. I submit this declaration in support of Plaintiff's Motion to Compel.

2. Attached hereto as **Exhibit 1** is a chart identifying the questions from the April 16, 2018 deposition of Defendant National Security Agency on which Plaintiff is moving to compel testimony.

3. Attached hereto as **Exhibit 2** is a true and correct copy of the redacted transcript of the April 16, 2018 deposition of Defendant National Security Agency's designated witness, Rebecca J. Richards, pursuant to Federal Rule of Civil Procedure 30(b)(6).

* * *

I declare under penalty of perjury that the foregoing is true and correct.

Ashley Gorski

Date: May 18, 2018
New York, New York

# Exhibit 1

*Wikimedia Foundation v. National Security Agency* et al.
No. 15 Civ. 00662 (TSE)

**Transcript Citations**

**Deposition of NSA Rule 30(b)(6) Witness Rebecca J. Richards**

The deposition questions fall into the three categories that Wikimedia identified in its opening brief, Pl. Br. 3–8, plus one additional category:

Category 1: Direct evidence that Wikimedia has been surveilled.[1]

Category 2: The meanings and definitions of key terms the government has used to describe Upstream surveillance to the public.

Category 3: Evidence concerning the scope and breadth of Upstream surveillance.

Category 4: Evidence rebutting speculation and hypotheticals that the government's outside expert intends to offer concerning Upstream surveillance. *See* Def. Mot. to Compel 11–14 (ECF No. 126-1).

Depending on how the Court chooses to structure its in camera review—for instance, by prioritizing straightforward admissions about the surveillance, or based on the assistance and input of the Court's own expert—Wikimedia will identify any subset(s) of questions that the Court may request.

| No. | Category 1 Excerpted Questions: Direct Evidence That Wikimedia Has Been Surveilled | Citation to Questions and Context |
|---|---|---|
| 1. | Does NSA now scan Wikimedia's communications in the course of Upstream surveillance? | Tr. 328:15-17 |
| 2. | In 2015, did NSA scan Wikimedia communications in the course of upstream surveillance? | Tr. 329:3-5 |
| 3. | Does NSA now copy Wikimedia communications in the course of upstream surveillance? | Tr. 329:11-13 |
| 4. | In June 2015, did NSA copy Wikimedia communications in the course of upstream surveillance? | Tr. 329:19-21 |
| 5. | Has NSA acquired Wikimedia communications as a result of upstream surveillance now? | Tr. 330:5-7 |

[1] Several questions in Category 4 also concern surveillance of Wikimedia specifically.

| | | |
|---|---|---|
| 6. | As of June 2015, had NSA acquired Wikimedia communications as a result of upstream surveillance? | Tr. 330:13-15 |
| 7. | If you assumed that Exhibit 54 related to upstream surveillance, it would indicate, wouldn't it, that the NSA had an intelligence interest in Wikimedia's communications, wouldn't it?<br>(Referring to Deposition Exhibit 54, NSA slide titled, "Why Are We Interested in HTTP?") | Tr. 331:15-19 |
| 8. | What is [Exhibit 55]?<br>(Referring to Deposition Exhibit 55, NSA slide titled, "Fingerprints and Appids") | Tr. 333:11 |
| 9. | If you assumed that Exhibit 55 related to upstream surveillance, it would indicate, wouldn't it, particularly on the second page in the first bullet point, that the NSA has an intelligence interest in Wikimedia's HTTP communications, wouldn't it?<br>(Referring to Deposition Exhibit 55, NSA slide titled, "Fingerprints and Appids") | Tr. 333:19-334:2 |
| 10. | Do Exhibits 54 or 55 relate to upstream surveillance?<br>(Referring to Deposition Exhibit 54, Slide titled, "Why Are We Interested in HTTP?," and Deposition Exhibit 55, NSA slide titled, "Fingerprints and Appids") | Tr. 334:8-9 |

| **No.** | **Category 2 Excerpted Questions:**<br>**The Meanings and Definitions of Key Terms** | **Citation to Questions and Context** |
|---|---|---|
| 1. | What do you understand the Foreign Intelligence Surveillance Court to mean in its use of the term "international Internet link" in that sentence?<br>(Referring to Deposition Exhibit 45, page 45, [*Redacted*], No. [Redacted], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011): "Indeed, the government readily concedes that NSA will acquire a wholly domestic 'about' communication if the transaction is routed through an international Internet link being monitored by NSA or is routed through a foreign server.") | Tr. 160:19-22 |

| | | |
|---|---|---|
| 2. | Is the NSA's understanding of the term ["international Internet link"] different from the general meaning of the term you described in response to an earlier question as a link between two countries? | Tr. 162:2-6 |
| 3. | Is it your understanding that an international Internet link is an Internet backbone circuit with one end in the United States and the other end in a foreign country? | Tr. 163:2-5 |
| 4. | In the context of upstream surveillance, can you tell me what an international chokepoint is? | Tr. 183:17-19 |
| 5. | [W]ith respect to upstream surveillance as it operated in 2015, . . . what other processes could be used to accomplished either the filtering or the screening described in the sentence you were reading from page 37 of Exhibit 43?<br><br>(Referring to Deposition Exhibit 43, Referring to Deposition Exhibit 43, Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* 37(2014), https://perma.cc/J3DZ-62HL ("PCLOB Report"):<br><br>"Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a task selector.") | Tr. 200:20-201:4 |
| 6. | Can an Internet protocol address be a selector under upstream surveillance? | Tr. 206:19-20 |
| 7. | Can a URL, or uniform resource locator, be a selector under upstream surveillance? | Tr. 207:6-8 |
| 8. | Could a URL be a selector under upstream surveillance as of June 2015? | Tr. 208:6-7 |
| 9. | What does "web activity" mean in the context of Internet communications? | Tr. 222:14-15 |
| 10. | Would Internet web browsing constitute web activity?<br><br>(Referring to Deposition Exhibit 47, page 30, June 1, 2011 FISC Submission, attached as Toomey Decl., Ex. 25 (ECF No. 125-28)) | Tr. 223:19-20 |
| 11. | I'm asking because your answer suggested that you believe "web activity" to be essentially used interchangeably with the very generic term "Internet traffic" or "Internet | Tr. 227:14-21 |

| | | |
|---|---|---|
| | communications," and I would assume, if that were the case, then the NSA would in fact use that term interchangeably, but I don't believe that to be the case. I'm asking why that is. | |
| 12. | Are the filtering or screening processes that you've described under upstream surveillance as conducted in June 2015 forms of deep packet inspection? | Tr. 244:18-21 |
| 13. | Do the Internet packets that constitute a single Internet transaction have a common destination? | Tr. 254:4-6 |
| 14. | Do the Internet packets that constitute a single Internet transaction have a common source? | Tr. 254:20-22 |
| 15. | Is an Internet transaction, as understood by the NSA, the same as a flow or network flow as used in the context of Internet communications? | Tr. 255:15-257:19 |

| **No.** | **Category 3 Excerpted Questions: Evidence Concerning the Scope and Breadth of Upstream** | **Citation to Questions and Context** |
|---|---|---|
| 1. | As of 2014, did the NSA conduct upstream surveillance on more than one Internet backbone circuit? | Tr. 123:7-9 |
| 2. | As of 2014, were multiple electronic communication service providers compelled to assist the NSA in the operation of upstream surveillance? | Tr. 126:7-128:4 |
| 3. | Can you tell us whether there have been more than one provider involved, even if not more than one at the same time? | Tr. 128:22-129:2 |
| 4. | Do you understand this sentence to confirm that service providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about task selectors as of April 16th, 2014?<br>(Referring to Deposition Exhibit 44, NSA Director Report 5:<br>"[S]ervice providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about tasked selectors.") | Tr. 132:7-133:13 |
| 5. | What is the number, or approximate number, of Internet backbone circuits on which upstream surveillance is | Tr. 145:14-18 |

| | | |
|---|---|---|
| | conducted . . . as of June 2015? | |
| 6. | What is the number, or approximate number, of Internet backbone circuits on which upstream surveillance is conducted today? | Tr. 146:10-12 |
| 7. | What is the approximate combined bandwidth of the Internet backbone circuits on which upstream surveillance was conducted in June of 2015? | Tr. 147:12-15 |
| 8. | What is the approximate combined bandwidth of the Internet backbone circuits on which upstream surveillance is conducted today? | Tr. 147:21-148:1 |
| 9. | What are the categories of circuits that were subject to upstream surveillance in June 2015? | Tr. 148:6-8 |
| 10. | What are the categories of circuits that are subject to upstream surveillance today? | Tr. 148:13-14 |
| 11. | Does the NSA conduct upstream surveillance on one or more international Internet links? | Tr. 180:2-5 |
| 12. | Did the NSA conduct upstream surveillance on one or more international Internet links in 2015? | Tr. 180:16-8 |
| 13. | Does the NSA conduct upstream surveillance today on more than one international Internet links? | Tr. 181:2-4 |
| 14. | Did the NSA conduct upstream surveillance on more than one international Internet links in June of 2015? | Tr. 181:10-12 |
| 15. | What is the number or approximate number of international Internet links on which the NSA conducted upstream surveillance in June of 2015? | Tr. 181:17-20 |
| 16. | What is the approximate number of international Internet links on which the NSA today conducts upstream surveillance? | Tr. 182:4-6 |
| 17. | Is upstream surveillance conducted on any international submarine cables? | Tr. 182:11-12 |
| 18. | Was upstream surveillance conducted on any international submarine cables in June of 2015? | Tr. 182:18-20 |
| 19. | What is the number or approximate number of cables on which the NSA conducted upstream surveillance in June | Tr. 183:3-5 |

| | | |
|---|---|---|
| | 2015? | |
| 20. | What is the number or approximate number of cables on which the NSA today conducts upstream surveillance? | Tr. 183:10-12 |
| 21. | Is upstream surveillance today conducted at one or more international chokepoints? | Tr. 184:6-8 |
| 22. | Was upstream surveillance in June 2015 conducted at one or more international chokepoints? | Tr. 184:13-15 |
| 23. | What number, approximate number, of international chokepoints was upstream surveillance conducted on in June 2015? | Tr. 184:21-185:1 |
| 24. | What number, approximate number, of international chokepoints is upstream surveillance conducted on today? | Tr. 185:6-8 |
| 25. | As of October 3rd, 2011, did the NSA conduct upstream surveillance on one or more international Internet links? | Tr. 186:11-13 |
| 26. | Do you understand th[at] sentence . . . to confirm that, as of October 3rd, 2011, that the government in fact conducted upstream surveillance at at least one international Internet link?<br>(Referring to Deposition Exhibit 45, page 45, [*Redacted*], No. [Redacted], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011):<br>"Indeed, the government readily concedes that NSA will acquire a wholly domestic 'about' communication if the transaction is routed through an international Internet link being monitored by NSA or is routed through a foreign server.") | Tr. 187:15-20 |
| 27. | Can you tell us what those certain circumstances would be in unclassified terms?<br>(Referring to Deposition Exhibit 44, NSA Director Report 5: "In certain circumstances, NSA's procedures require that it employ an Internet protocol filter to ensure that the target is located overseas.") | Tr. 194:15-16 |
| 28. | Are all transactions that were subject to upstream surveillance in June 2015 subjected to Internet protocol filtering . . . to eliminate potential domestic transactions from upstream surveillance? | Tr. 201:12-20 |
| 29. | Could you please describe all the ways in which the NSA | Tr. 202:17-20 |

| | | |
|---|---|---|
| | could determine in 2015, as part of upstream surveillance, whether a transaction is wholly domestic so as to filter it out? | |
| 30. | Were the selectors used for upstream surveillance the same as those used for PRISM surveillance in June 2015? | Tr. 208:21-209:3 |
| 31. | As of 2015, did the procedures approved by the FISC for upstream surveillance permit the NSA to collect an international HTTP transmission of a website if the text of that website contained a selector? | Tr. 219:10-14 |
| 32. | [D]id the NSA, in June of 2015, have the authority to collect the communications of a foreign target abroad with a website in the United States? | Tr. 234:5-8 |
| 33. | [U]nder upstream surveillance as conducted in 2015, did the NSA have the authority to collect the transactions of a foreigner abroad with a website in the United States if the website contained a selector task for collection? | Tr. 234:17-21 |
| 34. | Has the NSA collected webmail in-boxes as part of upstream surveillance? | Tr. 242:10-11 |
| 35. | [I]n the course of upstream surveillance, does the NSA review the contents of communications as they are in transit on the Internet backbone? | Tr. 258:15-18 |
| 36. | In the course of upstream surveillance in June 2015, did the NSA review the contents of communications as they were in transit on the Internet backbone? | Tr. 259:6-9 |
| 37. | In the course of upstream surveillance in June 2015, did the NSA scan the contents of communications as they were in transit on the Internet backbone? | Tr. 259:20-260:1 |
| 38. | [I]n June 2015, did the NSA scan the application layer data of communications that transit the Internet backbone? . . . When you say certain . . . application layer data, what you mean by "certain"? | Tr. 263:10-264:1 |
| 39. | Today does the NSA scan the application layer data of communications that transit the Internet backbone? | Tr. 266:5-7 |
| 40. | In June of 2015, if a transaction was scanned by the NSA in the course of upstream surveillance, and the NSA determined that it did not contain a selector, was the communication eliminated? | Tr. 266:15-19 |

| | | |
|---|---|---|
| 41. | Today, does the NSA seek to acquire email communications to and from its targets using upstream surveillance? | Tr. 268:15-17 |
| 42. | Could you please describe as fully as possible how, in June 2015, the NSA determined whether an Internet transaction contained a selector? | Tr. 269:3-6 |
| 43. | Beyond what you've already said or what appears in the NSA's discovery responses, could you please describe as fully as possible how the NSA today determines whether an Internet transaction contains a selector? | Tr. 269:18-22 |
| 44. | In the course of upstream surveillance in June 2015, did the NSA scan communications in bulk? | Tr. 270:14-273:9 |
| 45. | In the course of upstream surveillance today, does the NSA scan communications in bulk? | Tr. 274:8-9 |
| 46. | In the course of upstream surveillance today, does the NSA scan the metadata of communications in bulk? | Tr. 274:16-18 |
| 47. | In the course of upstream surveillance in 2015, did the NSA copy communications in bulk? | Tr. 275:2-3 |
| 48. | In the course of upstream surveillance today, does the NSA copy communications in bulk? | Tr. 275:8-9 |
| 49. | Would the NSA be permitted under upstream surveillance today to collect a target[']s communications with a U.S.-based website? | Tr. 284:4-6 |
| 50. | Can you please describe in as much detail as necessary to provide a complete answer how the NSA implemented any changes to "about" collection during or after April 2017? | Tr. 293:18-296:5 |
| 51. | [C]ould you please describe in as much detail as necessary to provide a complete answer how, after April 2017, the NSA attempts to avoid collecting communications that are solely about a selector? | Tr. 296:21-298:6 |
| 52. | [P]lease describe in as much detail as necessary to provide a complete answer how the change in April 2017 affected the filtering of communications subject to upstream surveillance? | Tr. 298:7-13 |
| 53. | [C]ould you please describe in as much detail as necessary to give a complete answer how the change in April 2017 affected the scanning of communications subject to upstream | Tr. 299:20-300:2 |

| | | |
|---|---|---|
| | surveillance? | |
| 54. | [P]lease describe in as much detail as necessary to give a complete answer which portions of an Internet transaction are scanned for selectors after April 2017? | Tr. 300:10-14 |
| 55. | Since April 2017, does the NSA first scan the contents of communications for selectors, and then discard those that are solely about a selector? | Tr. 300:20-301:1 |
| 56. | Since April 2017, does the NSA copy the contents of communications prior to scanning those communications? | Tr. 301:9-11 |
| 57. | Since April 2017, does the NSA copy the application layer data of packets prior to scanning the communications to which they belong? | Tr. 301:17-19 |
| 58. | Since April 2017, does the NSA review any portion of the contents of communications for selectors? | Tr. 302:3-5 |
| 59. | Since April 2017, does the NSA scan any portion of the contents of Internet transactions for selectors? | Tr. 303:5-7 |
| 60. | [W]hat portions of the contents of Internet transactions are scanned for selectors since April 2017? | Tr. 304:13-15 |
| 61. | Since April 2017, does the NSA scan the entire contents of Internet transactions for selectors? | Tr. 305:13-15 |
| 62. | Since April 2017, does the NSA scan any portion of the application layer data of Internet transactions for selectors? . . . And if I were to ask what portions of Internet transaction the NSA scans for selectors, would your answer be the same? | Tr. 306:2-15 |
| 63. | [S]ince April 2017, does the NSA scan the entire application layer of Internet transactions for selectors? | Tr. 306:21-307:1 |
| 64. | Are there any barriers to the NSA restarting "about" collection today? . . . [A]re there any other barriers besides the two that you just described? . . . What are those underlying issues? . . . And what were those issues? | Tr. 307:7-311:17 |
| 65. | Besides the barriers you already identified and what's described in Exhibit 51, are there any other barriers to the NSA restarting "about" collection?<br>(Referring to Deposition Exhibit 51, FISC Opinion dated | Tr. 313:17-20 |

| | | |
|---|---|---|
| | April 26, 2017, attached as Toomey Decl., Ex. 29 (ECF No. 125-32)) | |
| 66. | Has the NSA indicated to the FISC any interest in resuming "about" collection in the future? | Tr. 316:20-22 |
| 67. | Has the NSA indicated to the FISC that it intends to resume "about" collection in the future? | Tr. 317:13-15 |
| 68. | Today, does upstream surveillance involve the scanning of all international text-based communications on [the] individual circuit or circuits the NSA is monitoring? | Tr. 322:16-19 |
| 69. | In June 2015, did upstream surveillance involve the scanning of all international text-based communications on the individual circuit or circuits the NSA was monitoring? | Tr. 324:7-11 |
| 70. | Today, if some international text-based communications on a given circuit are not scanned, please explain in as much detail as necessary to completely answer why those communications are not scanned . . . [C]an you please fully explain in as much detail as necessary why some communications are not scanned? | Tr. 324:17-326:2 |
| 71. | [A]s of June 2015, if some international text-based communications on a given circuit were not scanned, please explain in as much detail as necessary to fully answer why those communications are not scanned. | Tr. 326:13-328:2 |
| 72. | At this time, HTTP communications are scanned for selectors in the course of upstream surveillance, aren't they? | Tr. 334:15-17 |
| 73. | As of June 2015, HTTP communications were scanned for selectors in the course of upstream surveillance, right? | Tr. 335:14-16 |
| 74. | At this time, HTTPS communications are scanned for selectors in the course of Upstream surveillance, aren't they? . . . Same question as to the June 2015 time frame. | Tr. 335:22-336:9 |
| 75. | Are Apache Kafka communications scanned for selectors in the course of upstream surveillance? | Tr. 336:15-17 |
| 76. | Open VPN communications are scanned for selectors in the course of upstream surveillance, aren't they? | Tr. 337:11-13 |
| 77. | As of June 2015, were open VPN communications scanned for selectors in the course of upstream surveillance? | Tr. 337:21-338:1 |

| | | |
|---|---|---|
| 78. | Other than public documents, public documents at large, hearing testimony that is transcribed, public documents you reviewed, documents that have been filed or served in this case, or your testimony today, what can you tell me about the volume of communications subject to upstream surveillance at this time using any unit of measurement you want to discuss volume of communications? | Tr. 338:8-16 |
| 79. | How many communications -- and you can use any unit of measurement you want -- did NSA retain as a result of upstream surveillance in each of the last three years? | Tr. 339:14-17 |
| 80. | What is the volume of communications copied in the course of upstream surveillance in each of the last three years? . . . Same question as to transactions. | Tr. 340:9-19 |
| 81. | What is the volume of communications or transactions that are subject to filtering in the course of upstream surveillance in the last three years? | Tr. 341:3-6 |
| 82. | [I]t's accurate . . . to say that upstream surveillance, as of June 2015, involved deep packet inspection, right? | Tr. 349:5-7 |
| 83. | Today, how many targets does NSA have for upstream surveillance? | Tr. 349:20-350:8 |
| 84. | In June 2015, how many targets did NSA have for upstream surveillance? | Tr. 351:3-4 |
| 85. | What's inaccurate about the sentence at the bottom of page 36, carrying over onto page 37, in Exhibit 43?<br>(Referring to Deposition Exhibit 43, PCLOB Report 36–37:<br>"Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet communications, what is referred to as the "Internet backbone.") | Tr. 110:4-112:3 |
| 86. | Is [the sentence] inaccurate as to the operation of upstream surveillance today?<br>(Referring to Deposition Exhibit 43, PCLOB Report 36–37, quoted above) | Tr. 115:8-22 |

| No. | Category 4 Excerpted Questions: Evidence Rebutting Defendants' Hypotheticals | Citation to Questions and Context |
|---|---|---|
| 1. | In the course of upstream surveillance in June of 2015, did the NSA deliberately attempt to filter out any of Wikimedia's international communications? | Tr. 275:14-17 |
| 2. | In the course of upstream surveillance today, does the NSA deliberately attempt to filter out any of Wikimedia's international communications? | Tr. 276:2-5 |
| 3. | In the course of upstream surveillance in June of 2015, did the NSA deliberately attempt to filter out all of Wikimedia's communications? | Tr. 276:10-12 |
| 4. | In the course of upstream surveillance today, does the NSA deliberately attempt to filter out all Wikimedia communications? | Tr. 276:17-19 |
| 5. | Does the NSA contend as a factual matter in this case that it deliberately filters out all Wikimedia communications? | Tr. 277:3-5 |
| 6. | Does anyone at the NSA know whether the NSA contends in this case, as a factual matter, that it deliberately filters out all Wikimedia communications? | Tr. 278:2-279:3 |
| 7. | Has the NSA programmed its surveillance equipment to disregard HTTPS communications altogether? | Tr. 281:1-3 |
| 8. | Does the NSA have the ability to decipher HTTPS communications? | Tr. 281:13-282:9 |
| 9. | Has the NSA configured its surveillance equipment to ignore all communications having source or destination IP addresses associated with Wikimedia? | Tr. 282:18-283:10 |
| 10. | Does the NSA deem communications to and from Wikimedia's website to be of low foreign intelligence value? | Tr. 283:19-21 |
| 11. | Could the term "foreign intelligence information" encompass information that a person surveilled using Upstream surveillance is reading on one of Wikimedia's websites? | Tr. 286:5-8 |
| 12. | [C]ould the term "foreign intelligence information" encompass information that a person surveilled using upstream surveillance is contributing to one of Wikimedia's | Tr. 288:4-289:18 |

| | | |
|---|---|---|
| | websites? . . . Could you please provide any classified information that you believe my question calls for? | |
| 13. | Today, does the NSA intentionally attempt to filter out all HTTPS communications from upstream surveillance? | Tr. 290:6-8 |
| 14. | [In] June 2015, [d]id the NSA at that time intentionally attempt to filter out all HTTPS communications from upstream surveillance? | Tr. 290:16-19 |
| 15. | Today, does the NSA intentionally attempt to filter out all Internet communications that use TCP port 443? | Tr. 291:3-5 |
| 16. | In June 2015, did the NSA intentionally attempt to filter out all Internet communications that used TCP port 443? | Tr. 291:10-12 |
| 17. | Today, does the NSA intentionally filter out all encrypted VPN communications? | Tr. 291:17-18 |
| 18. | In June 2015, did the NSA intentionally filter out all encrypted VPN communications? | Tr. 292:2-4 |
| 19. | Today, does the NSA intentionally filter out all open VPN communications? | Tr. 292:9-10 |
| 20. | In June 2015, did the NSA intentionally filter out all open VPN communications? | Tr. 292:15-17 |
| 21. | Today does the NSA intentionally filter out Wikimedia's encrypted VPN communications? | Tr. 293:2-4 |
| 22. | In June 2015, did the NSA intentionally filter out Wikimedia's encrypted VPN communications? | Tr. 293:10-12 |

# Exhibit 2

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MARYLAND

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>vs.<br><br>NATIONAL SECURITY AGENCY, et al.,<br><br>Defendants. | Case No.<br><br>1:15-cv-00662-TSE |

Deposition of REBECCA J. RICHARDS

Monday, April 16, 2018

Washington, D.C.

Reported by:

Dawn A. Jaques

Job no: 21368

Deposition of:

REBECCA J. RICHARDS,

the witness, was called for examination by counsel for the Plaintiffs, pursuant to notice, commencing at 9:12 a.m., at the offices of the Department of Justice, Civil Division, Federal Programs Branch, 20 Massachusetts Avenue, Northwest, Washington, D.C., before Dawn A. Jaques, CSR, CLR, and Notary Public in and for the District of Columbia.

APPEARANCES:

On behalf of the Plaintiffs:

ALEX ABDO, ESQ.
Knight First Amendment Institute
535 West 116th Street
314 Low Library
New York, New York 10027
PHONE: (212) 854-1128
EMAIL: alex.abdo@knightcolumbia.org

- AND -

DEVON HANLEY COOK, ESQ.
Cooley LLP
101 California Street, 5th Floor
San Francisco, CA 94111-5800
PHONE: (415) 693-2116
EMAIL: dhanleycook@cooley.com

ALSO PRESENT on behalf of Plaintiffs:

Patrick Toomey, Esq., ACLU
Ashley Gorski, Esq., ACLU

APPEARANCES (Continued):

On behalf of the Defendants:

RODNEY PATTON, ESQ.
JAMES J. GILLIGAN, ESQ.
U.S. Department of Justice
Civil Division
Federal Programs Branch
20 Massachusetts Avenue, N.W.
Washington, D.C. 20530
PHONE: (202) 305-7919 (Mr. Patton)
(202) 514-3358 (Mr. Gilligan)
EMAIL: rodney.patton@usdoj.gov
james.gilligan@usdoj.gov

ALSO PRESENT FROM THE NATIONAL SECURITY AGENCY:

JASON PADGETT, ESQ.
KATHLEEN [redacted]
(443) 479-2613
[redacted]
MARY [redacted]
(301) 688-6054
[redacted]

I-N-D-E-X


| WITNESS: | | PAGE: |
|---|---|---|
| REBECCA J. RICHARDS | | |
| | Examination by Mr. Abdo ..... | 11 |
| | Examination by Mr. Toomey ... | 257, 351 |
| | Examination by Ms. Hanley Cook ... | 327 |


E-X-H-I-B-I-T-S


| DEPOSITION EXHIBIT: | | PAGE: |
|---|---|---|
| Exhibit 41 | Notice of Deposition ..... | 18 |
| Exhibit 42 | Objections and Responses by Defendants to Plaintiff's Interrogatories ..... | 43 |
| Exhibit 43 | July 2, 2014, Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act ..... | 94 |
| Exhibit 44 | April 16, 2014, NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 ..... | 128 |
| Exhibit 45 | October 3, 2011, United States Foreign Intelligence Surveillance Court Memorandum Opinion by Judge John B. Bates NSA-WIKI 00149 - 00229 ..... | 158 |

INDEX (Continued)

E-X-H-I-B-I-T-S


| DEPOSITION EXHIBIT: | | PAGE: |
|---|---|---|
| Exhibit 46 | March 19, 2014, transcript of PCLOB Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance | 209 |
| Exhibit 47 | Notice of Filing of Government's Response to the Court's Briefing Order of May 9, 2011 NSA-WIKI 00234 - 00277 ..... | 219 |
| Exhibit 48 | The Comprehensive National Cybersecurity Initiative .... | 249 |
| Exhibit 49 | April 19, 2013, Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A) ..... | 250 |
| Exhibit 50 | March 26, 2018, Memorandum of Points and Authorities in Support of Defendants' Motion to Compel Discovery ..... | 278 |
| Exhibit 51 | April 26, 2017, United States Foreign Intelligence Surveillance Court Memorandum Opinion and Order of Judge Rosemary M. Collyer | 311 |
| Exhibit 52 | April 28, 2017, NSA Press Release "NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702" ..... | 316 |
| Exhibit 53 | April 28, 2017, Statement "NSA Stops Certain Section 702 'Upstream' Activities" ..... | 317 |

INDEX (Continued)

E-X-H-I-B-I-T-S


| DEPOSITION EXHIBIT: | | PAGE: |
|---|---|---|
| Exhibit 54 | Screenshot, "Why are we interested in HTTP?" ..... | 330 |
| Exhibit 55 | Screenshot, "Fingerprints and Appids" (2 pages) ..... | 330 |
| Exhibit 56 | January 9, 2009, Memorandum Opinion for the Counsel to the President ..... | 341 |
| Exhibit 57 | Notice of Filing of Government's Responses to FISC Questions RE: Amended 2011 Section 702 Certifications ..... | 353 |

P R O C E E D I N G S

MR. ABDO: Good morning, Ms. Richards. My name is Alex Abdo, and I'm here with the Knight First Amendment Institute and Columbia University, representing the Plaintiff in this case, Wikimedia Foundation.

I think you met everyone down the line, but I'm joined by my colleagues, Patrick Toomey from the American Civil Liberties Union; Devon Hanley Cook from Cooley LLP; and Ashley Gorski, also from the American Civil Liberties Union.

Would you just start out by stating your full name for the record and spelling it for us?

MR. PATTON: Could we just before we begin introduce the other attorneys here just for the record?

MR. ABDO: Please, yeah.

MR. PATTON: I'm Rodney Patton with the Department of Justice representing the NSA.

MR. PADGETT: Jason Padgett, the

Office of General Counsel at the National Security Agency.

MR. GILLIGAN: James Gilligan with the DOJ representing the defendants.

MS. [redacted] Mary [redacted] with the Office of General Counsel at the National Security Agency.

MS. [redacted] And Cathleen [redacted], Office of General Counsel, National Security Agency.

MR. ABDO: Great, I think we're done with appearances.

Ms. Richards, would you just state your full name and spell it for the record?

THE WITNESS: Rebecca Joan Richards, R-E-B-E-C-C-A, J. Richards, R-I-C-H-A-R-D-S.

MR. PATTON: This is Rodney Patton on behalf of Defendants in the case. The parties have agreed to the following rules governing the taking of this deposition.

One, counsel for the government may make such objections as he deems in good faith to

be necessary to prevent the unauthorized disclosure of protected, classified, or privileged information.

Two, counsel for the government may at any time direct the witness not to answer a question or to stop responding to a question if he deems it in good faith that it is necessary to prevent the unauthorized disclosure of protected, classified, or privileged information.

Number three, counsel for the government or the witness may stop the deposition at any time in order to confer privately in a Secure Compartmented Information Facility, known as a SCIF, for the purpose of preventing the unauthorized disclosure of protected, classified, or privileged information.

Four, nothing in the testimony of the witness will constitute or be construed as a waiver of the applicable protections or privileges subject to the plaintiffs -- or subject to the NSA reviewing the transcript.

Five, during the deposition, the

transcript may be displayed only on the court reporter's laptop, and it will not be otherwise transferred to or displayed on anyone else's electronic device during the deposition.

Six, after the deposition, the transcript will be transferred from the court reporter's laptop to counsel for the NSA by a CD or flash drive.

Seven, the transcript of the deposition will not otherwise be copied, except as appropriate by the NSA, or transmitted from the court reporter's laptop until counsel for the NSA provides the Agency's approval to do so.

Finally, in the meantime, the NSA will conduct a review of the transcript for protected, privileged, and classified information, and will redact any such information prior to the release of the transcript to plaintiff's counsel, or anyone other than the NSA and the court reporter.

That's all the ground rules. Thank you.

MR. ABDO: Ms. Jaques, have you sworn

Ms. Richards in? Would you mind doing so?

THE REPORTER: Raise your right hand, ma'am.

(The witness was administered the oath.)

Whereupon,

REBECCA J. RICHARDS,

was called as a witness, after having been first duly sworn by the Notary Public, was examined and testified as follows:

EXAMINATION BY COUNSEL FOR PLAINTIFF

BY MR. ABDO:

Q Ms. Richards, you understand that you're here today to give deposition testimony in the lawsuit of Wikimedia Foundation versus NSA, right?

A Yes.

Q And you understand that you're under oath?

A Yes.

Q Have you been deposed before?

A No.

Q Okay. So you heard a portion of the

procedures described by your counsel, Mr. Patton. I'll go over some other procedures for how the deposition will take place.

So we'll be asking you questions. Our questions and your answers will be recorded by Ms. Jaques. For that reason, it's important that you speak up and give your answers orally so that Ms. Jaques can record them, transcribe them. She won't be able to record a nod or a shake of the head.

Now, I may on occasion ask you a question that isn't clear, or that for some other reason you don't understand. If you don't understand one of my questions, let me know. It's my job to ask you clear questions. So if you say you don't understand one, I'll try to make it clearer. Do you understand that?

A Yes, I do.

Q Good. Your counsel may object at various points. If he does, please go ahead and answer the question that has been objected to unless your counsel specifically instructs you not

to answer. Do you understand that?

A Yes, I do.

Q We'll be taking periodic breaks during the deposition, but if you need to take a break at any other point, let us know. We will accommodate you. And I think you see that there's some water and coffee in the corner. If you need anything, just help yourself at any point during the deposition.

If at any point you realize that an answer you've given is incomplete or inaccurate and you'd like to supplement it or correct it in any way, let me know right away and we'll take care of it right then. Does that sound okay?

A Yes.

Q And if at any point in answering our questions you think of a document that would be helpful in refreshing your recollection, in answering the question, or in recalling what has been publicly disclosed and what hasn't about upstream surveillance, please tell us. We likely have many of those documents here today and would

be happy to provide you them. Is that okay?

A Yes, it is.

Q Great. So your counsel, Mr. Patton, outlined the process that the parties have agreed to for addressing objections based on information the NSA believes to be subject to the state secrets privilege or protected from disclosure under 50 U.S.C. § 3024(i)(1) and/or 50 U.S.C. § 3605(a). We will adhere to that process.

I'm going to use the term "classified" to refer to information the NSA believes is protected by any of those legal authorities. Is that okay with you --

A Yes.

Q -- that shorthand?

MR. PATTON: Can we just state for the record that not all of the information that will be protected by 3605, for example, is necessarily classified, but I understand your shorthand.

BY MR. ABDO:

Q Please take your time when answering

our questions. Our goal is not to trick you into disclosing protected information. We have a process in place to address those sorts of claims, but for that process to work, we need to make a clear record concerning any information the NSA believes is classified.

There are at least three scenarios that may arise. First, if you can answer a question fully without disclosing information that the NSA believes to be classified, you must do so.

Second, if you believe that a response to a question would disclose information the NSA considers classified, you should clearly state that for the record.

And, third, if you believe that a question calls for a response that is classified in part and unclassified in part, please also state that clearly for the record. You must answer and provide the unclassified information even if that does not constitute a complete response because there is also unclassified information.

Do you understand those three scenarios?

A Yes, I do.

Q Now, this case concerns surveillance that has taken place from 2015 to the present. Unless I say otherwise, my questions will apply to that full period.

If your answer would differ based on what specific portion of that period we're talking about, please say so, and please explain how it would differ for the relevant time frames.

We will do our best to make clear what time frame we're talking about, and then I'm sure your counsel will make sure we're making clear what time frame we're talking about, but if we haven't specified, please do your best to answer with respect to the full period.

Is there any reason you can think of why you would not be able to answer our questions fully and accurately today?

A No.

MR. PATTON: Other than that the

answers may be classified.

THE WITNESS: Yeah.

BY MR. ABDO:

Q Sorry, sorry. I mean are you taking any medications or drugs that would make it difficult for you to answer truthfully or accurately?

A No.

Q There's nothing that is affecting your memory today?

A No.

Q Okay. You stated before that you have not been deposed before; is that correct?

A That's correct.

Q Have you ever given testimony in a case?

A No, I have not.

Q Okay. You understand that you're appearing here today as a designated representative of the NSA, right?

A Yes.

(Deposition Exhibit 41 was marked for identification.)

BY MR. ABDO:

Q So you have in front of you what's been marked as Exhibit 41. Do you recognize that document marked as 41?

A Yeah.

Q What is it?

A These are the topics for examination. Do you want me to read more fully?

Q No, no, no.

A How detailed would you like me to be?

Q I'm asking whether that's the deposition notice that the plaintiff served on the defendants in this case.

A Oh, yes, it is. Sorry.

Q And you're appearing here today as a designee of the NSA on topics 2, 3, 4a, 4d and 6 as set forth in Exhibit 41; is that correct?

A Yes, that is correct.

Q Are you prepared to testify today about those topics?

A Yes, I am.
Q Can you tell us what you did to prepare?
A Reviewed the documents submitted, as well as a number of different documents that are already in the unclassified realm, ranging from previous minimization procedures, the NSA Civil Liberties and Privacy Office Report, the Privacy and Civil Liberties Oversight Board's report on 702, FISC opinions, as well as NSA's submissions at different points to the FISC.
Q The FISC opinions that you reviewed, are those all ones that have been disclosed publicly?
A Yes. I only reviewed the unclassified versions, so the redacted versions that are readily available on ODNI's website.
Q Did you also review any classified FISC opinions or other documents in preparing for today's deposition?
A No. We met with a subject -- I met with a subject matter expert. We discussed what

was classified and what was not classified, but otherwise I didn't review any classified documents.

Q So to the extent you talked about classified information, it was with a subject matter expert, but not reviewing any documents?

A Yes, that's correct.

Q Had you previously, unrelated to this litigation, reviewed classified versions of any of the documents that you reviewed in unclassified form?

A Yes.

Q Are you generally familiar with the classified portions of those documents?

A Yes, I am.

Q Did you meet with your counsel in preparing?

A I did.

Q You mentioned that you met with a subject matter expert. That's an NSA employee?

A Yes, it's an NSA employee.

Q What role does that individual have

within the NSA?

A An expert in upstream.

Q Is that the only subject matter expert within the NSA you met with?

A Yes, it is.

Q What's the general nature of what you talked about with that individual in unclassified form?

A We reviewed what was in the classified and in the unclassified to make sure we had a full understanding of how upstream worked and we were clear as to -- I was clear as to exactly where those lines, in terms of classification versus nonclassified information, could be discussed.

Q Okay. Was the primary purpose of that meeting to discuss that line between classified and unclassified information?

A It was more just to make sure that my memory from all of the work we had done over the last four years at NSA on upstream was current and understanding, and that I wasn't mixing and matching different activities.

So it was more of a verification that I knew exactly what it was, and this is what was classified and this wasn't.

Q Aside from preparing for this deposition, have you been involved in this litigation otherwise?

A No, I have not.

Q You've not reviewed any of the government submissions in this case?

MR. PATTON: Objection, vague as to time.

BY MR. ABDO:

Q You can answer the question.

A I reviewed all of the materials that have been provided, most everything in the binders. So, yes, I've read all of that material.

Q Did you review any documents before they were filed by the government in this case? Let me try that again.

Did you review any of the government submissions in this case prior to their being filed in court?

A I did not.

Q Have you been involved in any other litigation concerning Section 702 of the Foreign Intelligence Surveillance Act?

A No, I have not.

Q Are you familiar with other litigation concerning Section 702?

A I am.

Q What other litigation are you familiar with?

A There's at least one other lawsuit having to do -- that goes back quite a few years, sometimes referred to as the Jewel litigation.

Q Okay. So what's your current position at the NSA?

A I'm the Director of the Civil Liberties, Privacy, and Transparency Office.

Q How long have you been in that position?

A A little over four years.

Q What are your roles and responsibilities in that position?

A I set up the office four years ago, and I report directly to the Director of NSA. I'm an adviser on civil liberties, privacy, transparency issues to both the Director, as well as our Senior Leadership Team.

I review programs to identify civil liberties and privacy risks. I identify ways to mitigate them. I also work on transparency issues, publishing reports, meeting with civil society/non-governmental organizations, and then also act as the privacy advocate for NSA agency employees.

Q Are you responsible for that office's oversight of upstream surveillance?

A Could you clarify? I'm not sure what you mean by oversight of that.

Q Sure. Are you involved in your position in reviewing the operation of upstream surveillance as part of that office's mission?

MR. PATTON: Objection, vague.

You can answer.

THE WITNESS: My office reviews the

compliance incidents or other reports, oversight reports, as part of our role as information goes from NSA to ODNI.

BY MR. ABDO:

Q I just want to clarify that last portion. You said as part of your role, information goes from --

A ODNI. So -- sorry.

Our office is at a more strategic level, so we do not review every single compliance incident or every single activity specifically. We have a compliance group that does those types of functions.

My office is more strategic, so as specific reports or assessments are conducted either by ODNI or the Department of Justice, we're in that review process.

I'm also the main interlocutor with the Privacy and Civil Liberties Oversight Board, so to the extent that there are compliance incidences or changes to what -- any changes to how NSA is conducting its mission as it relates to

counterterrorism, we provide that type of information and those types of briefings to the PCLOB.

Q So in that role, you're not involved in the implementation of upstream surveillance?

MR. PATTON: Objection, vague.

THE WITNESS: So certainly at the -- there are decisions that are being made, we're informed, we will help decide, help with providing recommendations about whether it should go A or B or C, depending on specific questions that arise.

I'm not sure I'm answering your -- I'm not sure I'm fully understanding what you're trying to get at.

BY MR. ABDO:

Q Let me try to be clear.

When the government applies for authority from the Foreign Intelligence Surveillance Court to conduct upstream surveillance, is your office involved in that process?

A Yes.

Q And what's the nature of your office's involvement in that process?

A We review the minimum -- the proposed -- we will review any of the procedures. We will review any of the materials to ensure that we think that privacy has been properly protected, and civil liberties.

Q And that review happens prior to submission of an application to the Foreign Intelligence Surveillance Court?

MR. PATTON: Objection, vague.

You can answer.

THE WITNESS: Ask the question again.

BY MR. ABDO:

Q Sure. When the government is applying for authority to conduct surveillance under Section 702 of FISA -- are you familiar with the shorthand FISA for Foreign Intelligence Surveillance Act?

A I am.

MR. PATTON: Could I just interrupt?

I keep objecting to vague because

we're talking about 702, but there's PRISM and Upstream, and so if you want to be more specific, that's the nature of my objection.

MR. ABDO: That's helpful. Thanks, Rodney.

BY MR. ABDO:

Q When the government is applying for authority to conduct upstream surveillance from the Foreign Intelligence Surveillance Court, does your office review those applications prior to their submission to the Foreign Intelligence Surveillance Court?

A I understand. Hold on. Sorry, I'm looking for something specific to make sure I'm --

MR. PATTON: Take your time.

THE WITNESS: Can I talk -- take a break to make sure?

MR. PATTON: Sure.

BY MR. ABDO:

Q I just want to be clear. Just two quick things. Could you please first identify what you're looking at just for the record?

A I'm looking at the Objections and Responses by Defendant National Security Agency and Admiral Michael S. Rogers, Director, Plaintiffs' First and Second Sets of Requests for Admission.

Q And could you tell us whether you're looking to take a break to discuss classified versus unclassified information, or something else? Are you looking to discuss with your counsel the line between classified and unclassified information?

A Yes.

Q Okay. I think let me actually just withdraw that question. I don't think we need to take the time to go there.

MR. PATTON: Just to be clear to Mr. Abdo's point, the purpose of taking a break is not to talk about whatever the response is if it's not a subject of privilege.

The time to take a break and the need to take a break is related to whether to assert the privilege, and the nature and scope of the

privilege.

MR. ABDO: Thanks.

BY MR. ABDO:

Q You said that you had been in your current position for four and a half years?

A Yes.

Q Before that, were you also with the federal government?

A Yes.

Q And what position did you hold before your current one?

A I was the Senior Director for Privacy Compliance at the Department of Homeland Security in the Privacy Office.

Q How long were you in that position?

A Just shy of ten years.

Q And what were your roles and responsibilities there?

A I was in charge of developing the Privacy Impact Assessment process, publishing Privacy Act System of Records Notices, ensuring that the review of all IT systems within the

Department of Homeland Security had been reviewed for privacy considerations.

Q As part of that job, were you involved in any way in upstream surveillance?

A No.

Q As far as you know, did your roles or responsibilities in that job have any bearing on this lawsuit?

A No, not to the best of my knowledge.

Q Can you just briefly explain what a Privacy Impact Assessment is?

A Sure. It's a requirement of both the E-Government Act of 2002, as well as the Homeland Security Act, Section 222, which requires that the chief privacy officer ensure technology sustains and does not erode privacy.

It's the process by which the Department of Homeland Security and other federal agencies review technology to ensure they understand what the impact would be on privacy and how they might be able to mitigate it.

It's also a transparency document to

allow the public to know and understand what the agency is doing with their information.

Q And you were involved in the issuance of those sorts of assessments when you were at the Department of Homeland Security?

A Yes.

Q Prior to holding that position, were you also in the federal government?

A No. I worked for a small nonprofit called TRUSTe, which at the time was a nonprofit reviewing privacy policies and issuing seals of approval at the bottom of websites -- or generally seen at the bottom of websites, indicating that the privacy policy can be trusted.

Q How long were you in that position?

A I think about three years, maybe a little more, maybe a little less.

Q Were the two jobs within the federal government that you've discussed so far the only two jobs you've held in the federal government?

A No. Prior to working at TRUSTe, I worked at the Department of Commerce in the

e-commerce task force helping to negotiate the Safe Harbor Accord, which is the privacy agreement between the European Commission and the Department of Commerce for companies regulated by the Federal Trade Commission or the Department of Transportation to be able to transfer data from the EU to the US if they've agreed to a set of privacy policies.

Q What was your position then?

A I was the intern.

Q How long did you have that internship?

MR. PATTON: Don't knock it.

THE WITNESS: Don't knock it, man.

MR. ABDO: We all did.

THE WITNESS: I was there for a year. During that time frame, I went from being there called a co-op student, which means I was paid, to a full-time employee.

BY MR. ABDO:

Q But the full time you were there was one year?

A Yeah.

Q Okay. Is that the only other job you've had in the federal government?
A Yes.
Q Did that job in any way concern upstream surveillance?
A No. It was before upstream surveillance existed.
Q Can you describe your training in the areas of computer science, computer engineering, telecommunications networks, or network surveillance prior to joining the NSA?
A I do not have --
MR. PATTON: Object. Object to form, relevance.
MR. ABDO: You can answer.
MR. PATTON: You can answer.
THE WITNESS: Okay. I don't have any specific training on those four topics prior to being at NSA.
BY MR. ABDO:
Q Do you have any formal technical training from your -- let me try to be clear.

Do you have any training with respect to those four topics through, you know, college or any other graduate programs?

A No, I do not.

Q Do you have any familiarity with those topics from your time prior to joining the NSA?

MR. PATTON: Objection, vague.

THE WITNESS: Certainly my experience of working on Privacy Impact Assessments at the Department of Homeland Security, as well as working through different Internet activities, has given me a great deal of on-the-job experience.

I have no formal training to speak of in computer science or the other topics you've mentioned.

BY MR. ABDO:

Q Can you describe the on-the-job training you got in your position at the Department of Homeland Security on those four topics? And let me just be clear, on the topics of computer science, computer engineering, telecommunications networks, or network

surveillance.

A The first three are all part of the process by which we were having to review extensively the types of technology that DHS was putting forward and better understanding them to ensure we understood the privacy implications. So how did the computer systems work? Sort of how was the information being moved? Where was the information being moved?

I have no formal experience beyond my work at NSA on network surveillance.

Q For your time still at the Department of Homeland Security, would you consult with technologists to better understand how the conduct that you were reviewing might impact privacy?

A Absolutely.

Q Was that a frequent part of your job?

A Yes. We worked very closely with the chief information officer, the chief information security officer.

We also had external experts to the Department of Homeland Security who did have

experience in all of these different topics who would provide external expertise as part of the Federal Advisory Committee Act, or FACA.

All of those were available if we had questions to ensure that both we were fully understanding the privacy impact, that we had an appreciation of the information we needed to, and were getting those expertise from across -- wherever in DHS we needed.

Q You said that network surveillance was not a topic on which you received on-the-job training during your time at DHS?

A Correct.

Q Is that because there were no network surveillance programs that your office was called upon to review at your time at DHS?

MR. PATTON: Objection.

THE WITNESS: I need --

MR. PATTON: Just a second.

Objection. I'm not sure of the relevance of that particular question, but besides that, it is vague, ambiguous, but the witness can

answer.

THE WITNESS: We're now hitting into an area of classification that I would need to go and discuss any further conversation on this having to do with DHS activities.

BY MR. ABDO:

Q Let me take a step back then.

You said before that you hadn't received any on-the-job training with respect to network surveillance during your time at DHS.

That's correct, right?

A Maybe a better way would be if you could explain what you mean by "network surveillance," and then I can better answer that question.

Q Sure. I mean the use of computers to monitor communications over a telecommunications network.

A I think what I would like to do is revise what my answer is to say that, yes, I did have on-the-job training associated with that, and to go any further into that likely is classified.

Q Okay. I don't think we need to go further.

A Okay.

Q I just wanted to understand the nature of your technical training prior to your joining the NSA.

A Okay.

Q So now let's move to your time at the NSA. Can you describe in unclassified terms your on-the-job training with respect to those four areas, which again are computer science, computer engineering, telecommunications networks, or network surveillance?

MR. PATTON: Objection to the question to the extent it calls for source and methods of the NSA, operational details of Upstream, which are protected by the state secrets privilege and 50 U.S.C. § 3605(a), 50 U.S.C. § 3024(i)(1).

The witness can answer the question to the extent that it's unclassified.

MR. ABDO: And to be clear here, I'm asking just for unclassified information.

And, Rodney, can we agree on a short form of your invocation of the state secrets privilege and the other two statutory claims of protection?

MR. PATTON: I will work on that. We can maybe make a deal that you will shorten your record and I'll shorten mine.

But my concern with in unclassified terms is it may be very difficult for the witness to separate out when it's a broad question like that as opposed to a very specific question.

MR. ABDO: If instead of using the term "classified" we used the term "protected," would that be clearer?

MR. PATTON: For me I think it's just the tell me about everything nature of the question, which is very difficult for her to come up with what is classified and what is unclassified on the spot, whereas specific questions are much easier where she's -- you know, her job is to know where the line is, and she knows where the line is.

This is asking about her entire thing, so that's my concern.

BY MR. ABDO:

Q Ms. Richards, do you think you can answer my question without disclosing classified information?

A I can answer. I'm not sure it will give you what you're looking for, but ...

Q Why don't we start with what you can do.

A My answer is I have extensive ability to talk to and learn from anyone within NSA about how we do our job. To the extent that it means I'm interacting with people in all four of those categories, that's what I do.

Q Do you consider yourself to be well technically versed or conversant in those four areas?

MR. PATTON: Object to the form.

MR. ABDO: You can answer.

THE WITNESS: I do.

BY MR. ABDO:

Q I think that's fine.

As part of your job at NSA, have you ever been required to learn technical concepts relating to the programs you were reviewing that you felt unable to learn or understand?

MR. PATTON: Object to the form.

THE WITNESS: I don't understand your question, so help me.

BY MR. ABDO:

Q Sure, yeah. Your job at NSA involves reviewing NSA surveillance programs, correct?

A Correct.

MR. PATTON: Object to the form.

THE WITNESS: Correct.

BY MR. ABDO:

Q And as part of reviewing those programs, you mentioned that you talk with NSA employees about how those programs work; is that right?

A Yes.

Q When talking with those employees

about NSA surveillance programs, have you ever felt unable to comprehend technical detail that you were being explained?

MR. PATTON: Object to the form, vague. You can answer.

THE WITNESS: No, I have never felt like I couldn't understand what they were saying, or what the concepts that they were explaining to me. Is that what you're asking me?

BY MR. ABDO:

Q Yeah, that's what I'm asking you.

A Okay. No, I've never had -- they have all been able to fully explain it, both in concept and in fact.

Q Okay, great.

(Deposition Exhibit 42 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you now have in front of you what's been marked as Exhibit 42.

Do you recognize Exhibit 42?

A Yes, I do.

Q What is it?

A It is Objections and Responses by Defendants National Security Agency and Admiral Michael F. Rogers, Director, to Plaintiff's Interrogatories.

Q Could you please turn to page 17 of Exhibit 42 and read to yourself the question identified on that page as Interrogatory No. 12?

A (Witness reviewing document.)

Q Have you had a chance, Ms. Richards, to read just the interrogatory, the question itself, No. 12 on page 17?

A I'm sorry. Yes, I have.

Q Could you turn to page 18 of the same document, Exhibit 42, and read the paragraph on that page identified as RESPONSE, which is the response to Interrogatory No. 12 provided by the NSA, and let me know when you're done.

A (Witness reviewing document.) Okay.

Q Did you have any role in drafting or reviewing the NSA's response to Interrogatory No. 12?

MR. PATTON: Object to the form, vague as to time.

THE WITNESS: No, I did not.

BY MR. ABDO:

Q You didn't draft the response?

A I did not draft the response.

Q Did you see this response prior to its having been filed in federal court -- sorry, prior to this having been sent to the Plaintiffs in this lawsuit?

A No.

Q Since this response was provided to Plaintiff, have you reviewed this response?

A Yes.

Q And do you understand this response?

A Yes.

Q To your understanding, does the term "Internet backbone" include high-speed, ultra-high bandwidth data transmission lines between the networks of major Internet service providers?

MR. PATTON: Objection, calls for expert testimony of a telecommunications computer

expert. You can answer.

THE WITNESS: Certainly that is one example of what might be included in the Internet backbone.

BY MR. ABDO:

Q When you say -- what do you mean by "might be"?

A Well, as is noted in the definition, and as is actually when it first comes up in the testimony to the PCLOB, Internet backbone is a -- sort of for want of a better word, there's not a specific term that everyone turns to and says that is the Internet backbone, but rather is a general description.

And so there are a number of things, as is described here, that could be included in the Internet backbone. It's not yes or no.

Q But your understanding is that the high-speed, ultra-high bandwidth data transmission lines between the networks of major Internet service providers are one such example?

A Those could be one such example.

Q And the Internet backbone also includes high-speed, ultra-high bandwidth data transmission lines within the networks of major Internet service providers?

MR. PATTON: Objection to form, calls for expert testimony. You can answer.

THE WITNESS: You're making a distinction between within versus --

BY MR. ABDO:

Q Between, that's right.

A So with -- you're --

Q Sorry. My first set of questions related to data transmission lines between the networks of major Internet service providers -- in other words, those connecting one major Internet service provider to another -- and now I'm asking about the high-speed, ultra-high bandwidth data transmission lines within any given major Internet service provider.

MR. PATTON: Objection, calls for expert testimony. You can answer.

THE WITNESS: It certainly may be. I

wouldn't say -- it could be an example.

BY MR. ABDO:

Q Can you give other examples of high-speed, high bandwidth data transmission lines that would be part of the Internet backbone?

MR. PATTON: Objection, calls for expert testimony. You can answer.

THE WITNESS: There's the terrestrial and undersea circuits are other examples.

BY MR. ABDO:

Q Could you describe just a little bit more what you mean by those?

MR. PATTON: Same objection.

THE WITNESS: So both with Internet backbone, as well as terrestrial and undersea circuits, NSA doesn't have a specific NSA definition. It's what would be generally accepted by a telecom expert. So there's nothing special about what those are.

BY MR. ABDO:

Q And I'm not asking for a special definition of Internet backbone. I'm asking

whether your understanding of that term would encompass the sort of data transmission lines we were just discussing.

MR. PATTON: Objection to form, vague, and calls for expert opinion.

THE WITNESS: So I guess my answer hasn't changed, and to go any further would put us into classified information.

And so to the extent that the information you have in the response -- there's no additional information that is -- I can switch words around, but in essence, those are different types of examples that could be part of what the Internet backbone is, but there's no additional information I can provide to you that's not classified.

BY MR. ABDO:

Q I understand that you may not be able to provide an unclassified response to this question, but could you state whether the NSA considers high-speed, ultra-high bandwidth data transmission lines between and within the networks

of major Internet service providers to be part of the Internet backbone for purposes of upstream surveillance?

MR. PATTON: Objection, asked and answered. Objection, calls for expert testimony. And also objection that it is calling for classified information and information protected by the previously mentioned statutes, so I'll instruct the witness not to answer that question.

BY MR. ABDO:

Q Are you going to follow your lawyer's instruction not to answer the question?

A Yes.

MR. ABDO: Rodney, can we agree that every time you instruct Ms. Richards not to answer a question on the basis of its classification, you will consider us to have noted our objection to it and we can move on?

MR. PATTON: Absolutely.

MR. ABDO: Okay.

MR. PATTON: I mean, there may be other ways to ask the question to get around that.

That's part of the problem.

MR. PADGETT: Maybe we should take a break because I think there is something that could be said, but the question is throwing it off.

MR. PATTON: Right, that's what I was just saying. There may be an answer to the question, depending on how it's phrased, that we could provide an unclassified response, and so we want to try and provide as much of an unclassified response as possible, but the way the question is framed leads us into a classified area.

MR. ABDO: Let me try to ask it one other way.

BY MR. ABDO:

Q Is your understanding that telecommunications networks experts would consider the high-speed, high-bandwidth data transmission lines between and within the networks of major Internet service providers to be part of the Internet backbone?

MR. PATTON: Just take a pause.

(Counsel conferring.)

MR. PATTON: Just object to the form in terms of calling for expert testimony, but you can answer that question.

Do you need the question read back?

MR. ABDO: We can do that if that's easier.

THE WITNESS: Yeah, can you read the question one more time? Sorry. Too many things.

(The reporter read back the question.)

THE WITNESS: I think generally speaking, yes.

MR. ABDO: Rodney, if you want to take a -- if there's more you think that can be provided after a short break, we're happy to do that now.

MR. PADGETT: It might be helpful.

MR. GILLIGAN: Actually, 30 seconds.

MR. ABDO: Go off the record.

(Off the record at 10:02 a.m.)

(Resume at 10:05 a.m.)

MR. PATTON: So we've clarified the

lines as to where the privileged information in that line of questioning is, so you can ask your next question, hopefully get a response.

BY MR. ABDO:

Q Sure. Is there a way that I could have asked the last set of questions I was asking in a way that you could answer with unclassified information?

A To the extent the term "Internet backbone" is what is generally understood, as amorphous as that definition is, by a telecommunications expert, that's how NSA would describe it.

To the extent you are connecting it in some way to upstream, that's where you get to classified information.

So they're sort of differentiating between those two, but NSA doesn't have a special definition.

Q Right. And I think you answered the question with respect to the term "Internet backbone" as understood by telecommunications

networks professionals or experts, but just to be clear, that term, as used by telecommunications networks experts, includes the high-speed, ultra-high bandwidth data transmission lines between and within the networks of major Internet service providers, right?

A Yes.

MR. PATTON: Objection to the extent it calls for an expert opinion.

THE WITNESS: But generally yes, that would be what I believe they would say, and so that would be what NSA would say.

BY MR. ABDO:

Q Okay. Going back to the NSA's response to Interrogatory 12, what does the term "data transmission lines" refer to?

MR. PATTON: Objection, calls for expert opinion.

THE WITNESS: Lines that transmit data. I mean, beyond what a tele- -- so I'm not a telecommunications expert, as we've noted. That doesn't mean I don't understand how they work, but

there's no special definition here that is distinct to what NSA does.

BY MR. ABDO:

Q What I'm getting at is does the term "data transmission lines" refer to the physical means of transmission of data, or something else?

MR. PATTON: Same objection.

THE WITNESS: I will go back to that it has no special particular meaning beyond what a telecommunications expert would expect.

BY MR. ABDO:

Q Is your understanding that a telecommunications network expert will use that term, "data transmission lines," to refer to a physical means of transmission, such as, for example, a cable or a wire or an optical fiber?

MR. PATTON: Object. Object to the form, vague, and calls for expert testimony.

You can answer.

THE WITNESS: As opposed to?

BY MR. ABDO:

Q As opposed to logical or virtual

groupings of data transmitted from one point to another.

MR. PATTON: Same objections.

BY MR. ABDO:

Q I'm really just trying to understand the term that you've used in your response to Interrogatory No. 12, and the term is "data transmission lines," and what I'm trying to understand is whether that refers to physical lines of transmitting data, or other ways of transmitting -- other ways of understanding the transmission of data.

A Oh, okay.

Q Do you understand that question and what I'm trying to understand?

A Do you want to go a little further? What would be the -- I guess I'm tripping over this seems to be logical on its face, and so I'm not sure -- I'm having a hard time -- it sort of defines itself, so ...

Q So in another interrogatory response, the NSA uses the term "virtual circuit." I'm

trying to understand whether this term, "data transmission lines," is limited to physical transmission lines or something else, like virtual circuits?

MR. PATTON: Object to the form, calls for expert testimony.

THE WITNESS: Do you want to point to where virtual circuits is so I can make sure I'm not tripping up or -- I do remember seeing virtual circuits, I just don't --

BY MR. ABDO:

Q Turn to page --

A I want to make sure I'm looking at the same one that you're looking at.

Q If you turn to page 6 of Exhibit 42, it's the response to Interrogatory No. 2, designated on that page by the all caps word RESPONSE.

Do you want to take a second to read those two paragraphs to yourself?

A Yeah. (Witness reviewing document.)

Oh, okay.

Q Having read that, do you now understand what I'm asking with respect to the term "data transmission lines"?

A Yeah, it's physical data transmission lines. There's nothing -- there's nothing virtual or -- there's nothing -- it's a physical transmission line.

Q Okay, okay. Would a fiberoptic cable qualify as a data transmission line as that term is understood by telecommunications network experts?

MR. PATTON: Objection, calls for testimony by a telecommunications expert.

You can answer.

THE WITNESS: Yes, it would. That would be one example. I'm not saying that's the only example, but it's certainly an example of what might be included in that.

BY MR. ABDO:

Q Okay. Would it also include -- let me phrase the question fully.

Would the term "data transmission

line" also include optical fibers within a fiberoptic cable as that term is used by telecommunications networks and network professionals?

MR. PATTON: Objection to the extent it calls for testimony by those telecommunications experts. You can answer.

THE WITNESS: To the extent that's an example of what might be included in that, yes.

BY MR. ABDO:

Q Would a fiberoptic cable be a data transmission line as that term is understood by the NSA?

MR. PATTON: Same objection.

THE WITNESS: Can you repeat the question? I'm not sure I understood.

BY MR. ABDO:

Q Sure. Does the term "data transmission line," as the NSA has used it in response to Interrogatory 12, include fiberoptic cables?

MR. PATTON: Objection to the extent

it calls for expert testimony. You can answer.

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. And the same is true of --

A It's an example. I mean, all of these are examples. NSA doesn't have a special definition for "Internet backbone" or these other well-known telecom-like words that you're bringing up, data transmission line or fiberoptic line.

Q Does the term "data transmission line," again as used in the response to Interrogatory 12, include individual wavelengths of light carried over fiberoptic cables?

MR. PATTON: Object to the form to the extent it calls for expert testimony.

You can answer.

THE WITNESS: Certainly it is an example.

BY MR. ABDO:

Q Would the term include any subdivisions of a wavelength of light carried over a fiberoptic cable?

MR. PATTON: Same objections.

You can answer.

THE WITNESS: Would the subdivision of the light?

BY MR. ABDO:

Q Would any subdivisions of a wavelength of light carried over a fiberoptic cable constitute a data transmission line as the NSA has used that term in responding to Interrogatory 12?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: So to the extent that any of those are an example of what might be part of the Internet backbone, in which case it's providing high-speed, ultra-high bandwidth data transmission lines, the answer would be yes.

MR. ABDO: Okay. Do you mind if we take a five-minute break to use the restroom?

MR. PATTON: No.

(A break was taken at 10:15 a.m.)

(Resume at 10:25 a.m.)

BY MR. ABDO:

Q Ms. Richards, where do you acquire your understanding of the term "Internet backbone"?

A From both experts within NSA, as well as talking to -- or actually reading what's, you know, sort of been written on it in telecommunications just sort of generally.

Q Did you talk to anyone at the NSA about the meaning of the term "Internet backbone" in preparing for this deposition?

MR. PATTON: Objection to the question to the extent it calls for attorney-client privilege or any classified information, but you can answer to the extent that it is not attorney-client privileged.

THE WITNESS: Certainly in preparation for this we reviewed the definitions that have been provided to ensure that I understood them and that nothing had changed.

BY MR. ABDO:

Q Did you talk with any subject matter

experts at the NSA about the meaning of the term "Internet backbone"?

A Yes, I did.

Q Did you talk to them about anything beyond what was provided by the NSA in response to Interrogatory 12 asking for the definition of "Internet backbone"?

MR. PATTON: Object to the form, vague.

THE WITNESS: We discussed the definition and understood it to be the same as the definition that a subject matter expert in the telecommunications industry would use.

I'm not sure I'm understanding or answering what you're asking me.

BY MR. ABDO:

Q Did you talk about the terms used in the definition provided of the term "Internet backbone"?

A Yes.

Q You understand that the definition of the term "Internet backbone" is one of the terms

listed in topic 2 of the deposition notice of the case?

A Yes.

Q And you understand that the NSA has an obligation under the federal rules to provide somebody for this deposition who knows the Agency's understanding of that term?

A Yes.

MR. PATTON: Object to the extent it calls for a legal conclusion.

Just wait for my objection --

THE WITNESS: Sorry.

MR. PATTON: -- or non-objection.

BY MR. ABDO:

Q So you understand what I'm asking about? When I'm asking about the NSA's understanding of certain terms, I'm asking for the NSA's understanding, as you're a designee of the NSA today.

A Yes.

Q Okay. I want to move to a different term used in your definition.

The definition or use of the term "large, strategically interconnected computer network," what does that term mean?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: The words have no specific meaning beyond what you would expect from a telecommunications expert.

They're large, they're strategically connected, and they're computer networks. Perhaps when we --

BY MR. ABDO:

Q Is that the -- well, let me ask by example. Would that term, "large, strategically interconnected computer networks," include the networks of major Internet service providers inside the United States?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: To the extent that that might be one example of what would be included in the Internet backbone, yes, that's an example.

BY MR. ABDO:

Q I'm not sure I understood the first part of your response. Is it or is it not -- sorry, let me start that over.

Would or would not a network of a major Internet service provider constitute a large, strategically interconnected computer network as the NSA has used that term?

MR. PATTON: Object to the form to the extent it calls for expert testimony.

You can answer.

THE WITNESS: Let me clarify what I think you're asking to make sure I understand.

You're saying would a large -- I'm sorry, a communications provider in the United States be considered a strategically interconnected computer network?

BY MR. ABDO:

Q Yes.

A Yes.

Q Okay. Approximately how many data transmission lines are there that satisfy the

definition of "Internet backbone" given by the NSA?

MR. PATTON: Object to the form to the extent it calls for expert testimony.

You can answer.

THE WITNESS: If you go back and look at -- I believe it's the request for admission.

BY MR. ABDO:

Q You're welcome to refresh your recollection using that document, but I'd like your answer to that question.

A Okay, so could you ask your question one more time?

Q Sure. Approximately how many data transmission lines are there that satisfy the definition of "Internet backbone" given by the NSA?

MR. PATTON: Objection to the extent it calls for expert testimony.

THE WITNESS: How many data transmission lines meet the definition -- I'm sorry?

BY MR. ABDO:

Q Yeah, sorry, let me say it one more time. Approximately how many data transmission lines are there that satisfy the definition of "Internet backbone" given by the NSA?

MR. PATTON: Just object, first again to the extent it calls for expert testimony, and second, to the extent it is beyond the 30(b)(6) deposition notice.

Just to be clear, to the extent it's beyond the deposition notice, she'll be answering in her personal capacity as opposed to her capacity as a 30(b)(6) NSA designee.

I'll shorten that next time.

MR. ABDO: Just for the record, would you let us know what you're looking at?

THE WITNESS: I am looking at the Request for Admission response -- Request for Admission No. 1 and No. 2, just to try and make sure I'm -- I don't think that this -- how many data transmission lines are there that satisfy the definition.

MR. PATTON: The definition is Interrogatory Response 12; is that right?

THE WITNESS: Correct.

BY MR. ABDO:

Q If you don't know the answer, you don't know the answer. I'm asking whether you know the answer.

A I don't know the answer. I'm sorry.

Q Is there anyone at the NSA who would know the answer to that question?

A So to the extent that the answer to that question is available to the public -- so I guess to the extent that that information may be available in the public, we didn't -- I don't know, I mean, actually.

Q Do you know whether anyone at the NSA would know the answer to that question even if based on information not available to the public?

MR. PATTON: Well, object.

THE WITNESS: So I think --

MR. PATTON: Object to the form to the extent it calls for classified and otherwise

protected information.

The witness can answer the question if she's confident that the answer is unclassified. I'm not. I am not.

THE WITNESS: The answer to your question, to the extent it's unclassified, and to the extent it is known, would be in the public sphere and not something specific to NSA's -- to how NSA functions or what NSA does.

BY MR. ABDO:

Q Just so I understand it, is your response then that there's a further answer you could give, but will refuse to on the basis of its classification?

In other words, is there more you would say but for your belief that answering my question would disclose classified information or protected information?

MR. PATTON: Objection. The answer I believe calls for classified information and information otherwise protected by the statutory privileges, and I instruct the witness not to

answer.

BY MR. ABDO:

Q Are you going to follow your --

A I am going to follow my lawyer's --

Q -- instruction not to answer?

A -- instruction not to answer.

Q Is your understanding then that even answering my question of whether providing an answer to my question would disclose classified information is itself classified?

MR. PATTON: Same objection.

Just a second.

(Counsel conferring.)

THE WITNESS: I think it would --

MR. PATTON: Just a second.

MR. PADGETT: Could you read back the question?

THE WITNESS: I just wanted to read back the question, yeah, or you can restate the question.

BY MR. ABDO:

Q Let me restate the question. I'll go

back to what I think started us down this path.

I originally asked whether there's somebody at the NSA who knows how many data transmission lines there are that satisfy the definition of "Internet backbone" provided by the NSA. I believe you said you don't know the answer, so I asked whether somebody at the NSA would know the answer to that question.

Then I believe you said, please correct me if I'm wrong, that to the extent there's an answer that you can provide publicly to that question, it was provided in the NSA's responses to our requests for admission.

A Can we go out on a classified -- could we take a --

Q Sure.

MR. PATTON: Yes. I just want to say before we go off the record that object to the extent it misstates the prior testimony, and that she also said that it doesn't mean anything different in an unclassified sense than what telecommunications experts would say.

BY MR. ABDO:

Q Okay. You understand that I was asking about knowledge that the NSA has irrespective of whether that information is available to the general public.

A I did understand. What I said was I was not answering about what NSA knew or didn't know because there's a classification issue, but to the extent there was an answer to your question, it would be whatever you could find in the public.

And so similar to what you see in response to RFA 1, where we give the information that TeleGeography publishes, to the extent they have information that would say -- provide the answer to this question, but I don't think that the answer to RFA 1 was the same as what you were asking.

MR. PATTON: And so we'll go off the record and see if there's more information that can be provided unclassified.

MR. ABDO: That's fine, although I'm

also trying to establish whether there's somebody at the NSA who would be able to provide a classified response, even if not here today, whether there's somebody who could provide that response if we were to move to compel that response.

It sounds as though you're not that person from what you're saying. I'm trying to understand if there's somebody else who is that person.

THE WITNESS: And so could we please --

MR. PATTON: Wait a second.

And we're trying to figure out whether we can tell you that.

THE WITNESS: Yes, so let us go have that --

MR. ABDO: We'll go off the record for a few minutes.

(Off the record at 10:38 a.m.)

(Resume at 10:47 a.m.)

MR. PATTON: Have we got a question

pending?

MR. ABDO: Yes, we have a question pending, and as I understand it, Ms. Richards, you went out to consult with counsel about whether you could respond to my question without disclosing classified information.

Have you arrived at a conclusion?

MR. PATTON: Yes. It's like a jury, we have arrived at a verdict.

So just to put my objections on the record, one is that it calls for expert testimony; two, it is beyond the 30(b)(6) notice, and therefore the witness's answer, if she were to give one, would be in her personal capacity as opposed to her capacity as a 30(b)(6) witness.

And if I understand the question correctly, anything beyond the unclassified information that's already been provided in the RFA, we can neither confirm nor deny whether or not --

MR. PADGETT: I'm sorry.

(Counsel conferring.)

MR. PATTON: So striking the last part, whether NSA has any nonpublic information going beyond what's already in the RFA we can neither confirm nor deny, so on that basis, instruct the witness not to answer the pending question.

BY MR. ABDO:

Q And you'll follow your lawyer's instruction not to answer?

A I will follow my lawyer's advice not to answer.

Q Okay. Could you please turn to page 5 of Exhibit 42 -- sorry, page 6 of Exhibit 42. You were here a moment ago, but if you need to, would you please re-read the two paragraphs designated as "RESPONSE" on that page.

A I'm sorry, to clarify, we're on the interrogatories?

Q Yes. Exhibit 42 are the NSA's Responses and Objections to Plaintiff's First Set of Interrogatories, page 6.

A Page 6, yes.

Q If you need to, just refresh your memory of that response.

A Yes.

Q Is an international submarine cable that connects two stations a circuit as the NSA has defined that term in response to Interrogatory No. 2?

MR. PATTON: Objection to the extent it calls for expert testimony.

THE WITNESS: As with Internet backbone, "circuit" has no specific NSA meaning. It is the meaning that a telecommunications expert would expect it to mean. There's nothing something special. So I just want to make sure that that's clear, there's not some other definition out there.

To the extent that you asked whether two submarine cables would be -- I'm sorry, I just want to make sure.

BY MR. ABDO:

Q Whether an international submarine cable that connects two stations is a circuit.

A Yeah.
MR. PATTON: Same objection.
THE WITNESS: Yes.
BY MR. ABDO:
Q Okay. Is an international submarine cable that connects two stations a circuit on the Internet backbone?
MR. PATTON: Object to the form, vague. Objection to the extent it calls for expert testimony.
THE WITNESS: Say it one more time.
BY MR. ABDO:
Q Do you want me to repeat that?
A Yes, please.
Q Sure. Is an international submarine cable that connects two stations a circuit on the Internet backbone?
MR. PATTON: Objection to the extent it calls for expert testimony.
THE WITNESS: Yes.
BY MR. ABDO:
Q Okay. Is each optical fiber within an

international submarine cable that connects two stations a circuit?

MR. PATTON: Objection. Same objection as before.

THE WITNESS: Each of these is an example of what might be a circuit and what might be considered the Internet backbone.

So to the extent an optical fiber is given as an example of a circuit, then the answer would be yes, but they're an example.

BY MR. ABDO:

Q That's right. I'm not asking -- let me try to be clear.

A Okay.

Q Each of these questions is asking whether a particular data transmission line connecting two stations constitutes a circuit. I'm not asking for you to confirm that that's the only sort of circuit out there.

A Okay.

Q So I am asking whether these are examples of a circuit, not whether they are the

sum total of what might be a circuit.

A Okay.

Q With that understanding, is your answer to my last question -- what is your answer to my last question, which was is each optical fiber within an international submarine cable that connect two stations a circuit?

MR. PATTON: Objection to the extent it mischaracterizes the prior testimony. Objection, calls for expert testimony.

THE WITNESS: Circuit could -- the definition of "circuit" being two stations, instruments transmitting information, could be an example of -- could be an example. So it could be, yes.

BY MR. ABDO:

Q When you say it could be, you're referring again to an optical fiber within an international submarine cable?

A Yes, it could be.

Q If an optical fiber within an international submarine cable has been

multiplexed, would each of the subdivisions created by that multiplexing be a circuit?

MR. PATTON: Objection to the extent it calls for expert testimony. You can answer.

THE WITNESS: It could be.

BY MR. ABDO:

Q In what circumstance would it be, and in what circumstance would it not be?

A I'm trying to think if there's an example where it wouldn't be. I think the definition --

MR. PATTON: Same objection to that question and this line of questioning.

THE WITNESS: Yeah. So a telecommunications expert would undoubtedly consider it to be a circuit.

BY MR. ABDO:

Q Would the NSA also consider it to be a circuit?

A To the extent that there's no --

MR. PATTON: Object. Objection to the form to the extent it calls for expert testimony.

THE WITNESS: To the extent that there's no difference in the definition that NSA takes versus what a telecommunications expert takes, there's no special meaning to the word "circuit." So if they would consider it to be a circuit, then NSA would consider it to be a circuit.

BY MR. ABDO:

Q Okay. Can a single circuit span multiple physical paths between two stations?

MR. PATTON: Objection, vague. Objection, calls for expert testimony.

THE WITNESS: Can a single --

BY MR. ABDO:

Q Can a single circuit span multiple physical paths between two stations?

And I understand you'll make the same objections.

MR. PATTON: Same objections. And I would just add beyond the scope of 30(b)(6), and therefore the witness will be testifying in her personal capacity as opposed to her 30(b)(6)

designee capacity.

MR. ABDO: Rodney, if it's okay with you, can we shorten that objection to it's beyond the scope?

MR. PATTON: As long as you understand that what that means here is that she's testifying as Becky Richards and not testifying as a 30(b)(6) witness for the NSA.

MR. ABDO: Thanks. I will so understand it.

THE WITNESS: And I will --

BY MR. ABDO:

Q Let me restate the question.

A I've now lost what the question is as Becky answering.

Q Let me restate it, okay?

Can a single circuit span multiple physical paths between two stations?

MR. PATTON: Objection, calls for expert testimony. Objection, beyond the scope of 30(b)(6).

THE WITNESS: I'm going to answer I

don't know.

BY MR. ABDO:

Q Do you know whether there's anybody else at the NSA who would know the answer to that question?

MR. PATTON: You can answer if you have an unclassified --

THE WITNESS: I don't know.

BY MR. ABDO:

Q You don't know whether there's somebody else at the NSA who would know the answer to that question?

A Correct.

Q Did you talk to any subject matter experts at the NSA about the meaning of the term "circuit" prior to this deposition?

A I did.

Q As part of that conversation, did you do anything beyond reviewing the definition of "circuit" provided by the NSA in response to our Interrogatory No. 2?

MR. PATTON: Objection, vague.

THE WITNESS: We discussed generally what is meant by "circuit" in the context of a telecommunications expert.

We did not get to the specific whatever you just asked of a single circuit having multiple physical paths.

BY MR. ABDO:

Q Okay. What's your understanding of the term "virtual circuit"?

MR. PATTON: Object to the form, calls for expert testimony, and beyond the scope of 30(b)(6).

THE WITNESS: As described in the -- are we still on the interrogatories on page 6 in response to No. 2?

BY MR. ABDO:

Q Yes. Let me try to be clear.

What is your understanding of the term "virtual circuit" as used by the NSA in its response to Interrogatory No. 2?

A My understanding is that there's a way in which to use different techniques to divide the

circuits so that you have more than one -- multiple circuits on one circuit.

Q Let me just try to understand that. Do virtual circuits -- let me start over. Can a virtual circuit traverse multiple physical circuits?

MR. PATTON: Objection to the extent it calls for expert testimony, and beyond the scope of 30(b)(6).

THE WITNESS: I'll respond I don't know.

BY MR. ABDO:

Q Is there anyone at the NSA who would know the answer to that question?

A I don't know.

Q Did you talk with any subject matter experts at the NSA about the definition of or the meaning of the term "virtual circuit" as used in the NSA's response to Interrogatory No. 2?

A I did.

Q Is there anything about the meaning of the term "virtual circuit" that you can provide

beyond what is in the NSA's response to Interrogatory No. 2?

A Since I'm not the telecommunications subject matter expert, my answer is confined to what you see on the piece of paper.

Q Is there a telecommunications subject matter expert at the NSA who could more fully answer that question?

Let me restate the question.

Is there anyone at the NSA who could more fully define what the term "virtual circuit" means as used by the NSA in response to Interrogatory No. 2?

MR. PATTON: To the extent that the answer is yes or no, she can answer, but I'll note for the record that she's testified multiple times that the NSA does not mean anything different by the term "virtual circuit" other than what is understood within the telecommunications industry.

BY MR. ABDO:

Q What is the meaning of "virtual circuit" as understood within the

telecommunications industry?

MR. PATTON: I'm going to object to the question to the extent it calls for expert testimony, and beyond the scope of 30(b)(6).

BY MR. ABDO:

Q You can answer.

A I don't have anything further to define for you.

Q Is there anyone at the NSA who better understands the definition of "virtual circuit" as used by those in the telecommunications industry?

MR. PATTON: You can answer the question if it's unclassified.

THE WITNESS: I don't know.

MR. PATTON: You can't provide a name.

THE WITNESS: I don't know.

BY MR. ABDO:

Q You don't know whether there's anyone at the NSA?

A Correct.

Q It's true -- well, let me ask you.

Is it true that each Internet protocol

packet sent on the Internet is routed to its destination independently?

MR. PATTON: Object to the form of the question to the extent it calls for expert testimony, and outside the scope of 30(b)(6).

You can answer.

THE WITNESS: I'm sorry, can you ask the question again?

BY MR. ABDO:

Q Sure. Is it true that each Internet protocol packet sent on the Internet is routed to its destination independently?

MR. PATTON: Same objections.

THE WITNESS: Generally speaking, yes, that is my understanding.

BY MR. ABDO:

Q Are there circumstances you can think of where Internet protocol packets would not be routed independently on the Internet?

MR. PATTON: Object to the form to the extent it calls for expert testimony, and beyond the scope of 30(b)(6). You can answer.

THE WITNESS: Not off the top of my head, but I'm sure there are examples.

BY MR. ABDO:

Q Why are you sure there are examples?

A Just because every rule seems to have some sort of exception to it, so to say something is hard and fast to be always the case is not something I would like to do.

Q Okay. When Internet packets that constitute a single communication take different paths to a common destination, are those packets traversing different circuits or the same circuit?

MR. PATTON: Object to the form, lacks foundation, object to the vagueness of the term "single communication." Object that it calls for expert testimony, and it is beyond the scope of 30(b)(6). You can answer.

THE WITNESS: The question was if packets take a different path, are they on different circuits?

BY MR. ABDO:

Q Yes.

A I would say it depends. There's not, again, a hard and fast rule. Depending, it might be on the same circuit, it might be on a different circuit.

Q What does it depend on?

MR. PATTON: Same set of objections.

THE WITNESS: I guess it would depend on how -- what would it depend on?

It would depend on the nature of the circuit.

BY MR. ABDO:

Q What do you mean by the nature of the circuit?

MR. PATTON: Same objections.

THE WITNESS: Depending on how the packets were going and how you -- how is it routed? Do they take different paths, or are they on the same circuit?

So to the extent the circuit can be meant in a big sense or in a small sense, it's going to decide whether it's on the same circuit or not.

So you asked in a separate set of line, had a whole bunch of distinctions as to what was data transmission line and what were they, and was it a wavelength, or something further into that. So it will depend on how you define "circuit," which is why you were asking me to define "circuit."

BY MR. ABDO:

Q Let me just try to understand.

Does the answer to my question depend on whether the separate paths being taken by packets are being routed over one physical circuit or not?

MR. PATTON: Same set of objections.

THE WITNESS: One physical circuit?

BY MR. ABDO:

Q Suppose two packets that are part of the same communication traverse different optical fibers.

A Okay. Are those different circuits?

Q Yes, that's my question.

MR. PATTON: Object to the extent it

calls for expert testimony in a hypothetical, and also beyond the scope of 30(b)(6).

THE WITNESS: So --

MR. PATTON: Also asked and answered.

THE WITNESS: So if it's on two different circuits, then it's on two different circuits. I feel like I'm having a circular conversation, so I'm not sure. Can two packets be on the same circuit and take different paths?

MR. PATTON: I don't think that's the question.

THE WITNESS: Is that --

BY MR. ABDO:

Q My original question was whether packets that are traversing different paths to their common destination are traversing different circuits. And I believe, please correct me if I'm wrong, you said, generally, yes.

MR. PATTON: That's a misstatement of her prior testimony.

BY MR. ABDO:

Q Could you please tell us what your

answer is to that original question?

MR. PATTON: Do you want the question to be read back?

MR. ABDO: No. I mean, let's move on.

Would you mind, Ms. Jaques, marking this as Exhibit 43?

(Deposition Exhibit 43 was marked for identification.)

BY MR. ABDO:

Q So you have in front of you what's been marked as Exhibit 43.

Do you recognize that document?

A Absolutely.

Q And what is Exhibit 43?

A Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2nd, 2014.

Q What was the NSA's relationship to the drafting or review of the report marked Exhibit 43?

MR. PATTON: Objection as vague, and

objection to the extent it may call for deliberative process privilege that might be invoked by the PCLOB that we don't represent. So maybe if you could ask a more narrow question, we can avoid most of the deliberative process.

She can speak in general terms on that, that would be good, in answer to your question, but I don't want to too broadly object on deliberative process grounds to protect PCLOB's privilege.

BY MR. ABDO:

Q Let me ask a different related question. Was the NSA involved in the drafting of Exhibit 43?

MR. PATTON: Objection, vague.

THE WITNESS: NSA provided expert testimony to the Board as is described on page 4 of the report. We provided documentation, we provided presentations, and we answered questions throughout their process.

We then for the fact section reviewed -- we reviewed the document for factual

accuracy, as well as we reviewed the entire document for classification to ensure there was no classified material in it.

BY MR. ABDO:

Q So I believe that you said that the NSA provided testimony, documentation, and presentations to the members of the PCLOB in drafting Exhibit 43, right?

A That is correct.

Q Do you know how many sessions the NSA provided testimony about the subject matter of the report that's marked Exhibit 43?

A It was a handful. I don't remember the exact number, but certainly they came to NSA, and we went to the PCLOB a number of times, both ways. We had conference calls, and we had email exchanges.

Q And did that testimony involve both classified and unclassified information?

A Yes, it did.

Q Is the same true of the documentation that the NSA provided to the PCLOB?

A Yes, it was both classified and unclassified.

Q And is that also true of the presentations provided?

A Yes, all was classified and unclassified.

Q And you say that the NSA reviewed the factual section of the report marked Exhibit 43 for accuracy; is that correct?

A That is correct.

Q When you say "fact section," what specific pages are you referring to, or page range are you referring to?

A Page 16 to 79. In essence, Part 3, Description and History.

Q Did the NSA review any other portion of the report marked Exhibit 43 for factual accuracy?

MR. PATTON: Objection to the form, vague as to time.

THE WITNESS: NSA otherwise did a classification review of the document.

To the extent these documents have the opinions of the various board members, NSA was not reviewing that information beyond ensuring there was no classified material in it.

BY MR. ABDO:

Q If the NSA, during its classification review of the portions of the report, other than Part 3, noticed a factual inaccuracy, would the NSA have notified the PCLOB of that inaccuracy?

A NSA conducted a classification review of the document. As part of that classification review, to the extent that something would be described in some of the other pieces of the document that was not not, we would notify them as part of that, as is noted again on page 4.

Q Let me just make sure I understand.

A Yeah.

Q The NSA reviewed Part 3 of the report marked Exhibit 43 for accuracy, right?

A That is correct.

Q It reviewed the entire document for classification, right?

A Correct.

Q And if in the process of reviewing the entire document for classification it noticed an inaccuracy outside the portion that it reviewed solely for accuracy -- sorry, outside the portion that it reviewed when it was conducting its review for accuracy, your testimony is that the NSA would have notified the PCLOB of that inaccuracy?

A Correct.

Q Was the NSA's review for accuracy of the factual section of the report thorough?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q The NSA would have reviewed every sentence?

A Absolutely.

Q And what would the NSA have done if it noticed an inaccuracy in any portion of the report?

MR. PATTON: Objection, vague.

THE WITNESS: NSA would provide a

response explaining either why it was inaccurate or why the information in the classification review was classified, and there was -- as is important to remember in the Upstream, large portions of that program remain classified, and so necessarily with this report, with this NSA Civil Liberties and Privacy Office Report, the information is incomplete.

And so a lot of the conversation was a mixture of how do you provide an accurate representation of how Upstream works while keeping the sources and methods classified? And so a lot of the conversation, particularly around the accuracy and the classification, were tied together because of those reasons.

And so this gives, as does our report, and continues to, a broad accurate description of the outline of how the program runs, but does not get into some of the much more specific aspects to it.

BY MR. ABDO:

Q In the course of the review for

accuracy of the report, did the NSA notice inaccuracies and make recommendations to the PCLOB about how to fix those inaccuracies in what's now marked Exhibit 43?

A Yes.

Q Are you aware -- sorry, strike that.

Did the PCLOB generally accept those recommendations?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Could you read the question back?

(The reporter read back the question.)

MR. PATTON: Just object to beyond the scope of the 30(b)(6).

And if the answer to that question is yes or no, you can answer. If the answer to that question is going to be a narrative description of what the PCLOB did or did not accept, then we're concerned that we might be in the deliberative process.

MR. ABDO: I just want to state for

the record, Rodney, you don't represent the PCLOB, correct?

MR. PATTON: I do not, but I am with the Department of Justice, and we do represent the United States, so here we would be preserving their ability to later assert that privilege if need be. I certainly am not in a capacity to waive it on their behalf.

MR. ABDO: I'm just not sure you're in a position to assert it though. I'm not sure we're asking for anything that's going to reveal the deliberations anyway, but I note that we object to your quasi-invocation of the PCLOB's deliberative process.

MR. PATTON: I can rephrase it as a preservation of their right to assert the deliberative process privilege, since they are not here to invoke that themselves.

MR. GILLIGAN: I would add that our function as Department of Justice attorneys is to represent the interests of the United States in this proceeding, and PCLOB is an independent

establishment of the United States government, but I understand your objection.

MR. ABDO: Sure, but you also know that we had -- you know, Topic 6 very clearly included this report as a subject of this deposition.

MR. PATTON: I doubt, again, that you will be delving into the details of that. There's an awful lot --

MR. GILLIGAN: The facts, not recommendations.

MR. PATTON: There's an awful lot of questions that the witness is perfectly capable of answering, so I don't think we're going to be in any --

BY MR. ABDO:

Q Ms. Richards, can you answer the question?

A Yes, I'll answer the question.

What I would do is point you to, again, page 4 that specifically says that they considered the Intelligence Community's comments

regarding the operation of the program to ensure accuracy. None of the changes resulting from that process affected the Board's substantive analysis and recommendations.

So I would point you to that to avoid this whole conversation about what is or isn't sort of privileged between it to say that they accepted our changes, they didn't change substantively what they were doing. We went through a back-and-forth to ensure that everybody understood how the program worked, what was classified.

In some instances, they asked for information to be declassified in order to make the record full, and that didn't change. So we went through that process.

Q Let me ask my question again because I don't think that answered it.

A Sure, okay.

Q If the NSA identified an inaccuracy in the report marked as Exhibit 43 to the PCLOB, would the PCLOB generally fix that factual

inaccuracy, generally have fixed it?

MR. PATTON: Object to the form, vague.

THE WITNESS: Yes. The PCLOB was not interested in having an inaccurate description of how Section 702 -- it was not within -- they didn't want to have that, and so they worked closely with us to ensure that they -- I don't know if "closely" is the right word, but they worked with us extensively in order to ensure that they had an accurate representation that could be made unclassified, which was -- up until -- there had -- the record had been not as extensive.

BY MR. ABDO:

Q Okay. Are you aware of any inaccuracies, factual inaccuracies, in the report marked as Exhibit 43?

MR. PATTON: Object to form, vague.

THE WITNESS: If there's particular sentences you would like me to look at or there's particular questions that you have, I'd be happy to look at those and walk through.

As a general matter, the information in here is accurate as a description, but necessarily, as I mentioned before, not a full description of the program because many of those facts still remain unclassified. But if there's particular sentences that you would like to point me to, I'm happy to review.

I would also note that, as of 2017, NSA changed one of the ways it was doing its collection, so it was no longer getting "abouts" collection. And so to the extent the material in here accurately reflects what was happening in 2014, the general matter, there may be, you know, slight, slight differences, but this is true.

That information has changed, so we are no longer doing a collection that gets the, quote, "abouts" collection in upstream. So to the extent that that's no longer accurate, that would be the case.

BY MR. ABDO:

Q But at least as the NSA was conducting upstream surveillance as of July 2nd, 2014, which

is the date of that report, you're not aware of inaccuracies in the report?

A Again, I would ask --

MR. PATTON: Sorry, just object to asked and answered. Go ahead, you can answer.

THE WITNESS: Again, if there are specific sentences you would like me to go to that you think maybe are not accurate, I'm happy to talk about those particular sentences. It's a 191-page document.

As a general matter, NSA considers this to be an accurate outline of the unclassified portions of Upstream. There may be particular sentences as they describe them, but the facts we believe to be accurate.

BY MR. ABDO:

Q Okay. I want to turn your attention to page 36 of the report marked Exhibit 43. Could you please read the first sentence of the very last paragraph that starts on that page? It begins "once tasked." Again, that's at the bottom of page 36 of Exhibit 43, and that sentence ends

on the next page, 37.

A Okay, yes.

Q Is that sentence factually accurate?

MR. PATTON: Object to the form, vague.

BY MR. ABDO:

Q As of the time -- let me start over.

Is the sentence that I just asked you to read at the bottom of page 36, carrying over onto page 37 of Exhibit 43, an accurate description of how upstream surveillance operated as of July 2nd, 2014?

A Well, what I would do is I would point you, rather than to the sentence that's on page 36 of the PCLOB report, and instead suggest that the RFA, Request for Admission, on page 9, in response to RFA for No. 8, that describes how this is -- how the government describes it.

The other place I would suggest, which is the government's description, is also in the NSA Civil Liberties and Privacy Office Report at page 5.

Those are both more accurate descriptions of how we would talk about Upstream. The description on page 36 is necessarily vague.

Q What's inaccurate about the sentence at the bottom of page 36, carrying over onto page 37, in Exhibit 43?

MR. PATTON: Objection, mischaracterizes prior testimony. And just a second, there might be a classified response.

We will need to find out what her answer is going to be on this to determine whether the answer is partially classified, fully classified, or wholly unclassified. At this point, I don't know what her answer is going to be.

MS. HANLEY COOK: Why don't we take a five-minute break.

MR. ABDO: Go off the record, Dawn, please.

(Off the record at 11:30 a.m.)

(Resume at 11:56 a.m.)

MR. ABDO: Ms. Jaques, do you mind

reading back the last question before we broke?

(The reporter read back the question.)

MR. PATTON: Objection to the extent it misstates prior testimony, and objection to the extent that the answer calls for classified information and information subject to the statutory privileges.

You can answer to the extent your answer is unclassified.

THE WITNESS: Okay. So this sentence, as I mentioned about the entire document and the sort of public description of Upstream, is necessarily incomplete because of the classification of information.

This sentence is accurate as of 2014, but I would point you to the description that's provided in the RFA, Request for Admission No. 8, in the response. That provides an accurate description of how upstream Internet collection works today, with, again, the understanding that it's necessarily incomplete.

To provide you a description of what

is different between those two and why necessarily gets into the classified realm, and so I can't go any further into that.

BY MR. ABDO:

Q Let me just make sure I understand.

A Yep.

Q Is it true that the sentence we've been focusing on, the carryover sentence between pages 36 and 37 of Exhibit 43, is accurate as of 2014?

MR. PATTON: Objection, mischaracterizes prior testimony.

THE WITNESS: It is accurate, but incomplete, and that's a very important fact.

BY MR. ABDO:

Q And the reasons why it is incomplete you are saying are classified; is that correct?

A That is correct.

Q Is it incomplete because it omits additional information about the operation of upstream surveillance that is classified?

MR. PATTON: Let me just check to find

out whether the answer is yes or no.

(Counsel conferring.)

THE WITNESS: Ask your question one more -- can you repeat the question for me?

BY MR. ABDO:

Q I can ask it again.

Is the sentence that carries over between pages 36 and 37 of Exhibit 43 incomplete, which is the word you used --

A Correct.

Q -- because it omits information about the operation of upstream surveillance that is classified?

MR. PATTON: Just a second.

You can answer yes or no.

THE WITNESS: Okay, yes.

BY MR. ABDO:

Q Is it incomplete for any other reason other than that it omits additional information that is classified about the operation of upstream surveillance?

MR. PATTON: Object to form, but you

can answer.

THE WITNESS: It is incomplete because it omits classified information.

I'm not sure I understood your second question, what you were trying to -- what my other -- what other options you're providing for.

BY MR. ABDO:

Q A statement could be incomplete for a number of reasons. It could be incomplete because it omits relevant information, it could be incomplete because it includes information that is inaccurate or misleading, and I'm trying to understand why the NSA believes this sentence is incomplete?

A It's incomplete because it omits the classified information.

Q And for no other reason?

A Not that I can think of. I'm pausing because I can't -- I guess maybe you can be more specific, but I guess you said I could have added more information in -- they could have added more information into it and that's what makes it

incomplete? I'm not sure I understand. I guess I don't understand beyond omitting.

I'm willing say to say it's incomplete because it's omitting information. I'm not sure I understand the remainder of what you're trying to get at, so maybe you can rephrase it.

Q Let me ask it another way.

Is any of the information included in this sentence -- again, the sentence carrying over from pages 36 to 37 of Exhibit 43 -- inaccurate?

MR. PATTON: Objection, vague as to time.

MR. ABDO: As to the operation of upstream surveillance in 2014.

THE WITNESS: As I've said, it's incomplete.

BY MR. ABDO:

Q I'm asking if it's inaccurate.

A No. I've stated it's accurate. It's just incomplete.

Q Is it inaccurate as to the operation of upstream surveillance today?

MR. PATTON: Objection, calls for information that is classified and subject to the state secrets privilege, the other statutory privileges. I instruct the witness not to answer the question.

BY MR. ABDO:

Q Are you going to follow your lawyer's instruction not to answer?

A I'm going to follow my lawyer's direction not to answer.

Q Do you know the answer to the question that I asked? In other words, if you were to answer, could you?

A It would be classified, so I can't answer it because it's classified.

Q But do you know the information that you would provide in response but for --

A The classification?

Q Yes.

A Yes.

Q Is there anything you can say in response to the question without revealing

information you've been instructed not to provide?

A I would point you to the answer to the response that's on page 9 of the RFA, which accurately, to the extent possible given the classified nature, describes the current way Upstream works. And so I would -- that's how I would answer.

Q But specifically with respect to this sentence, is there anything you can say in response to my question, which was is the sentence accurate as to the operation of upstream surveillance today?

Is there anything you can say, aside from pointing me to other testimony or other information, that would not require you to disclose classified information?

A No.

Q Can you describe -- well, let me ask you this. Do you agree with your lawyer's instruction that answering the question would harm national security?

MR. PATTON: I'm going to object to

the form of the question as it seeks a legal conclusion, and as my colleagues just pointed out, beyond the scope of 30(b)(6).

MR. ABDO: You should take a look at guideline 7 of Appendix A of the local rules, which clearly contemplates counsel asking for the basis of assertions of privilege.

So my question is --

MR. PATTON: Same objection. That calls for a legal conclusion.

BY MR. ABDO:

Q Do you believe that answering the question would result in harm to national security?

A Yes.

Q Can you describe that harm?

MR. PATTON: No. I'm going to object to that question, as it would call for classified information and information subject to the statutory privileges, and I'll instruct her not to answer the question.

BY MR. ABDO:

Q Do you agree that describing the harm would itself result in harm to national security?

A Yes.

Q Have you discussed the invocation of the state secrets privilege with respect to this question with Admiral Michael Rogers?

MR. PATTON: With respect to this particular question?

MR. ABDO: Yes.

THE WITNESS: The question being -- I'm sorry, so just explain to me. The question is whether describing the difference between the sentence on page 36 and the interrogatory -- or the Request for Admission on page 9, whether describing what is different between those two would be a national security harm with him specifically?

BY MR. ABDO:

Q No. The original question was whether the carryover sentence from page 36 to 37 of Exhibit 43 is accurate with respect to upstream

surveillance as it is conducted today.

Have you discussed with Admiral Rogers whether answering a question seeking that information requires invocation of the state secrets privilege?

MR. PATTON: You can answer the question.

THE WITNESS: No, I have not.

BY MR. ABDO:

Q Have you more generally discussed the invocation of the state secrets privilege in this deposition with Admiral Rogers?

A I spoke to him extensively prior to the issuance of both the NSA Civil Liberties and Privacy Office Report, as well as the PCLOB Report, for him to understand what information was going to be in that.

So whether for today's testimony -- I did not go back to him and ask him specifically about any of this information, as that had largely been covered when we were issuing those reports back in 2014.

Q Okay. Is there anything else you can tell us about this assertion of the state secrets privilege?

MR. PATTON: Objection, vague.

THE WITNESS: I don't know what you're asking me.

BY MR. ABDO:

Q Is there anything that you can say that would be unclassified about the nature of the state secrets privilege invocation, or the reason for it, or the harm that would come about by answering the question?

A No, other than to say that this is sources and methods. You're getting into sources and methods, which is what we have -- we protect extensively.

Q Okay. As of 2014, did the NSA conduct upstream surveillance on at least one Internet backbone circuit?

MR. PATTON: Object to the question to the extent it calls for a classified answer, subject to the state secrets privilege, prior

statutory privileges.

You can answer the question to the extent not classified.

THE WITNESS: The question is at least one?

BY MR. ABDO:

Q Internet backbone circuit.

A One Internet backbone circuit.

MR. PATTON: This is probably another one of those questions where a yes-or-no answer would be unclassified, but --

MR. ABDO: That's what I'm looking for, a yes or no.

MR. PATTON: Any narrative answer we would have to break for.

THE WITNESS: At least one Internet --

BY MR. ABDO:

Q Let me restate the question.

A Okay.

Q As of 2014, did the NSA conduct upstream surveillance on at least one Internet backbone circuit? Yes or no.

MR. PATTON: Same classified objections to the extent that the question seeks classified information. To the extent it's yes or no, you can answer the question.

THE WITNESS: Yes.

BY MR. ABDO:

Q As of 2014, did the NSA conduct upstream surveillance on more than one Internet backbone circuit?

MR. PATTON: Object to that question to the extent it calls for classified information protected by the state secrets privilege, statutory privilege.

Instruct the witness not to answer the question.

THE WITNESS: I will follow my lawyer's direction.

BY MR. ABDO:

Q Your view is that stating a yes in response to that question or a no in response to that question would disclose state secrets?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: Still following my lawyer's description -- direction.

BY MR. ABDO:

Q Is --

MR. GILLIGAN: Excuse me, Counsel, just one moment.

MR. ABDO: Yeah, sorry.

(Counsel conferring.)

BY MR. ABDO:

Q Is your view that the sentence we've been discussing between pages 36 and 37 of Exhibit 43 discloses any classified facts or facts protected by the statutory authorities your counsel has cited?

A The sentence is unclassified.

Q Is that true notwithstanding the fact that the sentence states that upstream surveillance involves the acquisition of communications transiting through circuits -- that's a quote -- on the Internet backbone?

MR. PATTON: Object to the form of the

question, vague as to time.

MR. ABDO: As of 2014.

MR. PATTON: Same objections, vague as to time.

THE WITNESS: My answer remains the same.

BY MR. ABDO:

Q What's your answer?

A That the fact that the word "circuits" is plural does not change any of my previous answers.

Q You don't view that as inconsistent with the assertion of the state secrets privilege in response to my question of whether, as of 2014, upstream surveillance involved more than one Internet backbone circuit?

MR. PATTON: Objection, asked and answered, argumentative. Go ahead.

THE WITNESS: I don't see that as inconsistent.

BY MR. ABDO:

Q Why not?

MR. PATTON: Same objections.

THE WITNESS: As we've stated, we've stated that we were on at least one, and the fact that there's a plural there isn't dispositive one way or the other.

BY MR. ABDO:

Q As of 2014, were multiple electronic communication service providers compelled to assist the NSA in the operation of upstream surveillance?

MR. PATTON: Objection, calls for classified information, sources and methods, operational details, and subject to state secrets and statutory privileges.

I instruct the witness not to answer the question.

THE WITNESS: I will follow my lawyer's --

BY MR. ABDO:

Q Can you please turn to page 12 of what's marked Exhibit 43 and read, if you would, what is marked as Recommendation 6, which is the

final paragraph of page 12.

MR. PATTON: Read it to herself or out loud?

MR. ABDO: To yourself, yeah.

THE WITNESS: Yes.

BY MR. ABDO:

Q Do you understand -- well, strike that.

Is it true that in the operation of upstream surveillance in 2014, there were -- and I'm quoting from this recommendation -- affected telecommunication service providers?

MR. PADGETT: Could you read back the question?

(The reporter read back the question.)

MR. PATTON: I'm going to object to vagueness in terms of time, and object to the question to the extent it calls for classified information, sources and methods information protected by the statutory privileges.

The witness can answer the question to the extent unclassified.

BY MR. ABDO:

Q Let me specify with respect to time that I'm talking about July 2nd, 2014, the date of this report.

MR. PATTON: Same objections.

THE WITNESS: I'd like to go in the SCIF before I answer this question.

MR. PATTON: Okay.

MR. ABDO: Take a break.

(Off the record at 12:16 p.m.)

(Resume at 12:19 p.m.)

MR. PATTON: Same objections.

THE WITNESS: So as I said earlier, providing any information as to the number of telecommunication service provider beyond one is classified. Because this is temporally at one point, we can neither confirm nor deny that information, whether it was more than one. To the extent there was more than -- to the extent there is a program, there must be one.

BY MR. ABDO:

Q Can you tell us whether there have

been more than one provider involved, even if not more than one at the same time?

MR. PATTON: Objection, calls for classified information pursuant to the state secrets privilege. Instruct the witness not to answer, and to the statutory privileges.

THE WITNESS: I will follow my lawyer's direction.

MR. ABDO: Rodney, are you okay shortening that objection to something?

MR. PATTON: I'm trying.

MR. ABDO: Okay.

Ms. Jaques, do you mind marking this as Exhibit 44?

(Deposition Exhibit 44 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you have in front of you what's been marked as Exhibit 44. Do you recognize that document?

A Yes, I do.

Q Did you draft this document?

A I did.
Q What is the document?
A The document is the NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of Foreign Intelligence Surveillance Act, Section 702, dated April 16th, 2014. It's exactly four years old.
Q Did the NSA review this document for accuracy and classification?
A Did the NSA?
Q Yes.
A Yes, it did.
Q Was that review thorough?
A Yes, it was.
MR. PATTON: Objection, vague.
THE WITNESS: Sorry, too fast.
BY MR. ABDO:
Q What was the purpose of issuing this report?
A The purpose of issuing the report was to put on the public record a description from NSA's perspective of what the privacy protections

were in place as it relates to Section 702.

Q Was it important to the NSA in issuing Exhibit 44 that the report be accurate?

A Absolutely.

Q And why is that?

A Because this was submitted to the Privacy and Civil Liberties Oversight Board as part of their request for comment as part of their report on Section 702, and we wanted to put on the record an unclassified description that NSA stood behind as to how the program worked.

Q And was it also important that the report, to the extent publicly disclosed, not reveal classified information?

A Yes.

Q Could you turn to page 5 of the report, again what's marked as Exhibit 44? I want to direct your attention to the first sentence of the last paragraph of the page, which starts, "In the second."

A Mm-hmm.

Q Could you read that sentence to

yourself, please, and let me know when you're done.

A (Witness reviewing document.) Okay.

Q Is this sentence referring to upstream surveillance as it operated as of April 16, 2014?

A Yes, it is.

Q Does this sentence confirm that service providers, plural, are compelled to assist the NSA in the lawful interception of electronic communications to, from, or about task selectors as of April 16th, 2014?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PADGETT: Can you read back the question?

(The reporter read back the question.)

BY MR. ABDO:

Q Let me ask it differently.

Is this sentence accurate as of April 16, 2014?

A To the extent, as with the PCLOB report, it's necessarily incomplete. It is

accurate to the outline of how the program works.

Q When you say it's incomplete, is it incomplete because it omits classified information about the operation of upstream surveillance as of April 16, 2014?

A Yes.

Q Is it incomplete for any other reason?

A No.

Q Do you understand this sentence to confirm that service providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about task selectors as of April 16th, 2014?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: We need to take just, I promise, a very short break to make sure the answer is unclassified. Thanks.

(Off the record at 12:26 p.m.)

(Resume at 12:40 p.m.)

MR. ABDO: Do you mind reading back the last question to us, Ms. Jaques?

(The reporter read back the question.)

MR. PATTON: Objection, vague as to time, and objection to the extent it seeks classified and otherwise statutorily privileged information.

You can answer to the extent it's unclassified.

THE WITNESS: So this sentence -- here's the thing. Would it have been clearer if we had put parens between the S? Yes. But we're not here -- we can't confirm or deny whether -- we've said that there was one service provider, at least one service provider in Upstream. The fact that this is plural does not -- is not an indication that it was more than one at that point in time or less than one at that point in time.

And so this is just -- it probably would have been clearer if we had put the parens. We didn't put the parens, so you've found the S's in our report, but it's not meant to have provided classified information, the fact that the numbers are classified.

BY MR. ABDO:

Q You understand that at the time that this report was issued -- and for the record, we're talking about Exhibit 44 -- there was a relatively small amount of unclassified information available from the government about the operation of upstream surveillance, right?

MR. PATTON: Objection, vague.

THE WITNESS: Yes, that's why I wrote the report.

BY MR. ABDO:

Q And you understand that the public and the PCLOB, which received this report, would regard it as an authoritative source of public information from the government about the operation of upstream surveillance?

MR. PATTON: Objection, calls for speculation about others and their thought processes.

THE WITNESS: Yes.

BY MR. ABDO:

Q And that was precisely one of the

reasons that you drafted it and disclosed the report, right?

A Correct.

MR. PATTON: Objection.

BY MR. ABDO:

Q Were you careful throughout to ensure that the factual assertions in this report were accurate?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q And was that in part at least so as not to mislead the public or the PCLOB as to the operation of upstream surveillance at the time the report was issued?

A Yes.

Q Did you take great care throughout the rest of the report in every word used to ensure that what the words conveyed were accurate and unclassified?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q Was this sentence reviewed with that same level of care?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q Are you aware of any factually incorrect statements in Exhibit 44 as to the operation of upstream surveillance at the time that the report purports to describe the operation of upstream surveillance?

MR. PATTON: Objection, ambiguous.

MR. ABDO: I'm sorry, I didn't hear.

MR. PATTON: Objection, ambiguous.

THE WITNESS: Again, to the extent that the information in here is unclassified, and therefore is necessarily incomplete, yes, this is an accurate description.

This was also really one of the first times that the NSA had written, so to the extent we've gotten better at this as we've gone along, the first time is always -- we were doing our

best.

BY MR. ABDO:

Q Setting aside the question of incomplete information, are you aware of any factual inaccuracies in Exhibit 44 as to the operation of upstream surveillance at the relevant time periods described in the report?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Go ahead.

THE WITNESS: No, I'm not.

BY MR. ABDO:

Q Also setting aside the question of incompleteness, are you aware of any factual inaccuracies in Exhibit 43, the report of the PCLOB, as to the operation of upstream surveillance for the periods of time described in that report?

MR. PATTON: Objection, vague.

THE WITNESS: As I said earlier, and as we just then described going through these different sentences, the answer is I am not

generally aware of any inaccuracies.

To the extent you have a question about a particular sentence, I'm happy to, as we did on page 36, walk you through and understand whether there was classified information that makes that sentence more or less complete.

BY MR. ABDO:

Q I appreciate that, and we may do that for a few more sentences, but my question is whether, as you sit here today, you are aware of any inaccuracies, factual inaccuracies, in Exhibit 43 with regard to the operation of upstream surveillance as the report describes?

MR. PATTON: Objection, asked and answered.

THE WITNESS: My answer is still the same. You know, the information in it is, generally speaking, accurate.

If there's a particular sentence you want to discuss -- it's necessarily incomplete, and describing Upstream, which is classified, in an unclassified sentence is difficult, as you're

seeing with us having to walk back and forth and make sure that we're hitting those lines so that we are providing an accurate general description of the program without going into the classified sources and methods of the program.

So, you know, it still remains accurate to the extent that it was true in 2014. I'll just re-remind you that we are no longer do the "abouts" collection as it was described starting in 2017, and so that piece of this report is not accurate.

BY MR. ABDO:

Q The report doesn't purport to describe surveillances operated years later, correct?

A Correct. I'm just re-reminding that to the extent that we've changed certain aspects of the program, that's no longer accurate.

Q Okay. I'm going to ask you similar questions that I just asked you about Exhibit 44, but about Exhibit 43.

Did the NSA, as it did with Exhibit 44, also review each and every factual

disclosure in Exhibit 43 to ensure that it was accurate?

MR. PATTON: Object to the form, vague, asked and answered.

THE WITNESS: To the extent that NSA scrubbed through the facts provided in the historical, as we mentioned, section from 16 to roughly 79, and also looked at from a classification purpose, yes.

We were, again, doing our best to try and help provide an unclassified description of a classified program, and so it was necessarily incomplete.

BY MR. ABDO:

Q And at the time that report was issued, is it also fair to say that there was relatively little public information from the government describing the operation of upstream surveillance?

MR. PATTON: Object to the form, vague.

THE WITNESS: I'm pausing because I

don't exactly remember when a number of the different FISC opinions were declassified. So I believe that there were a number of -- they were actually issued -- that they were declassified prior to -- or they were reviewed and redacted.

So Judge Bates -- which are mentioned. There are a number of reports that are footnoted in here that are -- that were declassified. I just -- some of the timing.

BY MR. ABDO:

Q Is it fair to say that at the time this report was issued, it was the most comprehensive description from the government of how upstream surveillance operated at the time the report was issued?

MR. PATTON: Objection, vague.

THE WITNESS: Yes, to the extent, though -- I would just offer that to the extent that these are the words of an independent executive agency with oversight over the Intelligence Community as it relates to CT functions, you know, these are their words.

They're not NSA's words. They're not NSA submissions.

And so sometimes they may describe things slightly differently than we may have chosen to do so, and so I would refer you back to the NSA or the government submissions on the descriptions of the programs.

BY MR. ABDO:

Q Okay. Is it fair to describe the report marked Exhibit 43 as an exhaustive description of upstream surveillance as it operated in 2014?

MR. PATTON: Objection, vague.

THE WITNESS: I suppose that's one. I'm guessing that you have something over there that -- are you referring to a specific document where NSA may have said that?

BY MR. ABDO:

Q Well, I'm asking you first whether that's fair, setting aside what the NSA has otherwise said?

A Yes, I think it's fair.

MR. PATTON: In unclassified terms.

THE WITNESS: In unclassified terms.

MR. PATTON: I guess that's probably what that's talking about, right?

MR. ABDO: Yeah, no, I think -- let me ask the question clearly.

Is the PCLOB's description of the operation of upstream surveillance exhaustive?

MR. PATTON: Same objection.

THE WITNESS: So, again, I think what I would say is I think that their study was exhaustive. To the extent that there's classified information, they had access to that information, which makes the study probably exhaustive, but to the extent that the report is necessarily incomplete, it's as much information as possible without going into the classified material.

BY MR. ABDO:

Q Okay. I want to ask you a question that I've tried different versions of, so forgive the repetition. I'm asking it multiple ways because I'm looking for what I think you ought to

be able to provide, which is a clean yes or no.

Setting aside the incompleteness of the report marked Exhibit 43, are you aware now of any factual inaccuracies in the report and its description of upstream surveillance as Upstream was conducted at the time the report was issued?

MR. PATTON: Objection, asked and answered. Go ahead.

THE WITNESS: I am not aware of any inaccurate -- known inaccuracies in the document as described other than the fact that there's classified information that has been omitted.

BY MR. ABDO:

Q What is the number, or approximate number, of Internet backbone circuits on which upstream surveillance is conducted --

MR. PATTON: Objection.

MR. ABDO: -- as of June 2015?

MR. PATTON: Objection, calls for classified information, sources and methods, operational details subject to state secrets and the statutory privilege.

Instruct the witness not to answer.

THE WITNESS: I will follow my lawyer's direction.

MR. ABDO: Rodney, I think it might be in our interest to come up with a shortened version of that, at least for the next few minutes.

MR. PATTON: Yes, you have my word.

BY MR. ABDO:

Q What is the number, or approximate number, of Internet backbone circuits on which upstream surveillance is conducted today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Still following those directions.

BY MR. ABDO:

Q Okay. What is the average bandwidth of the Internet backbone circuits on which upstream surveillance was conducted in June 2015?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Following the instruction.

BY MR. ABDO:

Q What is the average bandwidth of the Internet backbone circuits on which upstream surveillance is conducted today?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Still following the instructions.

BY MR. ABDO:

Q What is the approximate combined bandwidth of the Internet backbone circuits on which upstream surveillance was conducted in June of 2015?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Still following instructions.

BY MR. ABDO:

Q What is the approximate combined bandwidth of the Internet backbone circuits on

which upstream surveillance is conducted today?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What are the categories of circuits that were subject to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What are the categories of circuits that are subject to upstream surveillance today?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any individual optical fibers on the Internet backbone subjected to upstream surveillance in June 2015 and/or any individual optical fibers on the Internet backbone subjected

to upstream surveillance today?

MR. PATTON: Just a second.

MR. PADGETT: Could you read back the question?

MR. ABDO: Sure. Let me --

MR. PATTON: I really am listening to your questions.

BY MR. ABDO:

Q I appreciate that. In the interest of speed, I was combining two, but let me be clear.

Are any individual optical fibers on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any individual optical fibers on the Internet backbone subjected to upstream surveillance as of June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Are any subdivisions of optical fibers on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any subdivisions of optical fibers on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Are any wavelengths of light carried on optical fibers on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Were any wavelengths of light carried on optical fibers on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What is the smallest subdivision by bandwidth of an optical fiber on the Internet backbone that was subjected to upstream surveillance in June 2015 and that is subjected to upstream surveillance today?

MR. PATTON: Objection, compound. Objection, same as before, classified.

MR. ABDO: We might go quicker if you would withdraw the compound objection.

MR. GILLIGAN: I like this pace, actually.

BY MR. ABDO:

Q Let me rephrase the question.

What is the smallest subdivision by

bandwidth of an optical fiber on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What was the smallest subdivision by bandwidth of an optical fiber on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same instruction, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What was the largest circuit by bandwidth on the Internet backbone subjected to upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q What is the largest circuit by

bandwidth on the Internet backbone subjected to upstream surveillance today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Is now a good time for you to break, Ms. Richards?

A Sure.

Q Okay, why don't we take a lunch break and go off the record, Dawn.

(Lunch break taken at 12:59 p.m.)

(Resume at 2:06 p.m.)

BY MR. ABDO:

Q We're back from lunch.

Ms. Richards, what does the term "Internet link" refer to?

MR. PATTON: Objection, vague.

THE WITNESS: Is there a specific place where you want me to look for "Internet link," or are you looking for the general telecommunications definition?

BY MR. ABDO:

Q That's right, the general definition.

A So it's similar to a circuit, and there's no special NSA meaning.

Q So the NSA's understanding of that term is consistent with the general understanding of the term within the telecommunications industry?

A That is correct.

Q Okay. What does the term "international Internet link" refer to?

MR. PATTON: Objection, vague, calls for expert opinion.

THE WITNESS: I'm sorry, international --

BY MR. ABDO:

Q International Internet link.

A Is there, again, something specific? I'm not sure of it.

Q The question is whether that term has a meaning to the NSA.

MR. PATTON: Just a second.

I'm just going to object to the extent that any response might call for a classified answer, subject to state secrets, statutory privileges.

If the witness has an unclassified answer, she can provide it.

THE WITNESS: I'm just going to take a minute to make sure I --

(Witness reviewing document.)

So just for clarification, you're looking for the definition of "international Internet link" --

BY MR. ABDO:

Q That's right.

A -- as was originally described in Judge Bates' order?

Q I'm asking for your understanding of it, not for Judge Bates' understanding.

A Okay, I just want to make sure.

So I'll say there's no special NSA meaning.

Q What is the meaning of it though, even

if there's not a special NSA one?

MR. PATTON: Objection to the extent it calls for expert opinion, and to the extent it may call for classified information and statutory privileges.

The witness can answer if the answer is unclassified.

Are you concerned that there's --

THE WITNESS: I'm concerned whether I'm going into classified. I'm just trying to under- -- I'm clicking through my head as to what's classified and what's not classified, so I'm sorry I'm taking a little bit more, and so maybe --

MR. PATTON: Do you need to talk about that?

THE WITNESS: Maybe we should just take a quick minute, go off the record.

MR. ABDO: Okay.

(Off the record at 2:11 p.m.)

(Resume at 2:28 p.m.)

MR. ABDO: Ms. Jaques, do you mind

re-reading the last question asked?

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for expert testimony.

THE WITNESS: I'm going to clarify my answer, which is the logical definition of an international Internet link would be an Internet link between two countries, but it's not I think a well -- it's not a telecommunications -- unlike some of the other descriptions that we provided in terms of "circuit" or "cable" or "Internet backbone," this is not a commonly understood telecommunications word -- or set of three words, I guess.

BY MR. ABDO:

Q Okay. But your understanding of it is a link between two countries essentially?

MR. PATTON: Same objection.

THE WITNESS: Yes, in the broad context of those three words, not in the context of anything specific.

BY MR. ABDO:

Q Okay. I want to go back for a moment to Internet link -- not international Internet link, just Internet link.

You said, I believe, and please correct me if I'm wrong, that it is similar to a circuit. Is that correct? Am I characterizing your previous testimony accurately?

MR. PATTON: Object to the extent it calls for expert opinion.

THE WITNESS: Yes.

BY MR. ABDO:

Q When you say "similar" -- or when you said "similar," did you mean analogous to, or did you mean identical to? I'm trying to understand, if there are differences between an Internet link and a circuit, what you believe those differences to be.

MR. PATTON: Same objection.

THE WITNESS: I don't see them -- I see them as being analogous. So sometimes you use "circuit," sometimes you use "link." I don't see

them as having any real difference between them.

BY MR. ABDO:

Q Okay. Would "interchangeable" be a better word than "analogous" then?

A Yeah.

MR. ABDO: Ms. Jaques, would you mind marking this Exhibit 45?

(Deposition Exhibit 45 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you have in front of you what's been marked as Exhibit 45.

Do you recognize that document?

A I do.

Q What is it? I should say, sorry, it's marked Exhibit 45, and it is Bates numbered NSA-WIKI 149 to NSA-WIKI 229. Wiki is spelled W-I-K-I. What is this document, Ms. Richards?

A This is the Judge Bates' Memorandum Opinion from October 3rd, 2011.

Q Could you turn to page 45, or NSA-WIKI 193 of Exhibit 45, and read the sentence

that begins, "Indeed, the government readily concedes." It is about halfway down the page.

A Got it.

Q "Indeed, the government readily concedes that NSA will acquire a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server."

Is that sentence true?

Let me rephrase that. Was that sentence true at the time Judge Bates issued this opinion?

MR. PATTON: Just a moment.

You can answer.

THE WITNESS: Okay. Yes, that sentence is accurate.

BY MR. ABDO:

Q What do you understand the Foreign Intelligence Surveillance Court to mean in its use of the term "international Internet link" in that sentence?

MR. PATTON: Objection, the question calls for classified information, information subject to the state secrets and the statutory privileges previously mentioned.

I instruct the witness not to answer the question.

BY MR. ABDO:

Q Do you --

A Hold on.

MR. PATTON: Do you have an unclassified response?

THE WITNESS: I have an unclassified response, at least in part.

MR. PATTON: So long as you're comfortable and it's unclassified.

THE WITNESS: NSA -- so unlike the other words that you had me go through in terms of definitions that were telecom provider -- you know, sort of generally what a teleco expert would be, NSA has an understanding of this term that is specific to how Judge Bates described it, but it's classified to provide any further information.

BY MR. ABDO:

Q I understand. Is the NSA's understanding of the term different from the general meaning of the term you described in response to an earlier question as a link between two countries?

MR. PATTON: Objection, calls for information subject to the statutory privilege, and instruct the witness not to answer the question.

THE WITNESS: I will follow instructions.

BY MR. ABDO:

Q Is it your understanding that in using the term "international Internet link," the Foreign Intelligence Surveillance Court meant an Internet link that terminates in a foreign country?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Is it your understanding that an international Internet link is an Internet backbone circuit with one end in the United States and the other end in a foreign country?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Following instruction.

BY MR. ABDO:

Q Is there anything you can tell us unclassified about the nature of the harm that would arise were you to provide an answer to the question of what the term "international Internet link" means as used by the Foreign Intelligence Surveillance Court in Exhibit 45?

MR. PATTON: Object to the question. The witness is not an official classification authority, nor is she the Director of the NSA or the Director of National Intelligence, who would invoke and assert the state secrets privilege to that.

You can answer the question to the

extent it's unclassified.

THE WITNESS: Sources and methods.

BY MR. ABDO:

Q Do you believe that disclosing the NSA's understanding of that term would harm national security?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Which was to not answer, or to answer to the extent --

MR. PATTON: To answer to the extent that you're able. You're not a classification authority, you're not asserting the state secrets.

THE WITNESS: So the question is whether I believe it would harm national security?

BY MR. ABDO:

Q Yes.

A Yes.

Q Do you believe it would substantially harm national security?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Yes.

BY MR. ABDO:

Q Are you familiar with the process through which the government seeks approval from the Foreign Intelligence Surveillance Court to conduct upstream surveillance?

MR. PATTON: Object to the form of that question as vague, and objection, beyond the scope of 30(b)(6).

THE WITNESS: Yes.

BY MR. ABDO:

Q Does the NSA provide information to the Foreign Intelligence Surveillance Court about the operation of upstream surveillance in support of the government's applications to that court to conduct upstream surveillance?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Is the information that the NSA provides in support of the government's applications to the Foreign Intelligence

Surveillance Court supposed to be accurate?

MR. PATTON: Objection. Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Is that information, in fact, accurate?

MR. PATTON: Objection, calls for speculation.

THE WITNESS: To the extent the government's job is to provide the Court with as accurate as information as possible at the time, that is what the NSA does.

BY MR. ABDO:

Q Does the NSA verify, under penalty of perjury, that its submissions to the Foreign Intelligence Surveillance Court are true and correct?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Does the NSA review the Department of

Justice's submissions to the Foreign Intelligence Surveillance Court seeking authority to conduct upstream surveillance?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Does it review the technical explanations of the way that upstream surveillance operates and drafts of those submissions before they are filed with the Foreign Intelligence Surveillance Court?

MR. PATTON: Same objections.

MR. PADGETT: Excuse me, could you read back the question?

(The reporter read back the record.)

THE WITNESS: Okay, yes.

BY MR. ABDO:

Q If there are mistakes in the drafts of the Department of Justice's submissions to the Foreign Intelligence Surveillance Court, would the NSA identify those mistakes to the Department of Justice?

MR. PATTON: Objection, vague.

THE WITNESS: Yes.

BY MR. ABDO:

Q Would it identify any inaccuracies in the explanations of the technical operation or implementation of upstream surveillance to the Department of Justice?

A Yes.

MR. PATTON: Objection, vague and ambiguous, and also beyond the scope of 30(b)(6).

THE WITNESS: Yes.

BY MR. ABDO:

Q To your knowledge, does the Foreign Intelligence Surveillance Court acquire information about the operation of upstream surveillance from anyone aside from representatives of the NSA or the Department of Justice?

MR. PATTON: Objection, calls for speculation. Objection, beyond the scope of 30(b)(6).

THE WITNESS: What time frame would

you be asking about? Just in general? Over a specific time frame?

BY MR. ABDO:

Q Why don't we -- if you can answer in general, please do. If you can't, let me know.

MR. PATTON: Are you asking -- I'm sorry, does this include just Upstream?

MR. ABDO: Just Upstream.

MR. PATTON: Same objections.

THE WITNESS: To the extent that the new law that was passed, and actually some previous ones over the last couple years, allow for an Amicus, there's certainly that opportunity for the Court to include that type of additional expert outside advice. Similarly -- yeah.

BY MR. ABDO:

Q The new law you're referring to is the USA Freedom Act?

A Yes. I'm sorry, yes, USA Freedom Act, and then the --

Q The reauthorization --

A -- reauthorization for 702 also has

the Amicus portion of it.

Q Is there anyone else, to your knowledge, from whom the Foreign Intelligence Surveillance Court might acquire information about the operation of upstream surveillance?

MR. PATTON: Same. Hold on.

(Counsel conferring.)

MR. PATTON: So same objections as before. There are, as you know, some ex parte communications, and while I'm a Department of Justice Civil Division attorney, I'm not a Department of Justice national Security Division attorney, and so there may be other things that the witness is not aware of.

Again, I'd objected before to the fact that the it was beyond the scope of 30(b)(6), so she may not be aware of certain other things that may go on that I'm not aware of as well. I don't want the record to be unclear. That's potentially beyond her personal knowledge.

MR. ABDO: Understood. To the extent you know the answer --

THE WITNESS: So his answer was exactly what I was about to say before we -- before my lawyer said that, which is fantastic, so I've given you the information I know.

I don't work for the FISC, I don't do anything before the FISC, so what the FISC -- what else the FISC has at their disposal is up to the FISC.

BY MR. ABDO:

Q Do you know whether the NSA reviews or participates in any review of opinions of the Foreign Intelligence Surveillance Court concerning upstream surveillance before those opinions are signed or issued?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Would you just read that back? I think it's fine, but I just want to be double sure.

(The reporter read back the question.)

MR. PATTON: Object as beyond the scope of 30(b)(6), but if you have personal

knowledge, you can give it.

THE WITNESS: To the best of my knowledge, no.

BY MR. ABDO:

Q If the NSA identifies an inaccuracy in an opinion of the Foreign Intelligence Surveillance Court concerning upstream surveillance after that opinion is issued, would the NSA notify the Foreign Intelligence Surveillance Court of that inaccuracy?

MR. PATTON: Objection. Same as before, beyond the scope of 30(b)(6).

You can answer if you know.

THE WITNESS: I think that's when you would go to the FISC Review Board. You would do an appeal.

BY MR. ABDO:

Q What if it were not a judgment that the Department of Justice or the NSA disagreed with, but a factual misstatement in the opinion that would not give rise to or necessitate an appeal?

MR. PATTON: Same objection.

THE WITNESS: It would be fact specific. I can't speak to one way or another.

BY MR. ABDO:

Q Okay. Do you imagine that it would be good practice for the NSA to correct factual misstatements in the Foreign Intelligence Surveillance Court's opinions if and when they identify them?

MR. PATTON: Objection, calls for a legal conclusion, opinion, speculation, and beyond the scope of 30(b)(6).

THE WITNESS: Again, I think it would have to be very fact specific -- you know, the sort of situation and fact specific would have to decide what to do next, but, I mean, it's an Article III judge signing something. We're not really one part of the government saying something to the other part of the government. You may want to be thoughtful about how to do that.

BY MR. ABDO:

Q Understood. Are there any

inaccuracies that you're aware of relating to the operation of upstream surveillance in Exhibit 45, October 3rd, 2011, Foreign Intelligence Surveillance Court opinion?

MR. PATTON: Objection, vague as to time, and object to the extent it calls for classified information or statutory privileges information.

The witness can answer to the extent unclassified.

THE WITNESS: So you're asking if there's any information as of October 3rd, 2011, that we believe would have been inaccurate in Judge Bates' Memorandum and Opinion?

BY MR. ABDO:

Q Yes.

A To the extent that there are certain opinions that the judge makes as it relates to different aspects of this, those are the opinions of the Court and not necessarily those of NSA.

To the extent that there are facts in here, I believe we stand behind those facts, as

they're based off of the submission from June 1st that the government made in the subsequent submissions.

Q Okay. Did the NSA conduct a declassification review of Exhibit 45?

A Yes.

Q I assume that was a thorough review?

A Yes.

Q And anything that would disclose classified information, the NSA would identify as classified to the FISC so as not to release it to the public?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: I'm sorry, could you read that question back?

BY MR. ABDO:

Q Let me rephrase it. That's all right.

Did the NSA -- sorry.

If the NSA identified classified information -- let me -- sorry, let me start over.

Who actually disclosed Exhibit 45 to

the public?

MR. PATTON: Objection, vague.

THE WITNESS: It's a FISC document, so while the government has -- while the Executive Branch reviews it for classification, I believe the FISC issues it, although I know that the documents actually sit on ODNI's website.

BY MR. ABDO:

Q Are the redactions in this opinion in Exhibit 45 the government's redactions or the FISC's redactions?

A So the process is with all these documents that the government -- the Executive Branch will review them for classification and suggest redactions, and then the FISC has the opportunity to say no, I think these should be put out, and there was a conversation. But as a general matter, I guess they're really the FISC's document.

Q Do you know whether there's any dispute between the NSA or the Department of Justice with the FISC relating to the

classifications in Exhibit 45?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: My colleague was just getting warm. You can keep answering the question.

THE WITNESS: Okay.

MR. PATTON: I think there's some confusion back and forth as to this particular document, when it was declassified, and then the standard way that it's now under USA Freedom Act taken care of.

But this was, as you know, declassified prior to USA Freedom Act, and so I want to make sure the witness's answers are both accurate and reflective of what occurred.

BY MR. ABDO:

Q Right. I'm asking specifically about this opinion, Exhibit 45.

A And to which I don't know. I was not working at NSA. This I believe was declassified in 2013, and I was not working at NSA at that

point, so I don't have any specific knowledge on that fact.

Q Is there somebody at NSA who would know the answer to that question?

A I imagine the answer is that there wasn't any disagreement, that this is the document that went out.

Q Just to confirm though, you say you imagine that. Is that a guess, or is that --

A No, that's a statement. I mean, this is the document that went out. If there were any disagreements, those were resolved.

Q Okay.

A There's no further information that can be provided as to what those would be or not be.

Q Okay. Would the NSA treat statements in a FISC opinion as classifiable if they revealed information that the government considered classified?

MR. PATTON: Objection to the question. It calls for the expertise of an

original classification authority, and it's beyond the scope of 30(b)(6). You can answer.

THE WITNESS: I'm not sure I understand your question, so ...

BY MR. ABDO:

Q Let me ask it a slightly different way.

Would the NSA treat a statement in a FISC opinion as classifiable if it revealed information the government considered classified even if the FISC were not quoting a statement made by an Executive Branch agent?

MR. PATTON: Objection.

BY MR. ABDO:

Q In other words, if the FISC were to make a factual statement using its own words about the operation of upstream surveillance, and the NSA believed that statement revealed classified information, would the NSA consider that statement to be classifiable?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. Does the NSA conduct upstream surveillance on one or more international Internet links? I'm looking for a yes or no, not a specific number.

(Counsel conferring.)

MR. PADGETT: Could you read it back?

(The reporter read back the question.)

MR. PATTON: I misheard, so object to that as seeking classified information, subject to state secrets and statutory privileges.

Instruct the witness not to answer the question.

THE WITNESS: I'll follow the --

BY MR. ABDO:

Q Did the NSA conduct upstream surveillance on one or more international Internet links in 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Does the NSA conduct upstream surveillance today on more than one international Internet links?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q Did the NSA conduct upstream surveillance on more than one international Internet links in June of 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instruction.

BY MR. ABDO:

Q What is the number or approximate number of international Internet links on which the NSA conducted upstream surveillance in June of 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the direction.

BY MR. ABDO:

Q What is the approximate number of international Internet links on which the NSA today conducts upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Okay. Is upstream surveillance conducted on any international submarine cables?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instructions.

BY MR. ABDO:

Q Was upstream surveillance conducted on any international submarine cables in June of 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q What is the number or approximate number of cables on which the NSA conducted upstream surveillance in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q What is the number or approximate number of cables on which the NSA today conducts upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Okay. In the context of upstream surveillance, can you tell me what an international chokepoint is?

MR. PATTON: Just a second.

Will you just read it back, please?

(The reporter read back the question.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q Is upstream surveillance today conducted at one or more international chokepoints?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q Was upstream surveillance in June 2015 conducted at one or more international chokepoints?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q What number, approximate number, of international chokepoints was upstream

surveillance conducted on in June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q What number, approximate number, of international chokepoints is upstream surveillance conducted on today?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. ABDO:

Q I want to go back to page 45 very briefly of Exhibit 45, the sentence we were talking about before, the one that begins, "Indeed, the government readily concedes."

A Yes, okay.

Q Is there a term -- well, let me scratch that for a moment.

A moment ago I asked you whether the government conducts upstream surveillance on one or more international Internet links in 2015, then

I asked about today.

Is there a way I could phrase that question that would allow you to respond with an unclassified response more fully than you've responded so far?

MR. PATTON: For any given time period?

MR. ABDO: For June 2015 to today, and in 2011, at the time of -- let me try rephrasing one thing.

As of October 3rd, 2011, did the NSA conduct upstream surveillance on one or more international Internet links?

MR. PATTON: Same objection, same instruction.

BY MR. ABDO:

Q Is there a way that I could rephrase that question to use a term other than "international Internet link" that would allow you to provide an unclassified response?

(Counsel conferring.)

MR. PATTON: We don't think she can.

This is Rodney Patton, counsel for government.

We don't think she can answer that as to specific time periods for anything related to international Internet link. There may be a more general statement that she can make, but I feel like she's probably already provided that to you.

MR. ABDO: Okay.

MR. PATTON: Perhaps if we could go out and check, we might be able to come up with --

MR. ABDO: Maybe at the next break. You can add this to --

MR. PATTON: That's fine.

BY MR. ABDO:

Q So back to page 45 very briefly of Exhibit 45. Do you understand the sentence we've been discussing, the one that begins, "Indeed, the government readily concedes," to confirm that, as of October 3rd, 2011, that the government in fact conducted upstream surveillance at at least one international Internet link?

MR. PATTON: Objection, mischaracterizes the language of page 45 of

Exhibit 45.

BY MR. ABDO:

Q You can answer.

A Do you want me to answer?

MR. PATTON: Not as it's phrased, no, she can not answer that question. It would call for a classified answer.

MR. ABDO: I'm sorry, I didn't hear that. So you're instructing the witness not to answer?

THE WITNESS: Yeah, that's classified.

BY MR. ABDO:

Q Okay. Do you understand the sentence to confirm that if a transaction -- that as of October 3rd, 2011, the NSA would in fact acquire a wholly domestic -- sorry, would in fact acquire a wholly domestic "about" communication if the transaction containing the communication were routed through an international Internet link being monitored by the NSA?

MR. PATTON: Objection as not exactly what the language of the sentence said. Let me

see if she can answer that question.

To avoid us having to go out to the SCIF and come back again, she can answer whether or not the statement in this, as exactly written, is correct as of October 3rd, 2011, in a yes-or-no answer. I believe she's already answered that, but --

MR. ABDO: I think you did already answer that this sentence, as written, is true as of October 3rd, 2011.

MR. PATTON: That she can answer.

MR. ABDO: Okay.

THE WITNESS: Do you want me to say it again?

BY MR. ABDO:

Q Sure.

A Yes, that sentence is accurate as of October 3rd, 2011.

Q Okay. Let me go back to Exhibit 42.

A Which one is 42?

Q The NSA's Responses and Objections to Plaintiffs' First Set of Interrogatories.

I direct your attention to page 7 to 8.

A 7 to 8, oh, yes.

Q The paragraph that carries over between the two, which is labeled "RESPONSE."

Would you mind just reading that to yourself?

MR. ABDO: Why don't we take a break right now. Can we go off the record for a minute?

(A break was taken at 3:06 p.m.)

(Resume at 3:15 p.m.)

BY MR. ABDO:

Q Ms. Richards, have you had a chance to look at page 6 of Exhibit -- sorry, page 7 to 8 of the carryover paragraph on pages 7 to 8 of Exhibit 42, the NSA's response to Interrogatory No. 3?

A Yes.

Q Is there anything beyond that response in Exhibit 42 that isn't classified that you could provide us about the NSA's understanding of the term "filtering mechanism," both in June 2015 and

today?

A Those are pretty good definitions you've got right there. I don't have anything else to add.

Q Does that mean that there isn't anything unclassified that you could add to those definitions?

A There's nothing unclassified I can add to those descriptions.

Q Okay. With respect to upstream surveillance as it operated in 2015, did the term "filtering mechanism" include the use of, quote, an Internet protocol filter to ensure that the person from whom the NSA seeks to obtain foreign intelligence information is located overseas?

A In 2015, filtering mechanism would have -- one of the examples that was used -- I'm sorry.

An example of a filtering mechanism was an IP address -- sorry. (Reviewing document.)

Okay, let me revise -- I'm sorry, let me just revise my answer.

Q Sure.

A So I would actually add from the Civil Liberties and Privacy Office Report, which is Exhibit 44, on page 5, where we give an example that, in certain circumstances, NSA's procedures require that it employ an Internet protocol filter to ensure that the target is located overseas.

Q Does that mean the answer to my question is yes, that the filter you just described is part of the filtering mechanism described in the NSA's response to Interrogatory No. 3?

A Yes, and so I was correcting the fact that when I said that was everything you could say in an unclassified.

What I'm saying is I'm correcting the record to say I could have additionally added the fact that that would include the IP -- that could include -- could include --

Q Could include, understood.

A -- as an example of what the filtering mechanisms are, so ...

Q In June of 2015, did the term "filtering mechanism" include the use of an Internet protocol filter? I'm trying to understand "did" versus "could" include.

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Object to form, vague.

You can answer.

THE WITNESS: Okay. To the extent that the information is classified -- to the extent that how this exactly works is classified, I use the term "could" as one of the examples of what a filtering mechanism is.

I can neither confirm nor deny exactly what was happening in 2015 as it relates to the specificity of the filtering mechanism. I can just tell you that it could include that as an example.

BY MR. ABDO:

Q Can you confirm whether it did include an Internet protocol filter as of the date of Exhibit 44, April 16th, 2014?

A As is specifically stated on page 5, it's a "could." It's not a "did."

Q Just for the record, could you tell us where you're reading from on page 5?

A Sure. It's the very last sentence on page 5 of Exhibit 44 that begins with "for example."

Q "In certain circumstances, NSA's procedures require that it employ an Internet protocol filter to ensure that the target is located overseas."

So in certain circumstances, they're required to.

A Mm-hmm.

Q Can you tell us what those certain circumstances would be in unclassified terms?

MR. PATTON: No, she can't. Object to the question to the extent it calls for classified information --

THE WITNESS: The information -- oh.

MR. PATTON: -- subject to the state secrets and statutory privileges, and instruct the

witness not to answer.

THE WITNESS: I'll follow.

BY MR. ABDO:

Q With respect to upstream surveillance as it operated in 2015, did the term "filtering mechanism" include, quote, the use of a screening device in the upstream Internet collection process to acquire only Internet transactions containing at least one task selector?

A It appears you're reading from something. Could you just refer me to where those words exactly are to make sure I have the full context?

Q Sure. The last portion of my question was a direct quote from the NSA's response to Interrogatory No. 5 in Exhibit 42 on page 10, the text marked "RESPONSE."

A Okay. And so could you read your question once more?

Q With respect to upstream surveillance as it operated in 2015, did the term "filtering mechanism" include, quote, the use of a screening

device in the upstream Internet collection process to acquire only Internet transactions containing at least one task selector?

A So I would look at Interrogatory 4. I understand you pointed me to the response to Interrogatory 5, but the process is we filter for wholly domestic communications, and then we do the scanning to ensure that we're only -- we're doing a scan using a screening device designed to identify for acquisition Internet transactions.

And in 2015, it would have been to, from, or about persons targeted; today, it's to or from persons targeted, in parens, with our targeting procedures.

Q Okay. What I'm trying to understand is whether the use of a screening device is part of the filtering mechanism process described in NSA's response to Interrogatory 3?

MR. PATTON: Objection, calls for information that's classified, subject to state secrets and statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Follow instruction.

BY MR. ABDO:

Q Would you be able to answer the question if I asked whether the use of a screening device could be part of the filtering mechanism described in the NSA's response to Interrogatory 3 on pages 7 to 8 of Exhibit 42?

MR. PATTON: Just a second.

Can you read back that question?

BY MR. ABDO:

Q Let me state it more clearly because that's a bit fragmentary.

With respect to upstream surveillance as it operated in 2015, could the term "filtering mechanism" include, quote, the use of a screening device in the upstream Internet collection process to acquire only Internet transactions containing at least one task selector?

MR. PADGETT: I'm sorry, I need to hear that one more time.

(The reporter read back the question.)

MR. PADGETT: I guess I would ask,

before we instruct the witness whether they can answer or not, are you referring to filtering mechanism as used in the document that's referred to by Interrogatory No. 3?

MR. ABDO: Yes.

MR. PADGETT: So can we see?

MR. ABDO: It's one of your briefs from the Fourth Circuit.

MR. PATTON: Let's go off the record.

(Off the record at 3:26 p.m.)

(Resume at 3:38 p.m.)

(The reporter read back the question.)

MR. PATTON: Objection, vague.

You can answer.

THE WITNESS: Okay. So I think the best description for how the process works in the unclassified realm is going to be on page 37 of the PCLOB Report, which is Exhibit 43.

To the extent that the -- so where it says -- the sentence starting, "The provider is compelled to assist the government in acquiring communications across these circuits, to identify

and acquire Internet transactions associated with the Section 702 task selectors on the Internet backbone. Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a task selector."

Now, my understanding is that there's this other brief that comes up with a new term called "filtering mechanisms"; that's not meant to be something special or otherwise different from the process that was described in PCLOB.

To the extent that you have specifics about the how and the when and the what, that would be classified, but those were not designed to be somehow describing something different.

BY MR. ABDO:

Q Okay. And for the record, you're reading from the top of page 37 of Exhibit 43, correct?

A That is correct.

Q The sentence beginning, "To identify and acquire"?

A That is correct.

Q So would the use of an IP filter fall within the description of that sentence in which it says, "Internet transactions are first filtered to eliminate potential domestic transactions"? Is that where an IP filter could be used?

A Yes, that is an example of where -- an IP filter is an example of something that could be used to do that filter.

Q Okay. And is the use of a screening device described in the NSA's response to Interrogatory 5 in Exhibit 42, is that use of a screening device what could be used to accomplish what is described in the second portion of the sentence that you were reading from page 37 of Exhibit 43, that second part saying, quote, then our screened capture only transactions containing a task selector?

A Yes.

Q Okay. And with respect to upstream surveillance as it operated in 2015, what else could the term -- sorry, what else -- what other

processes could be used to accomplish either the filtering or the screening described in the sentence you were reading from page 37 of Exhibit 43?

MR. PATTON: Objection, calls for classified information, information subject to the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Okay. Are all transactions that were subject to upstream surveillance in June 2015 subjected to Internet protocol filtering --

MR. PATTON: Objection.

BY MR. ABDO:

Q Sorry, let me just finish the question real quick.

-- to eliminate potential domestic transactions from upstream surveillance?

MR. PATTON: Objection, calls for classified information, information subject to the

statutory privileges.

Instruction not to answer the question.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Can you please describe all the ways in which the NSA could determine in 2015 or could determine today whether a transaction is wholly domestic in order to filter it out from upstream surveillance?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Could you break that down into 2015 to 2017 to make it clear?

BY MR. ABDO:

Q Could you please describe all the ways in which the NSA could determine in 2015, as part of upstream surveillance, whether a transaction is wholly domestic so as to filter it out?

MR. PATTON: Objection, calls for classified information in order to respond fully

to that question.

There may be an unclassified response to that question, but without knowing what the witness's answer would be, I'm not comfortable just turning that over to her, but I believe there is an unclassified response, but it's also one that she has given you already.

BY MR. ABDO:

Q Okay. If there's nothing more that you could say that's unclassified, let me know that you'll follow your counsel's instruction not to provide any further information.

A There's no additional information that can be provided. What you see here is as much unclassified information as available.

Q And by "here," you're referring to Exhibit 43, page 37?

A Page 37, or the interrogatories.

Q The responses we've been discussing?

A The responses, yeah. There's no additional information to be provided.

Q Okay. What does it mean to say, as

the NSA's response to Interrogatory 3 does, that wholly domestic Internet transactions are, quote, eliminated? And that's in Exhibit 42, I think at page 7 to 8.

MR. PATTON: Object to the extent it calls for classified information and information protected by the statutory privileges.

There is an unclassified answer that the witness can give.

THE WITNESS: So you're asking what does it mean to eliminate?

BY MR. ABDO:

Q Yes.

A So I think if you look at the response, it's important to understand that it starts with -- the sentence is that the devices utilized in the upstream Internet collection process that were designed to eliminate wholly domestic transactions.

So they were -- it's important to recognize it was designed, not that it was actually done.

Q Understood. So let me then be clear.

What does it mean to say -- what were they designed to do in eliminating wholly domestic --

A So that they wouldn't --

Q -- transactions?

MR. PATTON: Same objection, same instruction.

THE WITNESS: They're designed so that they don't make it through to being ingested by NSA's -- into NSA's repository. That's what it means to be designed to eliminate.

BY MR. ABDO:

Q And the repository is what holds communications that contain a selector and are not wholly domestic as of June 2015?

MR. PATTON: Object to the extent it calls for classified information and statutory privileges. You can answer to the extent unclassified.

THE WITNESS: So --

BY MR. ABDO:

Q I'm just trying to understand.

When you say "ingested," you're referring to the databases or the places in which the NSA stores communications that are ultimately authorized by Section 702 to collect?

A Yes, yes. It's when NSA collects it.

MR. PATTON: Same objections.

THE WITNESS: Yes. NSA collects, acquires, ingests. It's the point at which NSA now has it.

BY MR. ABDO:

Q Understood. Can an e-mail address be a selector under upstream surveillance?

A Yes.

Q Can a phone number be a selector under upstream surveillance?

A Yes.

Q Can an Internet protocol address be a selector under upstream surveillance?

MR. PATTON: Objection, calls for classified information and privileged information

pursuant to the statutes aforementioned, and instruct the witness not to answer the question.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Can a URL, or uniform resource locator, be a selector under upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

MR. PATTON: Just a moment.

MR. PADGETT: Let's go off the record to discuss.

(Off the record at 3:49 p.m.)

(Resume at 3:53 p.m.)

BY MR. ABDO:

Q We're back from break, and the question was can a URL be a selector under upstream surveillance?

MR. PATTON: Objection, calls for

classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will not answer.

BY MR. ABDO:

Q Could a URL be a selector under upstream surveillance as of June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. ABDO:

Q Are the selectors used for upstream surveillance the same as those used for PRISM surveillance as of June 2015?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Wait, I'm sorry. Can you ask the question again?

BY MR. ABDO:

Q Sure. I'll modify it slightly to make it grammatically correct.

Were the selectors used for upstream surveillance the same as those used for PRISM surveillance in June 2015?

MR. PATTON: Same objection, same instructions.

THE WITNESS: Can you just --

MR. ABDO: Ms. Jaques, would you mind marking this as Exhibit -- you're still looking at something for this question?

THE WITNESS: Yes, I am.

The only thing I would state which is definitely not classified is on page 6 of the Civil Liberties and Privacy Office Report, Exhibit 44. At the very top of page 6 it says, "The process for approving the selectors for tasking is the same for both PRISM and upstream collection."

I realize that's not exactly the question you were asking, but I just wanted to make sure you had that piece of information.

BY MR. ABDO:

Q Thank you. Ms. Jaques, would you mind

marking this 46? And it's the entire folder.

(Deposition Exhibit 46 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards --

A Oh, this is fabulous, okay.

Q You have in front of you what's marked as Exhibit 46. Do you recognize that document?

A I do.

Q And what is that document?

A This is the Privacy and Civil Liberties Oversight Board Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, March 19, 2014.

Q Did employees of the NSA testify at that hearing?

A Yes.

Q And they were testifying in their official capacity as NSA employees?

A Yes.

Q Could you turn to page 57 of the

transcript? Do you see at lines 17 to 20 there's a statement that's labeled as coming from Mr. De, spelled D-E?

Do you understand that to be -- who do you understand that to be?

A I'm sorry, we're at line?

Q Lines 17 to 20 of page 57.

A 17 to 20, okay.

Q Of Exhibit 46.

A Mr. De. Oh, let me just --

Q Before getting to the substance of that sentence, which we'll give you a chance to read in a second, do you know who this Mr. De is who is being referred to?

A Yes. He was the general counsel at the time of NSA.

Q And for the record, his full name is Rajesh De?

A Yes.

Q Could you now read those two lines -- those four lines, 17 to 20 on page 57, to yourself?

A (Witness reviewing document.) Okay.

Q What do you understand Mr. De to have been communicating in this first sentence? And the first sentence was, quote, "And it's the same selectors that are used for the PRISM program that are also used for upstream collection."

MR. PATTON: Objection to form, vague.

MR. ABDO: You can answer.

THE WITNESS: I think similar to what I just read to you, the words on the face of it seem accurate.

I'm not sure what you're trying to ask me. Maybe you can help clarify.

BY MR. ABDO:

Q What I'm trying to understand is whether the selectors that are used for PRISM are also used for Upstream collection, and that seems to be on the face of the statement what Mr. De said at the hearing transcribed in Exhibit 46, but I understood you to refuse to answer the question of whether the selectors that are used for the PRISM program are also used for Upstream

collection, so I'm trying to understand what the difference is between my question and this statement.

A I think I need to go -- sorry.

MR. PADGETT: Can I ask a clarifying question? Because it might involve an instruction.

MR. PATTON: Right. There's also a difference of what we're talking about here, so I don't know whether the witness is aware of that, the differences.

MR. ABDO: Are you saying you need to talk in the SCIF?

MR. PATTON: I don't know that we need time to talk in the SCIF, but the objection was to something A, and this is meaning something B, if you know what I mean, and therefore I want to get you that answer because I think that answer is unclassified.

MR. ABDO: Is there an answer that the witness --

MR. PATTON: Because I can understand

why you're having this question, but I'm trying to figure out the best way to get you that unclassified answer.

BY MR. ABDO:

Q Ms. Richards, do you understand the distinction your counsel is drawing between this statement by Mr. De at the hearing transcribed in Exhibit 46 and the question that I asked a few moments ago about whether selectors used for Upstream are the same as those used for PRISM surveillance?

If you know the answer to my question, could you please answer it?

A So let me see if I can restate the two different questions, and maybe I need to have you read back to me what you asked before and we objected to on classified, which is this statement states, "it's the same selectors that are used for the PRISM program that are also used for upstream collection."

A few minutes ago, you had asked whether this was true, and I declined to comment

for classified purposes.

Q Right.

A That's the --

Q Well, let me phrase it this way.

Is the statement that Mr. De made at this hearing in March of 2014 true, or was it true at that time that, quote, it's the same selectors that are used for the PRISM program that are also used for upstream collection?

A I would like to confer in the SCIF before I give you the answer to both of those questions.

MR. PATTON: I just want to seek clarification for the record.

Are you concerned that there's a privilege issue, a classification issue? Is that your concern?

THE WITNESS: Yes.

MR. PATTON: Okay.

THE WITNESS: Not with this sentence.

MR. PATTON: Not with the sentence, but whether or not you can answer --

THE WITNESS: With the other question that was asked.

BY MR. ABDO:

Q I see. If I were to rephrase my previous question to be were the selectors used for PRISM surveillance in June 2015 the same as those used for Upstream surveillance?

MR. PATTON: I have to object to the question as to its vagueness. There is an unclassified answer and there's a classified answer, and --

THE WITNESS: And I'm tripping over which one, so I just need to go --

MR. PATTON: -- and I want to get you the unclassified answer.

MR. ABDO: Okay. Can we take a break and go off the record while you guys confer in the SCIF?

(Off the record at 4:03 p.m.)

(Resume at 4:13 p.m.)

BY MR. ABDO:

Q We're back on the record.

The question we left with, Ms. Richards, was what Mr. De meant in the hearing in March 2014, transcribed in Exhibit 46, when he said, "And it's the same selectors that are used for the PRISM program that are also used for upstream collection."

MR. PATTON: Objection to the extent it calls for classified information and information protected by the statutory privileges.

You can answer to the extent unclassified.

THE WITNESS: Okay. So in looking at page 57, it's important to roll back to roughly around page 55 and understand what they were talking about at this point. And, specifically, I would bring you to -- okay, I'm sorry, go back to 54. Where did the language just go? Okay, I'm sorry, page 56.

So Mr. Wiegmann says, "About that selector, correct."

And then Mr. De says, "It is always focused on that account, so I think the key is,

the misperception that some may have that 'about' collection is somehow about a key word or about the person that may be behind that account.

"But all collections under Section 702, whether it's upstream abouts, which is a subset of upstream, or PRISM is all based on the selectors at issue."

Then we have Ms. Brand says, "Just to follow-up on that because that's a good line of inquiry, just to make sure that everyone understands. So you're saying that if someone is emailing about Rachel Brand or about explosives that would not be a permissible about query under your explanation?"

And Mr. De goes on, and what he's explaining then, when we get down to lines 17 to 20, is the type of selectors is the context for this exchange back and forth, which is then how this is -- in talking about the types of selectors, as opposed to "bomb" or "explosive" or a name, he's explaining that these are the same types of selectors.

That is what's the unclassified fact, and then it's furthered by the sentence I mentioned in the Civil Liberties and Privacy Office Report, as opposed to your question you asked earlier where we said that's classified.

BY MR. ABDO:

Q I think I understand.

A Okay.

Q Moving on a bit.

As of 2015, did the procedures approved by the FISC for upstream surveillance permit the NSA to collect an international HTTP transmission of a website if the text of that website contained a selector?

MR. PATTON: Objection, calls for classified information and information subject to the statutory privileges.

Instruct not to answer the question.

THE WITNESS: I will follow the instruction.

BY MR. ABDO:

Q Okay. Sorry, just one second.

(Deposition Exhibit 47 was marked for identification.)

BY MR. ABDO:

Q Ms. Richards, you have in front of you what's been marked as Exhibit 47.

Do you recognize this document?

A Yes.

Q What is it?

A This is the government's response to the Court's briefing order of May 9th, 2011.

Q With the Court being the Foreign Intelligence Surveillance Court?

A Yes.

Q Do you know which agency of government authored this document?

A It's submitted by the National --

MR. PATTON: Objection to form, vague.

THE WITNESS: -- National Security Division of the Department of Justice, and verified by National Security Agency.

BY MR. ABDO:

Q Okay. When you say "verified," you

mean verified as to the accuracy of the statements within it?

A Yes, to the best of the knowledge of the individual doing it.

Q Would you mind turning to page 30 of Exhibit 47? And I should have mentioned at the outset, Exhibit 47 is Bates stamped NSA-WIKI 237 -- sorry, I may not have the full version in mine. Sorry, NSA-WIKI 234 to 277.

Okay, if you turn to page 30, which is marked NSA-WIKI 266, toward the bottom there's a sentence that begins "this figure," and I'll read it. "This figure was then compared to the total take of Section 702 upstream collection of web activity for the month."

Do you know the context in which this sentence was written in unclassified terms?

A Can you clarify your question? I'm not sure I know what you're asking.

Q Was the context of this sentence an effort to respond to the FISC's inquiry of the NSA about the volume of certain forms of the NSA's

upstream collection?

A Can you repeat?

Q I'll repeat that.

Does this sentence come in a paragraph responding to the FISC's inquiry of the NSA about the volume of certain forms of the NSA's upstream collection activity?

A Yes.

Q And was this sentence explaining how the Department of Justice and the NSA arrived at certain figures it was relaying to the FISC in responding to the question?

A Yes.

Q What does "web activity" mean in the context of Internet communications?

MR. PATTON: Object to the form of the question to the extent it calls for a classified answer or an answer that would be subject to the statutory privileges.

The witness can answer if there's an unclassified answer.

THE WITNESS: I'm going to read this

answer over once more before I give you --

BY MR. ABDO:

Q Please. Maybe I can rephrase the question for you.

A Sure.

Q Do you understand "web activity" to refer to activity of the World Wide Web -- or activity on the World Wide Web?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: I'm just going to object to the vagueness.

THE WITNESS: I would refer that to meaning as a way of generally talking about the collection of discrete Internet communications.

BY MR. ABDO:

Q Would you understand it to refer to collection -- let me ask this.

Would Internet web browsing constitute web activity?

MR. PATTON: Objection, calls for classified information to the extent that it's

being asked in the context of upstream collection in this particular document, and subject to that objection and to the statutory privileges that would protect that.

I instruct the witness not to answer the question.

THE WITNESS: I will follow the instruction.

BY MR. ABDO:

Q Do you understand the meaning of the term "web activity" generally, not with regard to this document?

A Yes.

MR. PATTON: Object. Object that it's beyond the scope of the 30(b)(6), but the witness can answer.

BY MR. ABDO:

Q What does it mean generally beyond -- you know, outside of the context of this document, Exhibit 47?

MR. PATTON: Same objection.

THE WITNESS: You say activity on the

Internet?

BY MR. ABDO:

Q Any activity on the Internet. You don't understand "web activity" to be distinct from "Internet activity"?

MR. PATTON: Same objection.

THE WITNESS: I think it's a vague enough term it could be meant any number of different things.

BY MR. ABDO:

Q You don't understand it to mean specifically the protocol referred to as the World Wide Web, which encompasses HTTP and HTTPS communications? That's not how you understand an Internet professional would understand that term?

MR. PATTON: Same objection, adding objection that it calls for expert opinion, and also object that it's asked and answered.

THE WITNESS: I don't think there's a set definition for "web activity." I think it could mean Internet activity, it could mean World Wide Web activity. It could mean any of those

different -- those particular different ones.

I think you have to look at the context for the sentence, and then make a decision accordingly.

BY MR. ABDO:

Q Do you have any reason to believe that this sentence was inaccurate, "this sentence" again in Exhibit 47 beginning, "This figure was then compared"?

A No.

Q Does it disclose classified information?

MR. PATTON: As redacted?

MR. ABDO: As it appears in Exhibit 47.

THE WITNESS: I don't think so.

BY MR. ABDO:

Q To your knowledge, is the term "web activity" ever otherwise used by the NSA in publicly disclosed documents interchangeably with "Internet activity" at large?

MR. PATTON: Object to the form,

vague.

THE WITNESS: I don't know that I've seen "web activity" used in other documents that are unclassified -- that have been declassified. To the extent you're going to show me one next --

BY MR. ABDO:

Q I don't have one. I'm asking.

A So if this is the only instance of this and you're -- you know, I don't have -- I haven't seen it in any of the other documents I've read in the last few weeks, or since we've been prepping for this, so --

Q I'm not trying to play a game of gotcha. I'm asking because your answer suggested that you believe "web activity" to be essentially used interchangeably with the very generic term "Internet traffic" or "Internet communications," and I would assume, if that were the case, then the NSA would in fact use that term interchangeably, but I don't believe that to be the case. I'm asking why that is.

MR. PATTON: Object to the extent it

mischaracterizes prior testimony.

THE WITNESS: I don't have any specific further information that would help elucidate this conversation.

Anything further I might say would go into a classified discussion, and so I can't give you any further explanation as to the use of the word "web" there.

BY MR. ABDO:

Q Under upstream surveillance, as conducted in June 2015, was the NSA permitted to collect the communications of a foreign target with a website in the United States?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Object to the form, vague and ambiguous, and also object that it could call for classified information and information protected by the statutory privileges.

Depending on what the question means, there might be an unclassified answer.

BY MR. ABDO:

Q Do you have an unclassified answer, Ms. Richards?

MR. PATTON: And if she does, I'd like to hear it before she gives it to make sure that it is unclassified.

BY MR. ABDO:

Q Let me give you another question to consider.

A I was just going to say, do you have a whole bunch of them, and then we can go and confer on what those might be?

Q I have one other.

A Okay, but could you repeat that one again?

Q Let me repeat that one, and I'll tell you the other one.

A Yeah.

Q The first one is, under upstream surveillance as approved as of June 2015, was the NSA permitted to collect the communications of a foreign target -- that is, somebody who is a

foreign target of upstream surveillance -- abroad with a website in the United States?

Do you understand my question?

A I do understand.

I don't think there's an unclassified answer, but to the extent --

Q Okay. The second question that I hope you'll consider in the SCIF, under upstream surveillance as it was implemented in June 2015, was the NSA permitted to collect the transactions or communications of a non-targeted foreigner abroad with a website in the United States if the website contained a selector tasked for collection?

A A non-targeted foreigner abroad on a U.S. --

Q With a website in the United States.

A With a website in U.S.

Q If the website contained a selector task for collection. You're generally --

MR. GILLIGAN: I'm baffled by the question.

MR. ABDO: A non-foreign target -- I'm sorry, a non-targeted foreigner abroad communicating with a website in the United States, and the website contains a selector.

MR. GILLIGAN: You mean communicating with a website?

MR. ABDO: Yeah. They visit the website, for example. They're communicating with a website.

MR. GILLIGAN: Yeah, that's what was baffling, what you meant by "with."

MR. ABDO: Communications to and from.

THE WITNESS: So the selector is looking at the website?

BY MR. ABDO:

Q Suppose a non-targeted foreigner abroad is viewing a website, and the website is stored on a web server in the United States, and it contains a task selector --

A The website?

Q The website. And that task selector is being communicated back to this non-targeted

foreigner abroad, and it passes through something being monitored by the NSA in upstream surveillance, did the NSA have the authority in 2015 to collect that communication?

MS. HANLEY COOK: Should we go off the record now?

MR. ABDO: Okay, thanks.

MR. PATTON: Thank you.

(Off the record at 4:30 p.m.)

(Resume at 4:46 p.m.)

MR. PATTON: The witness has reviewed in the interim the applicable targeting procedures, the declassified public version of those, and is prepared to make a statement on that particular point, but we don't believe that anything beyond what she's going to say can be said on the public record.

So to the extent not covered by what she's about to say, we object to the questions to the extent they call for a classified response subject to state secrets and subject to the statutory privileges.

THE WITNESS: The examples you provided are classified. How the targeting might or might not occur is all classified on page 5. It's all black, so we can't go any further into that information.

If you would like to -- I'm sorry. I'm looking at Exhibit A, the procedures used by the National Security Agency for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978 as amended. These are dated June 2014.

BY MR. ABDO:

Q What page were you looking at of those?

A 5.

Q If I understand, page 5 relates to the NSA's method for assessing whether there would be a foreign intelligence purpose for collecting certain Internet communications, right?

A Yes.

Q My question didn't deal with whether the NSA in fact had reason to or would want to collect Internet communications.

My question was, did the NSA, in June of 2015, have the authority to collect the communications of a foreign target abroad with a website in the United States?

MR. PATTON: The answer to that question is classified and subject to statutory privileges.

Instruct the witness not to answer the question.

THE WITNESS: I'll follow the instructions.

BY MR. ABDO:

Q And under upstream surveillance as conducted in 2015, did the NSA have the authority to collect the transactions of a foreigner abroad with a website in the United States if the website contained a selector task for collection?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: I'll follow the instruction.

BY MR. ABDO:

Q Are you aware that the Office of Director of National Intelligence has acknowledged that there was a time when overcollection of webmail in-boxes had contributed to the -- had occurred under upstream collection?

MR. PATTON: Just a second.

(Counsel conferring.)

THE WITNESS: Can you point to the document or provide whatever that is?

BY MR. ABDO:

Q I'm asking whether you're aware that that's the case.

A I would want to see where exactly ODNI had said that information to make sure that I wasn't somehow going into some sort of classified discussion.

Without the context of what you're saying, as we've seen a few times, sometimes the

information on its face looks like it says one thing, as we just went through with Raj De's back and forth. So without seeing the context of whatever that is, I don't know how to answer.

Q Let me ask a different question then.

Do you know the answer to the question I asked? Well, let me ask that. Do you know the answer to the question I asked?

MR. PATTON: Objection, vague as to which question.

MR. ABDO: The question being whether you're aware that the Office of Director of National Intelligence has acknowledged that one of the overcollection problems that the NSA had with upstream surveillance involved the collection of webmail in-boxes? Do you know the answer to that question?

THE WITNESS: Again, without confirming or denying, I need to see the document you're referring to to better understand. I'm just concerned I'm in classified territory.

BY MR. ABDO:

Q I'm not asking you for an answer to that question. I'm asking whether you know the answer to that question first.

A I'm sorry, I don't know how to answer what you're saying.

MR. GILLIGAN: It's circular. The question is whether she knows, so I don't know whether she knows the answer to that question is the same question.

MR. ABDO: If forced to answer that question, do you know whether you would say yes or no? I'm not asking you to say yes or no, I'm asking whether you know which one you would say if you were forced to answer the question?

THE WITNESS: And so I'm sorry, I don't know what document you're referring to. I assume you're referring to some document somewhere that ODNI published, and if I could see that so that I could look at it, I would be able to tell you whether I know the answer or not.

But in the abstract question of, "Do

you know this?," I can't answer one way or the other. So without sort of having some basis in what we're looking at, I'm having a hard time answering.

BY MR. ABDO:

Q Okay. Was the collection of webmail in-boxes in fact one of the overcollection problems the NSA had with upstream surveillance specifically with regard to multi-communications transactions?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: I just want to state for the record that neither the witness nor I are trying to be difficult here. We are concerned about providing responses to information that we haven't seen, and so I don't want to instruct the witness not to answer the question if there's a public document out there.

I think it would be better if you show it to her. It will either refresh her recollection and she'll be able to explain whether

she's seen it before or anything like that, but at this point, she's not wanting to answer the question, and I'm concerned that the answer may be classified.

MR. ABDO: Are you able to determine whether the answer is classified without knowing whether there's a physical document in the world that contains the information? Is that the definition of "classified"?

MR. PATTON: No, it really gets to, at this particular point, we don't know what it is that you're referring to, and it may be an unclassified document that the Director of National Intelligence has said X, Y or Z. If that's it, it provides the context and some form of comfort for the witness, who is being asked to determine what's on one side of the classified line and what's not on the other.

She signed a Non-Disclosure Agreement and is -- I mean, her responses to you so far have tried to give you as much unclassified information as possible. She's evidently concerned that if

she provides a response to this outside of any context that she might be violating that NDA.

BY MR. ABDO:

Q Are you aware that the Office of Director of National Intelligence, on August 21st of 2013, held a conference call with reporters in which the Office of Director of National Intelligence described the overcollection of webmail in-boxes as an example of the overcollection problem the NSA experienced under upstream surveillance with regard to multi-communication transactions?

MR. PATTON: Again, that may have occurred on August 21st, 2013. It may be a document that is a newspaper article that may or may not be accurately depicting what ODNI said at that time. And so our concern again, in the abstract, is whether or not the information you're providing is both accurate and unclassified.

MR. ABDO: Okay. So can I confirm, at least for the time being, are you instructing the witness not to answer the question?

MR. PATTON: At the moment, I don't think the witness is in a position to answer the question. Factually, I don't know what it is that you're referring to. And given the amount of information that has been provided through unofficial sources, our concern, and my duty here, and the witness's duty, is to protect classified information, and we want to provide as much unclassified information as we can --

MR. ABDO: I understand. I'm just asking a simple question, Rodney. Are you instructing the witness not to answer?

MR. GILLIGAN: Tell you what, if we step outside, I might be able to suggest a way around this.

MR. ABDO: Can we go off the record?

(Off the record at 4:57 p.m.)

(Resume 5:04 p.m.)

THE WITNESS: Is there an outstanding question? Where are we?

BY MR. ABDO:

Q There was. Let me start with the

question outstanding, which was are you aware that the Office of Director of National Intelligence has acknowledged that the NSA has collected webmail in-boxes under upstream surveillance?

MR. PATTON: Object to the form as beyond the scope of the 30(b)(6) notice, and the witness can answer in her personal capacity.

THE WITNESS: I'm not aware.

BY MR. ABDO:

Q Has the NSA collected webmail in-boxes as part of upstream surveillance?

MR. PATTON: Object to the question, calls for classified information and information protected by the statutory privileges, and instruct the witness not to answer the question.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Okay. Are you familiar with the fact that the contents of Internet communications are transported in what is known as the application layer of Internet packets?

MR. PATTON: Object to the question to the extent it calls for classified -- I'm sorry, I'm so used to that -- to the extent it calls for expert opinion, and that it's beyond the scope of 30(b)(6).

THE WITNESS: Yes.

BY MR. ABDO:

Q Okay. Are you aware of the fact that the contents of an email communication are transported within the application layer of Internet packets?

MR. PATTON: Same objections.

THE WITNESS: Yes.

Isn't that what you just asked me?

BY MR. ABDO:

Q The first question was with respect to Internet communications generally, and the second question was with respect to email communications specifically.

A Okay.

Q Is your answer to both yes?

A Yes. It sounded like the same one,

and I worried I was missing something.

Q And are you aware of the fact that the contents of a website are transported within the application layer of Internet packets?

MR. PATTON: Same objections.

THE WITNESS: Yes.

BY MR. ABDO:

Q Are the filtering or screening processes that you've described with respect to upstream collection as it operates -- or excuse me, upstream surveillance as it operated in June 2015 -- forms of deep packet inspection?

MR. PATTON: Objection.

(Counsel conferring.)

MR. PATTON: I'm sorry, could you read that back?

BY MR. ABDO:

Q Sure. Are the filtering or screening processes that you've described under upstream surveillance as conducted in June 2015 forms of deep packet inspection?

MR. PADGETT: I'm sorry, one key thing

I didn't get. Could you read that back?

(The reporter read back the question.)

MR. PATTON: Object to the question because it calls for classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. ABDO:

Q Are you familiar with the term "deep packet inspection"?

MR. PATTON: Object to that question, beyond the scope of 30(b)(6), and it calls for an expert opinion.

THE WITNESS: In the general sense of the word, as in not specific to anything in particular, but known as the outside world?

BY MR. ABDO:

Q Not specific to upstream surveillance, but --

A Yes.

Q You are familiar with it?

A Yes.
Q What does it mean?
MR. PATTON: Same objections.
THE WITNESS: It's the concept of -- I'm sorry, I'm --
BY MR. ABDO:
Q Is it the process of examining or analyzing the application layer of packets traversing the network?
MR. PATTON: Same objections.
THE WITNESS: Yeah, I'm -- yes. Yes, that's a fine description.
BY MR. ABDO:
Q Tell me again your position at the Department of Homeland Security.
A I was the Senior Director for Privacy Compliance in the Privacy Office.
Q And you participated in the drafting of Privacy Impact Assessments?
A I did.
Q Were you involved in the Privacy Impact Assessments conducted for the Einstein 2 or

Einstein 3 programs?

A Yes, which is why I changed the answer when you asked about the four types of sort of --

Q Ah, got it.

A When I rechanged it, I realized that would probably constitute what you were considering to be surveillance.

Q Network surveillance?

A Network surveillance.

Q Did Einstein 2 involve deep packet inspection?

A I honestly don't remember.

MR. PATTON: Just object to that question as beyond the scope of 30(b)(6). I'm not sure whether the answer is unclassified or not since I have not consulted with the Department of Homeland Security, but if the witness knows of an unclassified answer, the witness can give an unclassified answer.

BY MR. ABDO:

Q Sorry, please go ahead.

A I apologize, but I don't remember what

is classified or unclassified about the Einstein 2 PIA, so unless you have a copy of what was published, I can't speak to the specifics of what was in it.

Q Okay. Are you familiar with Einstein 3? Generally, not anything specific, but are you aware of the Department of Homeland Security's intrusion detection and intrusion prevention program known as Einstein 3 Accelerated?

MR. PATTON: Objection to beyond the scope of 30(b)(6), potentially classified. I'll have to rely on the witness, who may be more familiar with the DHS program certainly than me. If there's a unclassified answer, you can give it in your personal capacity.

MR. ABDO: Surely the existence of this program is unclassified, but --

MR. PATTON: I'm not willing to take the risk.

BY MR. ABDO:

Q Did you work on the Privacy Impact

Assessment for Einstein 3?

MR. PATTON: Same set of objections.

THE WITNESS: Generally speaking, yes, because every PIA that was approved by the Department of Homeland Security at that point was reviewed by me.

BY MR. ABDO:

Q Okay. Are you aware that Einstein 3 was part of the comprehensive cybersecurity initiative announced by the Obama administration?

A Yes.

MR. PATTON: Same objections.

THE WITNESS: Oh, sorry.

BY MR. ABDO:

Q And are you aware that, in announcing that, the administration also made clear that Einstein 3 was implemented with the technological support of the NSA?

MR. PATTON: Same objections.

THE WITNESS: Do you have a document that provides that information?

MR. ABDO: Sure.

(Deposition Exhibit 48 was marked for identification.)

BY MR. ABDO:

Q You have what's been marked as Exhibit 48 in front of you, Ms. Richards.

Do you recognize this document?

MR. PATTON: Object to this document as beyond the scope of 30(b)(6), but the witness can answer this and any other series of questions you have that have unclassified answers and are within her personal knowledge.

THE WITNESS: Yes, I've seen this document before. It's been quite some time.

BY MR. ABDO:

Q Can you tell us what it is?

A It's the Comprehensive National Cybersecurity Initiative.

There it is. Look at that.

Q Would you turn to page 3 of it, about halfway down, two-thirds of the way down, the sentence beginning, "DHS is currently conducting a[n] exercise" -- I think they meant an

exercise -- "to pilot the EINSTEIN 3 capabilities described in this initiative based on technology developed by NSA to solidify processes for managing and protecting information gleaned from observed cyber intrusions."

A Yes.

Q So is it true that the Einstein 3 program was piloted based on technology developed by the NSA?

MR. PATTON: Just a moment.

(Counsel conferring.)

THE WITNESS: Do you have the date of this document?

BY MR. ABDO:

Q I believe it's 2010, but I don't know off the top of my head.

A Could I see your Einstein 3 PIA?

Q We've got another copy of it. Can we mark this too, Dawn?

(Deposition Exhibit 49 was marked for identification.)

BY MR. ABDO:

Q So just for the record, you're now looking at what's been marked as Exhibit 49.

Do you recognize that?

A Yes.

Q What is that document?

A The Privacy Impact Assessment for the National Protection and Programs Directorate, Department of Homeland Security, Einstein 3 Accelerated (E3A), dated April 19th, 2013.

Q Okay. And for the record, you participated in the drafting of that assessment?

A I reviewed it.

Q Okay. If you're not quickly familiar with the answer to a question, that's fine, we can move on. I was just asking whether the Comprehensive National Cybersecurity Initiative --

A So my answer to you --

MR. PATTON: Just a second.

THE WITNESS: I'm sorry.

MR. PATTON: Just preserving my objection that both Exhibit 48 and Exhibit 49,

that series of questions are outside the scope of 30(b)(6), and the witness is answering in her personal capacity.

THE WITNESS: To the extent that the CNCI information is from 2010, stating something specific about NSA-developed technology, and not having reviewed this in almost five years, I would have to look at those and really understand whether what was described in 2010 actually got implemented in 2013.

MR. ABDO: Understood. Okay.

MR. GILLIGAN: Sorry, is that 49 there?

MR. ABDO: 49, yeah.

THE WITNESS: I can read it if you would like me to, but --

BY MR. ABDO:

Q No, that's okay.

Is it correct that in upstream collection that NSA obtains what it calls transactions?

A Internet transactions.

Q Internet transactions. Sorry, yes, internet transactions.
A Yes.
Q Do the Internet packets that constitute a single Internet transaction have a common destination?
MR. PATTON: Objection. Just a second.
(Counsel conferring.)
MR. PATTON: We're just trying to see if there's an unclassified response to that.
THE WITNESS: Uh-uh.
MR. PATTON: Objection, calls for a classified response and information subject to the statutory privileges.
Instruct the witness not to answer.
THE WITNESS: Instructions will be followed.
BY MR. ABDO:
Q Okay. Do the Internet packets that constitute a single Internet transaction have a common source?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MR. ABDO:

Q Are you familiar with the term "flow" or "network flow" as used in the context of Internet communications?

MR. PATTON: Objection, it's beyond the scope of 30(b)(6), and it's calling for an expert opinion.

THE WITNESS: I am, but don't make me define them.

BY MR. ABDO:

Q Is an Internet transaction, as understood by the NSA, the same as a flow or network flow as used in the context of Internet communications?

MR. PATTON: Just a moment. I don't think she can answer that.

THE WITNESS: Uh-uh, no. No, I can't answer that.

(Counsel conferring.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: And will follow the instruction.

BY MR. ABDO:

Q And the reason you can't answer is because it would disclose classified information?

A No.

Q Not because you're not familiar with the definition of "flow"?

A No, not because -- no, that is correct. I know what flow is, I just don't -- that's classified.

Q Okay. Is the definition of "flow" classified?

MR. PATTON: Objection, beyond the scope.

BY MR. ABDO:

Q In general as that term is commonly used in the network communications industry?

MR. PATTON: Objection, it's beyond

the scope, and calling for telecommunications expert opinion.

THE WITNESS: As you've just described, it's the general meaning. There's no specific definition. Internet transaction is an NSA definition. It's not a commonly understood telecommunications one.

So it, like -- there was one another we had earlier today. So there's sort of different groups of NSA-specific versus the outside world would know what they are. "Internet transaction" is one of those.

BY MR. ABDO:

Q What about network flow, flow or network flow?

A Those would be the normal everyday use of the words.

Q In other words, the NSA doesn't have a special definition of that term?

A Correct.

Q Okay. Can we take a five-minute break?

MR. PATTON: Sure.

(A break was taken at 5:21 p.m.)

(Resume at 5:35 p.m.)

EXAMINATION BY COUNSEL FOR

WIKIMEDIA FOUNDATION AND THE ACLU

BY MR. TOOMEY:

Q Ms. Richards, so I'm going to be asking some --

MR. ABDO: Why don't you introduce yourself.

BY MR. TOOMEY:

Q I'm Patrick Toomey. I'm counsel for Wikimedia Foundation from the American Civil Liberties Union.

So carrying on, in the course of upstream surveillance, does the NSA review the contents of communications as they are in transit on the Internet backbone?

MR. PATTON: Objection, calls for information that's classified, subject to state secrets, and the other statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q Let's focus on the period of June 2015 for the questions that follow.

In the course of upstream surveillance in June 2015, did the NSA review the contents of communications as they were in transit on the Internet backbone?

MR. PATTON: Same objections, same instructions.

THE WITNESS: Will follow the -- oh.

MR. PATTON: There are unclassified facts that could come out with different questions, but for that particular phrasing, instruct her not to answer.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June 2015, did the NSA scan the contents of communications as they were in transit on the

Internet backbone?

MR. PATTON: Let me just confer, because there's a specific phrase that you're using that I think is causing both NSA counsel and I as a basis to object on classified information. So I don't want to appear we're overclassifying Einstein 3.

MR. GILLIGAN: So we can go off the record.

MR. TOOMEY: Let's go off the record for a minute.

(Off the record at 5:37 p.m.)

(Resume at 6:23 p.m.)

MR. PATTON: Can remind us of where we were?

MR. TOOMEY: Yes. We're going back on the record, and, Ms. Jaques, if you could read back the previous question, please.

(The reporter read back the question.)

MR. PATTON: Objection to the question to the extent it calls for classified information and information protected by the statutory

privileges. The witness can answer the question to the extent unclassified.

THE WITNESS: So I think what you're asking is sort of a two-part question, and so I wanted to unpack and provide the unclassified aspects of it, and then sort of acknowledge that we've got the classified.

So as part of the upstream, we scan the content of the Internet transactions, and we did that in 2015.

As to the question of basically the in transit or the location, that piece is classified.

BY MR. TOOMEY:

Q Thank you. In June of 2015, in the course of upstream surveillance, did the NSA scan the application layer data of communications that transit the Internet backbone?

MR. PATTON: I'm just listening to your question. There's a slight difference in that that I just need to consult.

(Counsel conferring.)

MR. PADGETT: Could you read the

question?

(The reporter read back the question.)

THE WITNESS: It's classified.

MR. PATTON: There's something unclassified.

MR. PADGETT: Can we just go off the record for a second?

(Off the record at 6:26 p.m.)

(Resume at 6:28 p.m.)

MR. PATTON: And there may be a lot of these back and forth on this, so ...

THE WITNESS: Can you repeat the question, please?

(The reporter read back the question.)

MR. PATTON: Objection to the extent it calls for classified information or information protected by the statutory privileges.

The witness can answer to the extent unclassified about June 2015.

THE WITNESS: So to make sure I'm accurately -- I want to make sure I'm understanding the question and making the

distinction.

So what you're saying is what I just said was part of upstream in 2015, we scanned the content of Internet transactions.

Your next question is are we -- is NSA scanning the application layer of the Internet -- of the Internet -- that doesn't make sense -- if we're scanning the Internet -- I'm sorry, the application layer?

BY MR. TOOMEY:

Q Yes. The question is, in June 2015, did the NSA scan the application layer data of communications that transit the Internet backbone?

MR. PATTON: Same objection, same instruction.

THE WITNESS: The answer is yes for 2015, that we scan certain application data of communications that transit the Internet backbone.

BY MR. TOOMEY:

Q When you say certain --

A Mm-hmm, that's important.

Q -- application layer data, what you

mean by "certain"?

MR. PATTON: Objection, misstates prior testimony. Same objections as before, same instruction.

THE WITNESS: I can't go any further. It's classified.

BY MR. TOOMEY:

Q In unclassified terms, in June 2015, how did the NSA determine whether an Internet transaction contained a selector?

MR. PATTON: Object to the extent it calls for -- the whole answer would be classified. The witness can answer to the extent unclassified.

THE WITNESS: I just want to refer to see if there's any additional information I can provide to you beyond what we've already given to you.

There's no additional information beyond what was provided in the Interrogatories 3, 4 and 5, so there's no additional unclassified information beyond the fact that that's conducted.

BY MR. TOOMEY:

Q Is there any classified information that would be responsive to that question?

A Yes. This is necessarily incomplete because of the classified nature of the program.

Q And you're --

MR. PATTON: We're still talking about June 2015?

MR. TOOMEY: That's correct, yes.

THE WITNESS: Still June 2015, yes.

BY MR. TOOMEY:

Q And you're refusing to provide that information on the basis of an instruction from your lawyer?

MR. PATTON: I haven't instructed her on that, but her answer did indicate what was unclassified, which was the interrogatory responses to 3, 4 and 5, I believe she said, and I believe she also said that anything else beyond that was classified.

And there wasn't a pending question, but to the extent that you asked her a question

such as tell me what that classified information is, I would instruct her not to answer.

BY MR. TOOMEY:

Q Understood. Thank you.

Today does the NSA scan the application layer data of communications that transit the Internet backbone?

MR. PATTON: Objection, calls for information that's classified, subject to the statutory privileges before mentioned, and instruct the witness not to answer.

THE WITNESS: I follow those instructions.

BY MR. TOOMEY:

Q In June of 2015, if a transaction was scanned by the NSA in the course of upstream surveillance, and the NSA determined that it did not contain a selector, was the communication eliminated?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PADGETT: Can you read the

question back?

(The reporter read back the question.)

MR. PATTON: Can we just go off the record for a second?

MR. TOOMEY: Can we go off the record?

(Off the record at 6:34 p.m.)

(Resume at 6:37 p.m.)

(The reporter read back the question.)

MR. PATTON: Object to that question to the extent it calls for classified information or otherwise privileged information.

The witness can answer to the extent unclassified.

THE WITNESS: So the process by which Internet transaction is filtered, and then scanned, if it doesn't have a test selector or isn't about the target, then that means that information will not be ingested into the NSA repository.

BY MR. TOOMEY:

Q And is that communication eliminated?

MR. PATTON: Objection. The question

calls for a classified answer, as well as an unclassified one, which the witness has already given.

The witness can answer again and provide the unclassified answer.

THE WITNESS: I have nothing additional beyond. If you'd like me to repeat what I said, I'd be happy to.

BY MR. TOOMEY:

Q No need to repeat.

And to the extent there is -- is there classified information that you are not providing in response?

A Yes.

Q Today, does the NSA seek to acquire email communications to and from its targets using upstream surveillance?

MR. PATTON: Object to the question. It calls for classified information and information protected by the statutory privileges.

I instruct the witness not to answer.

THE WITNESS: I will follow

instructions.

BY MR. TOOMEY:

Q Could you please describe as fully as possible how, in June 2015, the NSA determined whether an Internet transaction contained a selector?

MR. PATTON: Objection to the extent it calls for classified information, or information otherwise protected by the statutory privileges.

The witness can answer if she can regarding the unclassified response to that question.

THE WITNESS: There's no additional unclassified information beyond what I've already said.

BY MR. TOOMEY:

Q Thank you. Beyond what you've already said or what appears in the NSA's discovery responses, could you please describe as fully as possible how the NSA today determines whether an Internet transaction contains a selector?

MR. PATTON: Objection. The question calls for classified information and information protected by the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will --

MR. ABDO: Rodney, can we just try to compress if it's the same objection? Thanks.

MR. PATTON: If you ask the same -- exactly those kind of questions, I will do my best. Thank you.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June 2015, did the NSA scan communications in bulk?

MR. PATTON: Objection, calls for classified information. Just check and see if there's a --

(Counsel conferring.)

MR. PATTON: Just a second. Can we go off the record?

(Off the record at 6:40 p.m.)

(Resume at 6:43 p.m.)

MR. TOOMEY: Can you please repeat the question?

(The reporter read back the question.)

MR. PATTON: Objection. We'd need to go into the SCIF to discuss whether or not there's an unclassified response to this.

THE WITNESS: But before we do that, can you give a definition of what you mean by "bulk," scanning communications in bulk?

BY MR. TOOMEY:

Q Does the NSA ever use the term "bulk" in connection with surveillance activities?

A Yes.

Q And what do you understand the NSA to mean by the term "bulk"?

A To do collection without -- let's see, the definition is in Presidential Policy Directive No. 28, which I don't have with me, but it's something roughly along the lines of collection without discriminates.

Q That document describes bulk collection to the best of your recollection?

A Yeah.

Q Yes?

A Or it has a general description of it, and then carries on to provide when NSA can conduct bulk -- for what purposes the information can be used.

Q And so my question here is about whether in June 2015, in the course of upstream surveillance, the NSA scanned communications in bulk?

MR. PATTON: Go off the record.

(Off the record at 6:45 p.m.)

(Resume at 6:57 p.m.)

(The reporter read back the question.)

MR. PATTON: Objection to the extent it calls for classified information and information protected by the statutory privileges.

Instruct the witness to answer the question to the extent able in unclassified terms.

THE WITNESS: So in terms of

unclassified, the best information I can give to you is in the PCLOB report, which is Deposition Exhibit 43, page 103. The last line of the first paragraph that states the program does not operate by collecting communications in bulk.

BY MR. TOOMEY:

Q Could you please answer my question about whether in June 2015 the NSA scanned communications in bulk?

MR. PATTON: Objection. The answer to that question, to the extent not already provided by the witness, is classified and subject to statutory privileges.

Instruct the witness not to answer.

MR. GILLIGAN: And state secrets. Did you say state secrets?

MR. PATTON: I said classified. I'm trying to shorten it.

MR. GILLIGAN: Oh, okay. We're all for that.

MR. PATTON: Also subject to the state secrets privilege.

THE WITNESS: I will follow the instructions of my counsel.

BY MR. TOOMEY:

Q In the context of upstream surveillance, is scanning a communication different from collecting a communication?

A Yes.

Q In the course of upstream surveillance today, does the NSA scan communications in bulk?

MR. PATTON: Objection. The question calls for information that's classified, subject to the state secrets, and to the statutory privileges. Instruct the witness not to answer.

THE WITNESS: I will not answer.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA scan the metadata of communications in bulk?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance in 2015, did the NSA copy communications in bulk?

MR. PATTON: Same objection, same instructions.

THE WITNESS: Follow instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA copy communications in bulk?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instructions.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June of 2015, did the NSA deliberately attempt to filter out any of Wikimedia's international communications?

MR. PATTON: Objection. Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA deliberately attempt to filter out any of Wikimedia's international communications?

MR. PATTON: Same instruction, same objections.

THE WITNESS: Will follow instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance in June of 2015, did the NSA deliberately attempt to filter out all of Wikimedia's communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow instruction.

BY MR. TOOMEY:

Q In the course of upstream surveillance today, does the NSA deliberately attempt to filter out all Wikimedia communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow

instructions.

BY MR. TOOMEY:

Q Does the NSA contend as a factual matter in this case that it deliberately filters out all Wikimedia communications?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Could you go off the record?

(Off the record at 7:01 p.m.)

(Resume at 7:08 p.m.)

MR. TOOMEY: Could you read back the last question?

(The reporter read back the question.)

MR. PATTON: Object to the question as beyond the scope of 30(b)(6), improper 30(b)(6) question. The witness can answer in her personal capacity.

THE WITNESS: In my personal capacity, I have no idea, but to the extent that we do or do not filter something out would be classified in any event.

BY MR. TOOMEY:

Q Does anyone at the NSA know whether the NSA contends in this case, as a factual matter, that it deliberately filters out all Wikimedia communications?

MR. PATTON: Same objections, same instruction.

THE WITNESS: It's classified. I mean --

MR. PATTON: That's not the question he's asking.

THE WITNESS: That's not the question.

MR. PATTON: That's not the question he's asking.

THE WITNESS: So same answer, which I have no idea, and to the extent it is or isn't would be classified.

BY MR. TOOMEY:

Q To the extent it is or isn't what?

A Filtering out Wikimedia, as you were contending in your question.

Q My question is whether the NSA

contends that it is filtering out Wikimedia's communications. Do you know the answer to that question?

MR. PATTON: Objection. Same objections as before, and adding asked and answered.

THE WITNESS: I have nothing else to say on the topic.

MR. TOOMEY: Ms. Jaques, could you mark as the next exhibit this document, please?

(Deposition Exhibit 50 was marked for identification.)

BY MR. TOOMEY:

Q So the court reporter has handed Ms. Richards Exhibit 50, which is titled Memorandum of Points and Authorities in Support of Defendant's Motion to Compel Discovery. Sorry, we don't have as many copies of this one, sorry.

Could you please tell me what this document is?

MR. PATTON: Objection, lacks foundation.

BY MR. TOOMEY:

Q You can answer.

Have you seen this document before?

A I have not seen this document before.

Q Can you read the title of the document, please?

A Sure. Memorandum of Points and Authorities in Support of Defendant's Motion to Compel Discovery, dated March 26, 2018.

Q Thank you. Could you please turn to page 11 --

A Sure.

Q -- of Exhibit 50?

I'm going to read a sentence from the document in the last paragraph toward the bottom of the page.

"An entity seeking to conduct surveillance on the Internet that lacks the ability to decipher encrypted HTTPS communications may well decide to program its surveillance equipment to disregard such communications altogether."

Has the NSA programmed its surveillance equipment to disregard HTTPS communications altogether?

MR. PATTON: Objection, the question calls for classified information protected by the state secrets privilege and information protected by the statutory privileges.

Instruct the witness not to answer the question.

THE WITNESS: I'll follow the instructions.

BY MR. TOOMEY:

Q Can we now turn to page 12 of Exhibit 50. I'm going to read a passage from the first paragraph toward the top of the page.

"If the NSA lacked the ability to decipher HTTPS communications," dot dot dot, "then nothing --

MR. PATTON: It's an important dot dot dot.

MR. TOOMEY: We'll get there. I'm going to start again. I'm going to read the

passage again.

"If the NSA lacked the ability to decipher HTTPS communications ... then nothing in the 'technical rules of how the Internet works' ... would prevent the configuration of devices used in connection with Upstream surveillance to exclude HTTPS communications."

Does the NSA have the ability to decipher HTTPS communications?

MR. PATTON: Objection, outside the scope of 30(b)(6), and the question calls for classified information protected by the state secrets privilege, statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q I'm going to read a passage now from page 12 of Exhibit 50 in the second paragraph toward the bottom of the page.

"If the NSA deemed communications to and from Wikimedia's websites to be of low

foreign-intelligence value, then nothing in the technical rules of the Internet would prevent the configuration of equipment used in connection with Upstream surveillance to ignore all communications having source or destination IP addresses associated with Wikimedia."

Has the NSA configured its surveillance equipment to ignore all communications having source or destination IP addresses associated with Wikimedia?

MR. PATTON: Objection, beyond the scope of 30(b)(6), and objection, it calls for classified information, subject to state secrets, statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Does the NSA deem communications to and from Wikimedia's websites to be of low foreign intelligence value?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: Will follow instruction.

BY MR. TOOMEY:

Q Would the NSA be permitted under upstream surveillance today to collect a targets communications with a U.S.-based website?

A How is this question different than the last one?

MR. PATTON: I'm not sure it is.

THE WITNESS: Okay.

MR. PATTON: Can we go off the record?

(Off the record at 7:16 p.m.)

(Resume at 7:23 p.m.)

BY MR. TOOMEY:

Q Back on the record.

Ms. Jaques, could you please read back the prior question?

(The reporter read back the question.)

MR. PATTON: We object to that question. It calls for a classified answer.

The witness has reviewed during the break the currently applicable declassified and

public targeting procedures, and there's no unclassified answer we can give. So as a result, we object to the question, it calls for classified information, subject to the state secrets and subject to the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I'll follow the instructions.

BY MR. TOOMEY:

Q Is it possible that a targets communications with Wikimedia could contain foreign intelligence information that would be of interest to the NSA?

(Counsel conferring.)

MR. PATTON: You'll like this one.

Object as beyond the scope of 30(b)(6) and speculative. The witness can answer in her own capacity to the extent the answer is unclassified.

THE WITNESS: It's speculative. I can't speak to who would or wouldn't be, what particular individual might be targeted. If an

analyst decides a particular selector or person meets the targeting standards, then that would be appropriate.

BY MR. TOOMEY:

Q Could the term "foreign intelligence information" encompass information that a person surveilled using upstream surveillance is reading on one of Wikimedia's websites?

MR. PADGETT: Could I get that read back?

(The reporter read back the question.)

MR. PADGETT: Do you want to talk about it? Let's go off the record.

(Off the record at 7:26 p.m.)

(Resume at 7:28 p.m.)

MR. TOOMEY: Ms. Jaques, could you please read back the last question?

(The reporter read back the question.)

MR. PATTON: Objection, beyond the scope of 30(b)(6), speculative, and calls for legal conclusion. The witness can answer in her personal capacity.

THE WITNESS: I'm sorry, can you read that question one more time?

(The reporter read back the question.)

MR. PATTON: Same objections.

THE WITNESS: Can we go off the record? Sorry.

(Off the record at 7:30 p.m.)

(Resume at 7:32 p.m.)

MR. PATTON: Same objections, same instruction.

THE WITNESS: So you have a couple of different things, which is why we kept having to walk outside to unpack that, and so I want to unpack what's classified and what's unclassified.

So the first part of your question would be is there possibly foreign intelligence information on the Wikimedia sites, to which the answer, from my perspective, is there could be. I don't actually know. I haven't trolled through the Wikimedia websites, but it's possible.

The second part of that question had to do with how it would function in the upstream

context, and that piece of it is what's classified.

BY MR. TOOMEY:

Q Similar question, could the term "foreign intelligence information" encompass information that a person surveilled using upstream surveillance is contributing to one of Wikimedia's websites?

MR. PATTON: Same objections, same instruction.

THE WITNESS: I would give the same answer, which is I would separate those two pieces to say it's possible that somebody at one of your contributors is creating foreign intelligence information in a hypothetical. I don't actually know.

To the extent it has anything to do with upstream, any piece of that would be classified.

BY MR. TOOMEY:

Q And you're not answering that portion to that aspect of the question based on your

lawyer's instruction?

A Correct.

MR. PATTON: Not based on my instruction. When we broke the last time, the witness had a question as to what aspect of this that she could talk about. She provided the information that she could talk about and indicated to you there's another classified component, and the nature of that classified information, and she declined to answer based on that.

Had you asked her a follow-up question as to the content of that classified information, I would have instructed her not to answer.

BY MR. TOOMEY:

Q Could you please provide any classified information that you believe my question calls for?

MR. PATTON: I respect that question. It keeps our record clean.

Object to the question to the extent it calls for classified information, information

subject to the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow those instructions.

BY MR. TOOMEY:

Q Today, does the NSA intentionally attempt to filter out all HTTPS communications from upstream surveillance?

MR. PATTON: Objection, the question calls for classified information, subject to the state secrets and to the statutory privileges.

Instruct not to answer.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Same question, but for June 2015. Did the NSA at that time intentionally attempt to filter out all HTTPS communications from upstream surveillance?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Will follow the

instruction.

BY MR. TOOMEY:

Q Today, does the NSA intentionally attempt to filter out all Internet communications that use TCP port 443?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally attempt to filter out all Internet communications that used TCP port 443?

MR. PATTON: Same objections, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q Today, does the NSA intentionally filter out all encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally filter out all encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q Today, does the NSA intentionally filter out all open VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally filter out all open VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Today does the NSA intentionally filter out Wikimedia's encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q In June 2015, did the NSA intentionally filter out Wikimedia's encrypted VPN communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Can you please describe in as much detail as necessary to provide a complete answer how the NSA implemented any changes to "about" collection during or after April 2017?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Object to the question to the extent it calls for classified information and information protected by the statutory privileges.

If there is an unclassified response, the witness can provide it.

MR. TOOMEY: Rodney, to be clear, just so we can try to consolidate things, are you also instructing the witness not to provide any unclassified information?

MR. PATTON: No. I'm instructing --

MR. TOOMEY: Sorry, any classified information, just so --

MR. PATTON: I would love her to provide any unclassified information, but if there's any classified information, I'm instructing her not to answer.

There may be some unclassified information that she can provide, and that's what I'm authorizing her to do.

THE WITNESS: As of 2017, April 2017, NSA changed the way it did its upstream collection

so that it no longer collected the "abouts" collection.

There's not any additional information beyond the information that was either in the 2017 opinion or our associated unclassified information that NSA put out on its website.

MR. PATTON: That's the April 2017 FISC opinion?

THE WITNESS: Sorry, yes, the April 2017 FISC opinion.

BY MR. TOOMEY:

Q Besides the information you just identified, is there any other unclassified information that you could provide to this question?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Not that I'm aware of.

BY MR. TOOMEY:

Q Is there classified information that would answer the question that you are not providing at the instruction of your attorney?

MR. PATTON: Objection to the extent it calls for classified information.

If the witness's answer is yes or no, she can provide that information.

THE WITNESS: Yes.

BY MR. TOOMEY:

Q Apart from the information you identified in response to my last question, could you please describe how the NSA attempts to avoid collecting communications that are solely about a selector?

MR. PATTON: Object to the form of the question, vague as to time. Potentially classified.

(Counsel conferring.)

MR. PATTON: Would you mind rephrasing to specify the time period?

MR. TOOMEY: Sure, I'll rephrase.

MR. PATTON: Thanks.

BY MR. TOOMEY:

Q Apart from the unclassified information that you provided in response to my

last question, could you please describe in as much detail as necessary to provide a complete answer how, after April 2017, the NSA attempts to avoid collecting communications that are solely about a selector?

(Counsel conferring.)

MR. PATTON: Can we go off the record?

(Off the record at 7:42 p.m.)

(Resume at 7:43 p.m.)

MR. PATTON: Would you mind reading back the question, please?

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for classified information.

If the witness's answer is yes or no, she can answer that.

THE WITNESS: There's no additional information beyond what I've pointed to. I have no additional --

BY MR. TOOMEY:

Q There's no additional unclassified information?

A No additional unclassified information.

Q And is there classified information that you're not providing at the instruction of your counsel?

A Yes.

Q Apart from the unclassified information that you provided in response to my question, my previous question, please describe in as much detail as necessary to provide a complete answer how the change in April 2017 affected the filtering of communications subject to upstream surveillance?

(Counsel conferring.)

MR. PATTON: Can we go off the record?

(Off the record at 7:45 p.m.)

(Resume at 7:59 p.m.)

MR. TOOMEY: Could you please read back the last question?

(The reporter read back the question.)

MR. PATTON: Objection to the question to the extent it calls for classified information

and information subject to the statutory privileges.

To the extent the witness is aware of an unclassified answer, she may provide a response.

THE WITNESS: The only point I would provide to you on this, which is not necessarily anything new, but we still stand behind the information about how the filtering works in our Civil Liberties and Privacy Office Report, and that remains true today as it did in 2014, when we wrote the report.

BY MR. TOOMEY:

Q Is there classified information you're not providing in response to my question at the instruction of your lawyer?

A Yes.

Q Thank you. Similar question, apart from the unclassified information that you've already provided today, could you please describe in as much detail as necessary to give a complete answer how the change in April 2017 affected the

scanning of communications subject to upstream surveillance?

MR. PATTON: Object to the question, calls for classified information and information subject to statutory privileges, and instruct the witness not to answer the question.

THE WITNESS: I will not answer.

BY MR. TOOMEY:

Q Apart from the unclassified information you've already provided today, please describe in as much detail as necessary to give a complete answer which portions of an Internet transaction are scanned for selectors after April 2017?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA first scan the contents of communications for selectors, and then discard those that are solely about a

selector?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA copy the contents of communications prior to scanning those communications?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA copy the application layer data of packets prior to scanning the communications to which they belong?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the

instruction.

BY MR. TOOMEY:

Q Since April 2017, does the NSA review any portion of the contents of communications for selectors?

MR. PATTON: Object to the form, vague as to "review," and object to the question as seeking classified information, subject to the state secrets and statutory privileges, and instruct the witness not to answer.

THE WITNESS: Will follow the directions.

BY MR. TOOMEY:

Q Would your answer have been the same if I had said does the NSA scan any portion of the contents of communications for selectors --

MR. PATTON: One moment.

MR. TOOMEY: -- since April 2017?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Could you rephrase the question in terms of an Internet transaction?

It's fine if you don't, but that might take care of something.

MR. TOOMEY: Sure, let me rephrase.

BY MR. TOOMEY:

Q Since April 2017, does the NSA scan any portion of the contents of Internet transactions for selectors?

(Counsel conferring.)

MR. PATTON: I think we need to go off the record.

MR. TOOMEY: Let's go off the record.

(Off the record at 8:04 p.m.)

(Resume at 8:18 p.m.)

MR. TOOMEY: Could you please read back the prior question?

(The reporter read back the question.)

MR. PATTON: Objection to the question to the extent it seeks classified information and information protected by the statutory privileges.

The witness can answer the question to the extent that it's unclassified.

THE WITNESS: So NSA scans a portion

of the Internet transaction to identify the task selector in order to acquire the Internet transaction that is to or from the target.

To go any further in terms of whether it's in the content or the metadata, or any of those further things, is classified.

MR. PATTON: And I instruct her not to answer beyond that unclassified answer.

BY MR. TOOMEY:

Q And you're following your counsel's instruction?

A I am.

Q So just to confirm, what portions of the contents of Internet transactions are scanned for selectors since April 2017?

MR. PATTON: I was waiting for you to finish.

Objection to the extent that it mischaracterizes the prior testimony. The witness can answer the question to the extent it's unclassified. Any classified answer, I instruct her not to provide.

THE WITNESS: You're asking me what portion of the Internet transaction we're scanning, just so I'm clarifying?

BY MR. TOOMEY:

Q Correct, after April 2017.

A After April 2017?

I am not able to answer that question. The answer to that question is classified.

Q Since April 2017, does the NSA review the entire contents of communication of Internet -- let me strike that. I'll restate the question.

Since April 2017, does the NSA scan the entire contents of Internet transactions for selectors?

MR. PATTON: Objection, calls for classified information, information protected by the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MR. TOOMEY:

Q Since April 2017, does the NSA scan any portion of the application layer data of Internet transactions for selectors?

MR. PATTON: Same objection, same instructions.

THE WITNESS: Will follow the instruction.

BY MR. TOOMEY:

Q And if I were to ask what portions of Internet transaction the NSA scans for selectors, would your answer be the same?

MR. PATTON: Are we talking about post April 2017?

MR. TOOMEY: Yes, post April 2017.

MR. PATTON: Same objection, same instruction.

THE WITNESS: Yes, my answer would be the same.

BY MR. TOOMEY:

Q And since April 2017, does the NSA scan the entire application layer of Internet

transactions for selectors?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Are there any barriers to the NSA restarting "about" collection today?

MR. PATTON: Objection, beyond the scope of 30(b)(6) notice, calls for a legal conclusion.

THE WITNESS: NSA --

MR. PATTON: Just a second. There may be an additional objection.

(Counsel conferring.)

MR. PATTON: I would just add that to the extent that the question calls for a classified answer, I object to that based on the state secrets privilege and the statutory privileges. If there's an unclassified answer, the witness can provide.

And my colleague let's me know that

there's also a vagueness objection.

BY MR. TOOMEY:

Q You can answer to the extent --

A Sure. With the passage of the 702 FAA Reauthorization, there is a requirement for once the FISC has approved us going back to "abouts," that we have to give a 30-day notice to Congress before we can move forward with any type of collection.

MR. PATTON: Any type of "abouts" collection.

THE WITNESS: Any type of "abouts" collection. Apologies for not being clear.

BY MR. TOOMEY:

Q Do you consider that statutory requirement a barrier to the NSA restarting "about" collection?

MR. PATTON: Objection, beyond the scope of 30(b)(6), vague as to what a barrier is, calls for a legal conclusion.

The witness can answer in her own capacity.

THE WITNESS: Can you explain what you mean by barrier? I mean, to the extent -- yeah.

BY MR. TOOMEY:

Q I mean by barrier any obstacle, impediment to restarting "about" collection.

MR. PATTON: Same set of objections, and add in the one that to the extent there's any classified response to that, the witness should not answer as to classified information. You can otherwise provide an unclassified answer in your personal capacity.

THE WITNESS: Certainly getting FISC approval and notifying Congress are additional barriers beyond just being able to turn it on tomorrow.

BY MR. TOOMEY:

Q And could you please state whether there is any -- first of all, are there any other barriers besides the two that you just described?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Go off the record.

(Off the record at 8:25 p.m.)

(Resume at 8:36 p.m.)

MR. TOOMEY: All right, let's go back on the record.

THE WITNESS: Can you read it back?

(The reporter read back the question.)

THE WITNESS: Are you answering first or am I?

MR. PATTON: Sorry, putting this away. Object to the question to the extent it calls for classified information and information protected by the statutory privileges. The witness can answer the question to the extent unclassified.

THE WITNESS: So as noted, the FISC would have to approve us going back to doing "abouts," so we would have to address any of the underlying issues as it relates to getting the FISC approval, as were described in the 2017 Memorandum Opinion.

BY MR. TOOMEY:

Q What are those underlying issues?

MR. PATTON: Object to the question to the extent it calls for classified information and information protected by the statutory privileges.

The witness can answer the question to the extent unclassified.

THE WITNESS: So the two unclassified descriptions that were provided in the 2017 Memorandum Opinion indicated there were both technological issues, as well as human error issues.

BY MR. TOOMEY:

Q And what were those issues?

MR. PATTON: Objection to the extent it calls for classified information and information protected by the statutory privileges.

The witness can answer to the extent unclassified.

THE WITNESS: Could I have the 2017 so I can point you to those sections? Do you want to introduce that in? Is that what's coming next?

MR. TOOMEY: Could you please mark that?

(Deposition Exhibit 51 was marked for identification.)

BY MR. TOOMEY:

Q Please take a look at Exhibit 51 which the court reporter has just handed you.

Could you tell me, are you familiar with this document and what it is?

A Yes. This is the Memorandum Opinion and Order of the Foreign Intelligence Surveillance Court dated April 26, 2017.

So I will start with page 14 to 15 --

MR. GILLIGAN: Sorry, did we mark this?

THE WITNESS: Yes, it's 51.

So the first indication of this discussion is starting at the bottom of page 14. The sentence begins, "The October 26, 2016 Notice disclosed that an NSA Inspector General review and report and NSA Office of Compliance for Operation verification activities indicated that, with greater frequency than previously disclosed to the Court, NSA analysts had used U.S.-person

identifiers to query the results of Internet 'upstream' collection, even though NSA's Section 702 minimization procedures prohibited such queries."

BY MR. TOOMEY:

Q So if I could stop you there.

A Sure.

Q Is it accurate to say that the technical and human error issues that the FISC identified related to queries of the results of Internet upstream collection?

(Counsel conferring.)

MR. PATTON: If the answer is yes or no, the witness can answer the question.

THE WITNESS: Yes.

BY MR. TOOMEY:

Q Besides the barriers you already identified and what's described in Exhibit 51, are there any other barriers to the NSA restarting "about" collection?

MR. PATTON: Objection to the extent that it calls for classified information and

information protected by the statutory privileges.

If there's an unclassified answer the witness can provide, she can provide it.

THE WITNESS: I'm sorry, can we go off the record?

(Off the record at 8:42 p.m.)

(Resume at 8:43 p.m.)

THE WITNESS: To the extent that NSA considers budget, time, intelligence needs, risk to the agency, privacy and civil liberties impact, all of those will also be considered as NSA decides whether or not to spend its next intelligence needs to go into "abouts."

Whether that's a particular barrier or not, those are all considerations that NSA will take into consideration as it thinks about whether or not it should go forward with "abouts."

BY MR. TOOMEY:

Q Okay. Is there any other barrier you haven't already described?

A No.

Q Has the NSA disavowed any intention of

resuming "about" collection in the future?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Just object to beyond the scope of 30(b)(6). The witness can answer if she knows.

THE WITNESS: No.

BY MR. TOOMEY:

Q Has the NSA indicated to any member of Congress any interest in resuming "about" collection in the future?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Same objection as beyond the scope of 30(b)(6). The witness can answer if she's aware.

THE WITNESS: Admiral Rogers testified that he would consider going back up on "abouts" collection if he could make it through all the -- you know, if it met the needs -- met intelligence needs, and they were in a position to meet all the needs of the FISC and notification to Congress.

BY MR. TOOMEY:

Q Do you know when Admiral Rogers provided that testimony?

A I want to say roughly October time frame 2018 -- I'm sorry, sorry 2017 -- in the future. Somewhere in the September/October 2017. It might have been part of one of the threat briefings.

Q Do you know to whom he provided that testimony? Which congressional committee or --

A I believe it was SSCI, Senate Select Committee on Intelligence. I'm pretty certain that's who it was.

Q Thank you.

A It could have been part of an appropriations hearing, but ...

Q And was that testimony public testimony?

A Yes, it was.

Q Has the NSA indicated to the FISC any interest in resuming "about" collection in the future?

MR. PATTON: Objection.

(Counsel conferring.)

MR. PATTON: The objection is twofold. One, beyond the scope of 30(b)(6) and, two, object to the extent it calls for a classified answer, and also one subject to statutory privileges. But if the witness is personally aware of that fact and it's unclassified, she can answer.

THE WITNESS: The answer is classified, and I'm following the instructions of my lawyer.

BY MR. TOOMEY:

Q Has the NSA indicated to the FISC that it intends to resume "about" collection in the future?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Same answer.

MR. TOOMEY: Can we mark as the next exhibit, please, this document?

(Deposition Exhibit 52 was marked for identification.)

BY MR. TOOMEY:

Q Could you please take a look at Exhibit 52 and tell me if you recognize this document and what it is?

A I recognize this document. It is the NSA press release dated April 28, 2017, stating, "NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702."

Q Thank you. Let me move to a different -- can we please mark this document as Exhibit 53?

(Deposition Exhibit 53 was marked for identification.)

BY MR. TOOMEY:

Q Could you please take a look at this document, state whether you're familiar with it, and describe it.

A Yes, I am familiar with it. It is the statement from April 28th, 2017, stating, "NSA Stops Certain Section 702 'Upstream' Activities."

Q And I'm going to read a short passage from the first paragraph at the end, which says,

"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."

Is that sentence accurate?

A Yes.

Q Did any court order the NSA to stop "about" collection?

MR. PATTON: One second.

(Counsel conferring.)

MR. PATTON: My only objection is to vagueness as to the term "stop" in the context of a court order.

MR. GILLIGAN: Beyond the scope.

MR. PATTON: It's also beyond the scope then.

MR. TOOMEY: You can answer.

THE WITNESS: Actually, I would just like more specificity. What are you -- I'm not sure I entirely understand.

If you read -- maybe I'll give a

little bit more answer. If you read on the second page of Exhibit 53, it states, "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."

So could you be clearer of the particular court?

BY MR. TOOMEY:

Q Could you read me the title of Exhibit 53?

A Sure. NSA statement, "NSA Stops Certain Section 702 'Upstream' Activities," dated April 28th, 2017.

Q And my question is did any court order the NSA to stop "about" collection?

MR. PATTON: Same objections.

THE WITNESS: Can you describe what court you're talking about?

BY MR. TOOMEY:

Q I'm asking about any court.

A Any court?

Q But any court would include the FISC.

MR. PATTON: Same objections. Also, this particular one calls for a legal conclusion too. You can answer.

THE WITNESS: Okay.

So the Attorney General and the DNI put forward a set of targeting procedures to the FISC, and the FISC agreed with those procedures. There was no FISC ordering us to stop.

BY MR. TOOMEY:

Q Did Congress prohibit the NSA from conducting "about" collection in April of 2017?

MR. PATTON: Objection, vague as to April 2017. Same set of objections as before, beyond the scope of 30(b)(6), calls for a legal conclusion, vague.

THE WITNESS: No.

BY MR. TOOMEY:

Q Congress hasn't since prohibited the

NSA from restarting "about" collection, correct?

MR. PATTON: Objection, beyond the scope, calls for a legal conclusion.

THE WITNESS: With the passage of the 702 FAA Reauthorization, it puts in place a requirement for notification 30 days between when the FISC approves it and when we could start, unless there's extenuating circumstances.

BY MR. TOOMEY:

Q So that statute doesn't contain a prohibition on restarting "about" collection?

A Correct.

MR. PATTON: Same set of objections.

THE WITNESS: Correct.

BY MR. TOOMEY:

Q Today, does upstream surveillance involve the scanning of all international text-based communications on individual circuit or circuits the NSA is monitoring?

MR. PATTON: Objection, calls for classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow instructions.

MR. GILLIGAN: Could I hear the question again, please?

(The reporter read back the question.)

MR. GILLIGAN: Can we go talk, please? Off the record.

(Off the record at 8:57 p.m.)

(Resume at 9:22 p.m.)

BY MR. TOOMEY:

Q Let's go back on the record.

Ms. Jaques, could you please read back the last question?

(The reporter read back the question.)

MR. PATTON: Objection to the question, that calls for a classified answer, and also an answer that seeks information protected by the statutory provisions.

Instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

MR. TOOMEY: So going forward, can we shorten that to assert state secrets and statutory privileges?

MR. PATTON: I will shorten it as fast as I can.

BY MR. TOOMEY:

Q In June 2015, did upstream surveillance involve the scanning of all international text-based communications on the individual circuit or circuits the NSA was monitoring?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Today, if some international text-based communications on a given circuit are not scanned, please explain in as much detail as necessary to completely answer why those communications are not scanned.

MR. PATTON: Please repeat the

question.

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for classified information and information protected by the statutory privileges.

The witness can answer the question to the extent that she is aware of an unclassified answer to that question.

THE WITNESS: Can you read the question one more time to make sure I have it entirely accurate?

(The reporter read back the question.)

THE WITNESS: As we were discussing in the existing Civil Liberties and Privacy Report, the process is that there's filtering, and then there's scanning. So to the extent that we have filtered wholly domestic communications out as part of that, those would not be scanned.

BY MR. TOOMEY:

Q Beyond that response and beyond the unclassified information you've already provided today, can you please fully explain in as much

detail as necessary why some communications are not scanned?

MR. PATTON: Object to the question, calls for classified information, information protected by the statutory privileges.

Instruct not to answer.

THE WITNESS: Will follow the instructions.

BY MR. TOOMEY:

Q Same question as of June 2015. If you need me to restate the question, I can.

A Can you restate the question?

Q Apart from the unclassified information you've already provided today, as of June 2015, if some international text-based communications on a given circuit were not scanned, please explain in as much detail as necessary to fully answer why those communications are not scanned.

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Object to the question,

calls for classified information and information protected by the statutory privileges.

If there's any information that the witness is aware of that has not already been provided either in the interrogatory responses or in the prior testimony that would answer that question, she can go ahead and give it.

If not, I would instruct her not to answer the question based on those privileges.

THE WITNESS: There's no additional information, so I'll follow counsel's directions.

BY MR. TOOMEY:

Q There's no additional unclassified information?

A There's no additional unclassified information that I can provide you beyond what we've already provided you.

Q And there is classified information which you're not providing based on your counsel's instruction?

MR. PATTON: To the extent that the answer to that question is yes or no, you can

answer the question.

THE WITNESS: Yes, that's correct.

MR. TOOMEY: Thank you. Let's go off record.

(Off the record at 9:29 p.m.)

(Resume at 9:39 p.m.)

EXAMINATION BY COUNSEL FOR PLAINTIFFS

BY MS. HANLEY COOK:

Q Hi, I'm Devon Hanley Cook. We spent the day together, but nice to meet you. I want to thank you for your patience and for putting up with all our questions and going so late today. I also want to thank you, Dawn. I know it's been a really long day for everybody.

Does NSA now scan Wikimedia's communications in the course of upstream surveillance?

MR. PATTON: Objection, calls for classified information, subject to state secrets privilege and to statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow the

instructions.

BY MS. HANLEY COOK:

Q In 2015, did NSA scan Wikimedia communications in the course of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Does NSA now copy Wikimedia communications in the course of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q In June 2015, did NSA copy Wikimedia communications in the course of upstream surveillance?

MR. PATTON: Same objection, same

instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Has NSA acquired Wikimedia communications as a result of upstream surveillance now?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q As of June 2015, had NSA acquired Wikimedia communications as a result of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MS. HANLEY COOK:

Q Can I have Tab X, please? Let's save time, let's do X and Y, please.

MR. GILLIGAN: 54 and 55 then?
THE REPORTER: Yes, 54 and 55.
(Deposition Exhibits 54 and 55 were marked for identification.)
BY MS. HANLEY COOK:
Q Let's start with Exhibit 54.
Have you seen Exhibit 54 before?
MR. PATTON: Just a second.
(Counsel conferring.)
MR. PATTON: Object to the question as beyond 30(b)(6). The witness can answer yes or no if she has personally seen this Exhibit 54 before.
THE WITNESS: No.
BY MS. HANLEY COOK:
Q If you assumed that Exhibit 54 related to upstream surveillance, it would indicate, wouldn't it, that the NSA had an intelligence interest in Wikimedia's communications, wouldn't it?
MR. PATTON: Object to the question, calls for a classified answer, subject to the state secrets privilege and to the statutory

privileges.

Instruct the witness not to answer the question.

THE WITNESS: Will follow those instructions.

BY MS. HANLEY COOK:

Q Turning to Exhibit 55, have you seen this document before? Actually, let me -- Exhibit 54. Recognizing that you have not seen the document before, what do you think it is?

MR. PATTON: Objection. Same objection as before, same instruction.

THE WITNESS: Which instruction was that? Classified?

MR. PATTON: Classified, subject to the state secrets privilege and to statutory privileges.

The witness is instructed not to answer the question.

THE WITNESS: I will follow those instructions. I just had to make sure I knew what the instructions were.

BY MS. HANLEY COOK:

Q Makes sense.

Exhibit 55, have you seen this document before?

MR. PATTON: Object to the question to the extent it's beyond 30(b)(6). The witness can answer yes or no if she has seen this document in her personal capacity.

THE WITNESS: Yes.

BY MS. HANLEY COOK:

Q What is it?

MR. PATTON: Object to the question, calls for a classified answer, subject to the state secrets and to statutory privileges.

Instruct the witness not to answer.

THE WITNESS: I will follow those instructions.

BY MS. HANLEY COOK:

Q If you assumed that Exhibit 55 related to upstream surveillance, it would indicate, wouldn't it, particularly on the second page in the first bullet point, that the NSA has an

intelligence interest in Wikimedia's HTTP communications, wouldn't it?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow those instructions.

BY MS. HANLEY COOK:

Q Do Exhibits 54 or 55 relate to upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow those instructions.

BY MS. HANLEY COOK:

Q At this time, HTTP communications are scanned for selectors in the course of upstream surveillance, aren't they?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PATTON: Same objection, same instructions. Do you need a reminder on the --

THE WITNESS: I just need to remind

what --

MR. PATTON: Do you need the question read back?

THE WITNESS: Could you read the question again?

(The reporter read back the question.)

MR. PATTON: Object to the question, calls for classified information, information protected by the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow those instructions.

BY MS. HANLEY COOK:

Q As of June 2015, HTTP communications were scanned for selectors in the course of upstream surveillance, right?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instructions.

BY MS. HANLEY COOK:

Q At this time, HTTPS communications are

scanned for selectors in the course of upstream surveillance, aren't they?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Same question as to the June 2015 time frame.

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Are Apache Kafka communications scanned for selectors in the course of upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Do you know what Apache Kafka communications are?

MR. PATTON: Object to the question, beyond the scope, calls for expert testimony.

The witness can answer in her personal capacity.

THE WITNESS: Not well enough to describe to you.

BY MS. HANLEY COOK:

Q Open VPN communications are scanned for selectors in the course of upstream surveillance, aren't they?

MR. PATTON: Objection, vague as to time period, calls for classified information and information protected by the statutory privileges.

Instruct the witness not to answer.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q As of June 2015, were open VPN communications scanned for selectors in the course

of upstream surveillance?

MR. PATTON: Same objection without the vague as to time.

Same instruction not to answer.

THE WITNESS: Will follow the instruction.

BY MS. HANLEY COOK:

Q Other than public documents, public documents at large, hearing testimony that is transcribed, public documents you reviewed, documents that have been filed or served in this case, or your testimony today, what can you tell me about the volume of communications subject to upstream surveillance at this time using any unit of measurement you want to discuss volume of communications?

MR. PATTON: Just one moment.

Can we go off the record?

(Off the record at the 9:49 p.m.)

(Resume at 9:49 p.m.)

MR. PATTON: Could you read back the question, please?

(The reporter read back the question.)

MR. PATTON: Other than the officially disclosed government statements, whether they be publicly by ODNI or by NSA or filed in this particular case or filed in the FISC and declassified, any other information that the witness would have would be classified, and so I would instruct her not to answer the question based on the state secrets privilege and statutory privileges.

THE WITNESS: I'll follow the instructions.

BY MS. HANLEY COOK:

Q Okay. How many communications -- and you can use any unit of measurement you want -- did NSA retain as a result of upstream surveillance in each of the last three years?

MR. PATTON: Objection, vague as to the term "communication," and classified, subject to the state secrets privilege and statutory privileges, and instruct not to answer.

THE WITNESS: Will follow the

instruction.

BY MS. HANLEY COOK:

Q Same question as to transactions.

MR. PATTON: Same objections except for vagueness, same instruction.

THE WITNESS: I will follow the instructions.

BY MS. HANLEY COOK:

Q What is the volume of communications copied in the course of upstream surveillance in each of the last three years?

MR. PATTON: Objection, vague. Objection, seeks classified information protected by the state secrets privilege, statutory privileges, instruct not to answer.

THE WITNESS: I will follow the instructions.

BY MS. HANLEY COOK:

Q Same question as to transactions.

MR. PATTON: Same objections with exception of vagueness, same instruction.

THE WITNESS: Following the

instructions.

BY MS. HANLEY COOK:

Q What is the volume of communications or transactions that are subject to filtering in the course of upstream surveillance in the last three years?

MR. PATTON: I'm sorry, did you use the term "Internet transactions"?

MS. HANLEY COOK: No.

MR. PATTON: I'm sorry, could you read the question back?

(The reporter read back the question.)

MR. PATTON: Objection, vague as to communications, and objection to the rest for the same reasons set forth before, instruct not to answer.

THE WITNESS: Will follow the instructions.

BY MS. HANLEY COOK:

Q Would the answer be the same if I used the term "Internet transactions"?

MR. PATTON: The instruction not to

answer would be the same, but there would be no vagueness objection, if that helps, or deemed compound since it was previous communications or transactions, but the instruction not to answer would remain the same, yes.

(Deposition Exhibit 56 was marked for identification.)

BY MS. HANLEY COOK:

Q Please take a look at Exhibit 56. Have you seen this document before?

MR. PATTON: We need to go off the record.

MS. HANLEY COOK: Okay.

(Off the record at 9:53 p.m.)

(Resume at 9:59 p.m.)

BY MS. HANLEY COOK:

Q The question was have you seen this document before?

MR. PATTON: Objection as beyond the scope of 30(b)(6). The witness can answer in her personal capacity if she's seen the document before.

THE WITNESS: I've certainly seen portions of it. I'm not sure I saw it in its entirety when I was working at DHS. I don't know that I saw it all in its entirety.

BY MS. HANLEY COOK:

Q What is it?

MR. PATTON: Same objection.

THE WITNESS: Memorandum Opinion for the Counsel to the President on 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, dated January 9, 2009.

BY MS. HANLEY COOK:

Q Thank you. Please turn to page 4 of Exhibit 56, the second paragraph that begins "EINSTEIN 2.0."

A Mm-hmm.

Q I'd like you to read the first two sentences to yourself, and tell me when you're done.

A (Witness reviewing document.) Yeah.

Q Exhibit 56 says that Einstein 2.0 sensors will scan a temporary copy of traffic, right?

MR. PATTON: Same objections.

THE WITNESS: That's what the sentence says, yes.

BY MS. HANLEY COOK:

Q Is that sentence containing "temporary copy" accurate to the best of your knowledge?

MR. PATTON: Same objection, lack of foundation as well.

THE WITNESS: To the extent that I at some point reviewed a Privacy Impact Assessment associated with Einstein 1 or Einstein 2, it was many years ago, so I can't speak to whether the specificity -- I didn't review this document in advance of any of this conversation, so I would want to go back and look at all those materials before I gave you an answer one way or the other.

I have no reason to say it's not, but I have no reason to know whether that was exactly how it was implemented, or whether it remains true

today.

BY MS. HANLEY COOK:

Q But this document at least says that it will create a temporary copy, right?

MR. PATTON: Objection, the document speaks for itself.

THE WITNESS: Yes, that's what the sentence says.

BY MS. HANLEY COOK:

Q The next sentence that I had you read says that, "Einstein 2.0 operations will not disrupt the normal operations of federal systems."

Did I read that right?

A Yes, you did.

Q Do you know why Einstein 2 involves the creation of a temporary copy of the traffic being scanned?

MR. PATTON: Objection, beyond the scope of 30(b)(6), calls for -- it also -- it also indicates I'm getting tired -- beyond the scope and lacks foundation.

THE WITNESS: Well, you can read the

words that are on the page.

BY MS. HANLEY COOK:

Q Do the words on this page indicate to you why Einstein 2 involves the creation of a temporary copy of the traffic being scanned?

MR. PATTON: Same objections.

THE WITNESS: Well, it says it's for the purpose of scanning by the sensors. I guess that's not the why.

BY MS. HANLEY COOK:

Q Doesn't Einstein 2 create a temporary copy of the traffic being scanned so that it will not disrupt the normal operations of federal systems?

MR. PATTON: Same objections, including lack of foundation.

THE WITNESS: I'm not -- again, in my personal capacity, having done work on this in previous positions, without having reviewed all those documents, I'm not willing to expound one way or the other on the particular information provided here beyond what you see on the piece of

paper.

BY MS. HANLEY COOK:

Q In June 2015, did upstream surveillance involve the scanning of a temporary copy of the transactions scanned?

MR. PATTON: Objection, calls for classified information, information subject to the statutory privileges, and instruct the witness not to answer.

THE WITNESS: I will follow the instructions.

BY MS. HANLEY COOK:

Q Going back several hours now --

A Awesome.

Q -- you testified I think, but correct me if I'm wrong, that as of June 2015, the NSA scanned at least some portions of the application layer of Internet transactions as part of upstream collection, right?

MR. PATTON: Just a second.

(Counsel conferring.)

MR. PADGETT: Can you read the

question?

(The reporter read back the question.)

THE WITNESS: Can we go off the record?

MS. HANLEY COOK: Yeah, thank you.

(Off the record at 10:06 p.m.)

(Resume at 10:11 p.m.)

THE WITNESS: Can you repeat your sentence one more time to make sure I was accurately -- or can you repeat what you --

MS. HANLEY COOK: Dawn, do you mind reading it? Thanks.

(The reporter read back the question.)

THE WITNESS: Yes, that's correct.

BY MS. HANLEY COOK:

Q You also testified that deep packet inspection refers to the scanning of the application layer of Internet packets, right?

A In the general -- oh.

MR. PATTON: Object to the extent it may mischaracterize the testimony, and beyond the scope, but the witness can answer.

THE WITNESS: In the general sense, as is traditionally understood for what deep packet inspection means, not specific to upstream.

BY MS. HANLEY COOK:

Q But it's accurate then to say that upstream surveillance, as of June 2015, involved deep packet inspection, right?

MR. PATTON: Just a moment.

(Counsel conferring.)

MR. PATTON: Objection as to vague, beyond the scope of 30(b)(6), and to the extent there's any classified information, instruct the witness not to answer.

If there's an unclassified answer that she can provide, she can provide that now.

THE WITNESS: I have no further information. I will take the instructions and not provide classified information.

BY MS. HANLEY COOK:

Q Today, how many targets does NSA have for upstream surveillance?

MR. PATTON: Objection, calls for

classified information, and information protected by the statutory privileges, instruct not to answer.

THE WITNESS: Could you ask the question again, please?

BY MS. HANLEY COOK:

Q Sure. Today how many targets does NSA have for upstream surveillance?

MR. PATTON: Same objection. If the witness is aware of any unclassified answer, we should probably talk about that.

THE WITNESS: Okay, why don't we go talk about that.

MR. PATTON: Off the record.

(Off the record at 10:14 p.m.)

(Resume at 10:14 p.m.)

MR. PATTON: Read the question back, please.

(The reporter read back the question.)

MR. PATTON: Same objections, same instructions.

THE WITNESS: I will follow the

instructions.

BY MS. HANLEY COOK:

Q In June 2015, how many targets did NSA have for upstream surveillance?

MR. PATTON: Same objection, same instruction.

THE WITNESS: I'll follow the instructions.

BY MS. HANLEY COOK:

Q Without revealing the -- you good?

MR. PATTON: Yeah.

BY MS. HANLEY COOK:

Q Without revealing the contents of any conversations that you had with your attorneys outside this room today, and with the exception of conversations related to determining whether classified information was responsive to a question, where the line was properly drawn on classified information, state secret classifications, during breaks in the deposition today, did you discuss with anyone the substance of your testimony during the deposition?

MR. PATTON: Subject to those caveats you said, plus the statutory privileges, the witness can answer.

THE WITNESS: No.

MS. HANLEY COOK: I have no further questions.

MR. TOOMEY: Can we take a break?

MS. HANLEY COOK: Strike that I said that. Take a break for five minutes to be sure, just go back through the outline.

(Off the record at 10:16 p.m.)

(Resume at 10:26 p.m.)

FURTHER EXAMINATION

BY MR. TOOMEY:

Q When a communication is encrypted using HTTPS, does some of the communication's metadata remain unencrypted?

MR. PATTON: One second.

(Counsel conferring.)

MR. PATTON: Object to the question as beyond the scope of 30(b)(6), calling for an expert opinion. The witness can answer in her

personal capacity to the extent that she is aware of the answer.

THE WITNESS: In the general sense, it will depend on the type of encryption that's being used, and it will depend on the nature of how it's being transmitted, so there's not one answer that fits all.

BY MR. TOOMEY:

Q So when a communication is encrypted using HTTPS, does some of the communication's metadata remain unencrypted?

MR. PATTON: Object to the term "communication" as vague, and same prior objections and instruction to the witness.

THE WITNESS: To the extent that the question is somewhat vague, I'll say generally speaking, yes, but I think there are different ways you could do things that might change that answer.

BY MR. TOOMEY:

Q When a communication is encrypted using HTTPS, are the senders and recipients'

IP addresses unencrypted?

MR. PATTON: Same objection, same instruction.

THE WITNESS: Generally speaking, they will -- I'm sorry, say the question one more time.

(The reporter read back the question.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: Again, the question is somewhat vague, and so I would answer generally that is true, but there are undoubtedly a number of exceptions that also could make that untrue.

MR. TOOMEY: Could you please mark this document as 57.

(Deposition Exhibit 57 was marked for identification.)

BY MR. TOOMEY:

Q Could you please take a look at the document, describe what it is, and tell me if you're familiar with it.

A This is the Notice of Filing of Government's Responses to FISC Questions Regarding

the Amended 2011 Section 702 Certifications, dated November 15th, 2011.

Q Thank you.

A Yes, I am familiar with these documents.

Q Could you please turn to page 9?

A Sure.

Q I'm going to read from about the third paragraph down in the middle of the personal knowledge, which says, "Metadata that has been extracted from Internet transactions consistent with Section 3(b)(5)(b)(4) is subject to the two-year retention limit set forth in Section 3(c) of the amended NSA minimization procedures."

Was that statement accurate at the time this document was filed with the FISC on November 15th, 2011?

A Yes.

Q So the NSA extracts metadata from communications collected in the course of upstream surveillance, correct?

MR. PATTON: Just a moment.

(Counsel conferring.)
MR. PATTON: Objection, vague as to time period, but the witness can answer.
THE WITNESS: Could you ask the question again?
(The reporter read back the question.)
MR. PATTON: Objection, vague as to time.
THE WITNESS: So I would just offer that the answer to your question is metadata has been extracted from the Internet transactions. I believe that the question said communications, in which case that would be consistent with the information that was provided here.
BY MR. TOOMEY:
Q So I'll rephrase.
The NSA extracts metadata from Internet transactions collected in the course of upstream surveillance, correct?
MR. PATTON: Objection, vague as to time.
THE WITNESS: Consistent with 2011,

what's written here at 2011, yes, that is true.

BY MR. TOOMEY:

Q Today, the NSA retains metadata associated with its targets' communications in the course of upstream surveillance, correct?

MR. PATTON: Hold on.

(Counsel conferring.)

MR. PATTON: Sorry, could you read the question back, please?

(The reporter read back the question.)

MR. PATTON: Object to the question to the extent it calls for classified information or otherwise privileged pursuant to the aforementioned statutes.

If there is an unclassified answer, the witness can provide it.

THE WITNESS: Could you read the question one more time?

(The reporter read back the question.)

MR. PATTON: Same objection, same instruction.

THE WITNESS: NSA retains -- I would

again go back to, instead of saying "communications," I would say "Internet transaction." I would say generally, yes, this is true.

BY MR. TOOMEY:

Q Sorry, I didn't hear you. Could you say that again?

A Sure. NSA retains metadata -- may retain metadata associated with Internet transactions in the course of upstream.

Q The NSA has an interest in the metadata of its targets' communications or Internet transactions, correct?

MR. PATTON: Objection as vague, beyond the scope of 30(b)(6).

The witness can answer.

THE WITNESS: NSA is interested in the metadata associated with the Internet transactions of a targeted selector -- to or from a targeted selector.

BY MR. TOOMEY:

Q So just to be clear, just to make sure

I understood your answer, the NSA has an interest in the metadata of communications to and from a targeted selector?

MR. PATTON: Objection, beyond the scope. The witness can answer.

THE WITNESS: Could you repeat the question?

(The reporter read back the question.)

THE WITNESS: I would not use the word "communications." I would use the word "Internet transactions."

BY MR. TOOMEY:

Q So just to be clear, the NSA has an interest in the metadata of Internet transactions to and from a targeted selector?

MR. PATTON: Objection, beyond the scope, asked and answered.

THE WITNESS: Yes.

MR. TOOMEY: Thank you. All right, we do not have any further questions right now.

MR. PATTON: Before we get off the record, the government is going to invoke Federal

Rule of Civil Procedure 30(e) to reserve the right to review and signature of the witness.

(Whereupon, at 10:36 p.m., the taking of the deposition was concluded. Reading and signature were reserved.)

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

| | | |
|---|---|---|
| WIKIMEDIA FOUNDATION, | : | |
| Plaintiff, | : | Case No. |
| vs. | : | 1:15-cv-00662-TSE |
| NATIONAL SECURITY AGENCY, et al., | : | |
| Defendants. | : | |

ACKNOWLEDGMENT OF DEPONENT

I, REBECCA J. RICHARDS, do hereby acknowledge that I have read and examined pages ~~11~~ 9 through ~~239~~ 359 of the transcript of my deposition taken on Monday, April 16, 2018, and that:

(Check appropriate box):

( ) the same is a true, correct and complete transcription of the answers given by me to the questions therein recorded.

(X) except for the changes noted in the attached errata sheet, the same is a true, correct and complete transcription of the answers given by me to the questions therein recorded.

5/15/18
DATE

SIGNATURE

**Wikimedia Foundation v. NSA, et al., 15-cv-00662-TSE (D. Md.)**

**ERRATA SHEET of REBECCA J. RICHARDS**

| Page | Line | To | From | Justification |
|---|---|---|---|---|
| 9 | 8 | Kathleen | Cathleen | Spelling Error |
| 45 | 4 | Michael S. Rogers | Michael F. Rogers | Spelling Error |
| 161 | 19 | telecom | teleco | Spelling Error |
| 169 | 19 | USA FREEDOM Act | USA Freedom Act | Capitalization |
| 192 | 6 | Protocol | protocol | Capitalization |
| 196 | 13 | (with our targeting procedures) | in parens | Transcription Error |
| 263 | 17 | scanned | scan | Clarification |

CERTIFICATE OF NOTARY PUBLIC

I, DAWN A. JAQUES, a Notary Public in and for the District of Columbia, before whom the foregoing deposition was taken, do hereby certify that witness whose testimony appears in the foregoing pages was duly sworn by me; that the testimony of said witness was taken by me in shorthand at the time and place mentioned in the caption hereof and thereafter reduced to typewriting under my supervision; that said deposition is a true record of the testimony given by said witness; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this deposition is taken; and, further, that I am not a relative or employee of any attorney or counsel employed by the parties thereto, nor financially or otherwise interested in the outcome of the actions.

Dawn A. Jaques

Dawn A. Jaques, CSR, CLR
Notary Public in and for
District of Columbia

My commission expires:
January 14, 2020

*** ERRATA SHEET ***
TRANSPERFECT DEPOSITION SERVICES
216 E. 45th Street, Suite #903
NEW YORK, NEW YORK 10017
(212) 400-8845

CASE: WIKIMEDIA FOUNDATION v. NATIONAL SECURITY AGENCY, et al.
DATE: APRIL 16, 2018
WITNESS: REBECCA J. RICHARDS REF: 21368

| PAGE | LINE | FROM | TO |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

_____
REBECCA J. RICHARDS

Subscribed and sworn to before me

this ____ day of _____, 20__.

_____
Notary Public

**A**

**Abdo** 3:3 5:4 8:2,3 8:19 9:11 11:22 12:11 15:21 18:3 19:3 23:12 26:4 27:15 28:14 29:4 29:6,19 31:2,3 34:14,19 35:15,20 36:16 39:6 40:21 41:12 42:3,20 43:1,10,16 44:10 44:18 46:4 47:5 48:9 49:2,10,20 50:17 51:10,14,20 52:13,15 53:6,13 53:19 54:4 55:13 56:3,11,21 57:4 58:11 59:19 60:10 60:17 61:3,19 62:5,17 63:1,21 64:16 65:14 66:12 67:1,18 68:8 69:1 69:15 70:4 71:10 72:2,21 74:1,22 75:18 76:2 77:7 78:20 79:4,12,21 80:11 81:16 82:6 82:17 83:8,14 84:2,9,12 85:2,9 86:7,16 87:12 88:20 89:5,17 90:9,16 91:3,21 92:11 93:8,16 94:13,21 95:4,9 96:11 97:4 99:5 100:14 101:21 102:22 103:9 104:3,16 106:14 107:20 108:16 109:6 110:18,22 112:4,15 113:5,17 114:7 115:13,17 116:6 118:4,11 119:1,10,19 120:9 121:7 122:6,12,17 123:6,18 124:4,8 124:10 125:2,7,21 126:6,19 127:4,6 128:1,9,21 129:9 129:12,17 130:17 132:17 133:21 135:1,11,21 136:5 136:11 137:1,6,13 138:2,12 139:7 140:12 141:14 142:10 143:8,18 144:5,18 145:13 145:18 146:4,9,17 147:3,11,20 148:5 148:12,18 149:5,8 149:17 150:2,9,16 151:1,8,16,20 152:6,14,21 153:6 153:14 154:1,16 155:13 156:19,22 157:15 158:1,12 159:2,6,10 160:18 161:7 162:1,13 163:1,9 164:3,16 165:2,11,19 166:5 166:14,21 167:6 167:17 168:3,12 169:3,8,16 170:21 171:9 172:4,17 173:4,21 174:15 175:17 176:8 177:17 179:5,14 180:1,15 181:1,9 181:16 182:3,10 182:17 183:2,9,16 184:5,12,20 185:5 185:12 186:8,16 187:7,10,13 188:2 188:8,12 189:8,12 189:15 190:8,12 193:19 195:3 197:2,10 198:5,7 199:16 201:11,16 202:6,16 203:8 204:12 205:13 206:1,12 207:5,18 208:5,12,20 209:7 209:21 210:4 212:8,14 213:12 213:20 214:4 216:3,16,21 219:6 219:21 220:3,21 223:2,16 224:9,17 225:2,10 226:5,14 226:17 227:6 228:9 229:1,7 231:1,7,12,15 232:7 233:15 234:16 235:4,14 236:11 237:1,11 238:5 239:5 240:3 240:20 241:10,16 241:21 242:9,18 243:7,15 244:7,17 245:9,18 246:6,13 247:20 248:17,21 249:7,14,22 250:3 250:14 251:14 252:1 253:11,14 253:17 254:19 255:5,14 256:6,19 257:13 258:9 270:6

**Abdo's** 30:17

**ability** 42:11 103:6 280:19 281:16 282:2,8

**able** 13:9 17:19 32:21 34:6 44:13 50:18 75:2 145:1 164:12 187:9 197:3 237:20 238:22 239:5 241:14 272:21 305:7 309:14

**abouts** 107:10,17 140:9 218:5 295:1 308:6,10,12 310:17 314:13,17 315:18

**abroad** 230:1,12,15 231:2,17 232:1 234:7,19

**Absolutely** 37:16 51:19 95:13 100:17 131:4

**abstract** 237:22 240:18

**Accelerated** 6:12 248:10 252:10

**accept** 102:7,19

**accepted** 49:17 105:8

**access** 144:13

**accommodate** 14:5

**accomplish** 200:13 201:1

**Accord** 34:2

**account** 217:22 218:3

**accuracy** 97:1 98:9 98:18 99:19 100:5 100:7,10 101:14 102:1 105:2 130:9 221:1

**accurate** 101:10,17 106:11 107:2,18 108:8,12,15 109:3 109:10 110:1 111:15,18 112:9 112:13 115:19 117:11 119:22 131:3 132:19 133:1 136:8,19 137:18 139:18 140:3,7,11,17 141:2 160:17 166:1,7,12 177:16 189:17 212:11 240:19 313:8 319:6 325:11 344:9 349:5 355:15

**accurately** 17:20 18:7 107:12 117:4 158:8 240:16 262:21 348:10

**acknowledge** 261:6 361:10

**acknowledged** 235:6 236:13 242:3

**ACKNOWLED...** 361:9

**ACLU** 3:19,20 258:5

**acquire** 63:2 160:5 168:14 170:4 188:15,16 195:8 196:2 197:17 199:1,22 233:10 268:15 304:2

**acquired** 330:5,13

**acquires** 206:10

**acquiring** 198:21

**acquisition** 124:19 196:10

**act** 5:15,18 24:4 25:11 28:19 31:21 32:13,14 38:3 95:18 130:6 169:18,19 177:11 177:14 210:15 233:13

**action** 362:13

**actions** 362:17

**activities** 6:19,21 22:22 36:11 39:5 271:14 312:20 318:8,20 319:5 320:5,15

**activity** 26:11 221:15 222:7,14 223:6,7,8,20 224:11,22 225:3,4 225:5,20,21,22 226:19,21 227:3 227:15

**add** 83:20 103:19 187:11 191:4,6,8 192:2 307:16 309:7

**added** 114:20,21 192:17

**adding** 225:16 279:5

**additional** 50:11,14 112:20 113:19 169:14 203:13,21 264:15,18,20

268:7 269:14 295:3 297:17,19 297:21 298:1 307:14 309:13 327:10,13,15
**additionally** 192:17
**address** 16:3 191:20 206:13,19 310:17
**addresses** 283:5,10 354:1
**addressing** 15:5
**adhere** 15:9
**administered** 12:4
**administration** 249:10,16
**Admiral** 30:3 45:3 119:7 120:2,12 315:17 316:2
**admission** 30:5 68:7 69:18,19 73:13 109:16 111:17 119:15
**advance** 344:17
**advice** 77:10 169:15
**adviser** 25:3
**Advisory** 38:3
**advocate** 25:11
**aforementioned** 207:1 357:14
**agencies** 32:19
**agency** 1:7 4:15 9:2 9:7,10 25:11 30:2 33:2 45:3 142:20 220:14,20 233:8 314:10 361:5 363:4
**Agency's** 11:13 65:7
**agent** 179:12
**ago** 25:1 77:14 185:20 214:9,21 344:15
**agree** 41:1 51:14 117:19 119:2
**agreed** 9:19 15:4 34:7 321:11
**agreement** 34:2 239:19
**Ah** 247:4
**ahead** 13:20 108:5 125:18 138:10 145:8 247:21 327:7
**al** 1:7 361:6 363:4
**Alex** 3:3 8:3
**alex.abdo@knig...** 3:9
**allow** 33:1 169:12 186:3,19
**altogether** 280:22 281:3
**ambiguous** 38:22 137:12,14 168:10 228:17
**amended** 7:10 233:13 355:1,14
**Amendment** 3:4 8:4
**American** 8:9,11 258:13
**Amicus** 169:13 170:1
**amorphous** 54:11
**amount** 135:5 241:4
**analogous** 158:14 158:21 159:4
**analysis** 105:3
**analyst** 286:1
**analysts** 312:22
**analyzing** 246:8
**and/or** 15:8 148:21
**announced** 249:10
**announcing** 249:15
**answer** 10:5 13:21 14:1,11 16:8,19 17:8,16,19 18:6 23:13 25:21 28:12 35:15,16 39:1,14 39:20 40:19 42:5 42:7,11,20 44:5 47:1 48:6,21 49:7 50:6 51:9,12,15 52:7 53:4 54:7 56:19 59:14 60:7 61:1,16 62:2,11 62:16 63:15 66:5 66:19 67:11 68:5 68:11 70:5,6,7,8 70:10,11,17 71:2 71:3,5,12,19 72:1 72:5,6,9 73:7,8,11 74:9,16,17 76:13 77:5,9,11 80:9 81:4,4 82:4 84:22 85:4,6,11 87:14 88:4,8,15,15 89:6 89:12 90:6,22 91:17 93:10 95:1 96:7 102:16,17,17 104:17,19 108:5 110:11,12,14 111:5,8,9 113:1 113:15 114:1 116:4,8,10,11,13 116:15 117:2,7 118:21 120:6 121:21 122:2,10 122:14 123:4,14 125:5,8 126:15 127:21 128:7 129:6 133:18 134:6 138:22 139:16 146:1 155:3,6 156:6,6 157:6 160:15 161:5 162:9 163:12,22 164:9 164:10,11 169:4 170:22 171:1 172:13 174:9 178:4,5 179:2 180:12 187:2 188:3,4,6,7,10 189:1,3,6,9,11 191:22 192:8 193:8 195:1 196:22 197:3 198:2,14 201:8 202:2 203:4 204:8 205:19 207:2 208:3,4 212:8,20 213:18,18,20 214:3,12,13 215:11,22 216:10 216:11,15 217:10 219:18 222:18,18 222:20,21 223:1 224:5,16 227:14 228:21 229:2 230:6 234:9,12 236:4,6,8,16 237:2,4,5,9,11,15 237:21 238:1,18 239:2,3,6 240:22 241:2,12 242:7,15 243:21 245:6 247:2,15,18,19 248:15 250:9 252:15,18 254:16 255:20,22 256:7 258:22 259:16 261:1 262:18 263:16 264:12,13 265:16 266:2,11 267:12 268:1,4,5 268:21 269:11 270:4 272:20 273:7,10,14 274:13,14 277:17 278:15 279:2 280:2 281:8 282:14 283:15 284:20 285:2,6,17 285:18 286:21 287:18 288:12 289:10,14 290:2 290:12 293:19 294:17 295:21 296:3 297:3,15,16 298:11 299:4,22 300:6,7,12 302:10 302:14 303:20 304:8,8,20,21 305:7,8,19 306:12 306:18 307:18,20 308:3,21 309:9,10 310:13 311:4,16 313:13,14 314:2 315:5,15 317:5,8 317:9,18 319:18 320:1 321:7 323:1 323:17,18,20 324:20 325:6,8 326:6,18 327:6,9 327:22 328:1,21 331:11,21 332:2 332:19 333:7,13 333:15 335:10 337:6,17 338:4 339:8,21 340:15 341:16,20 342:1,4 342:20 344:19 347:9 348:22 349:13,14 350:3 350:10 352:3,22 353:2,6,19 354:10 356:3,10 357:15 358:16 359:1,5
**answered** 51:5 54:20 94:4 96:19 105:18 108:5 125:18 139:15 141:4 145:8 189:6 225:18 279:6 359:17
**answering** 14:16,19 15:22 27:12 64:15 69:11 71:16 72:8 74:7 84:15 104:14 117:20 118:12 120:3 121:12 177:5 238:4 253:2 288:21 310:7
**answers** 13:5,7 18:1 125:11 177:15 250:10 361:16,19
**anybody** 85:3
**anyway** 103:12
**Apache** 336:15 337:2
**apart** 296:7,21

298:7 299:18 300:9 326:13
**Apologies** 308:13
**apologize** 247:22
**appeal** 172:16,22
**appear** 260:6
**appearances** 3:1 4:1 9:12
**appearing** 18:19 19:17
**appears** 195:10 226:14 269:19 362:5
**Appendix** 118:5
**Appids** 7:6
**applicable** 10:19 232:12 284:22
**application** 28:9 242:21 243:10 244:4 246:8 261:16 263:6,9,12 263:17,22 266:6 301:18 306:3,22 347:17 348:18
**applications** 29:10 165:15,22
**applies** 27:17
**apply** 17:6
**applying** 28:15 29:7
**appreciate** 139:8 149:9
**appreciation** 38:7
**appropriate** 11:11 286:3 361:15
**appropriations** 316:16
**approval** 11:13 33:12 165:4 309:13 310:19
**approve** 310:16
**approved** 219:11 229:20 249:4 308:6
**approves** 322:7
**approving** 209:15
**approximate** 145:14 146:10 147:12,21 181:17 182:4 183:3,10 184:21 185:6
**Approximately** 67:21 68:14 69:3
**April** 1:13 5:16 6:11,15,18,20 130:6 132:5,11,20 133:5,13 193:22 252:10 293:21 294:21 295:7,10 297:3 298:11 299:22 300:14,20 301:9,17 302:3,18 303:5 304:15 305:5,6,9,13 306:2,14,15,21 312:10 318:6,19 320:16 321:15,17 361:13 363:4
**area** 39:3 52:12
**areas** 35:9 40:11 42:18
**argumentative** 125:18
**arrived** 76:7,9 222:10
**article** 173:17 240:15
**Ashley** 3:20 8:10
**aside** 23:4 117:13 138:3,13 143:20 145:2 168:16
**asked** 51:4 54:6 73:2,7 78:17 86:5 93:1 94:4 105:13 108:5 109:8 116:12 125:17 139:14 140:19 141:4 145:7 157:1 185:20 186:1 197:4 214:8,16,21 216:2 219:5 224:1 225:18 236:7,8 239:16 243:14 247:3 265:22 279:5 289:12 359:17
**asking** 13:4 19:13 40:22 42:1 44:9 44:11 48:16 49:21 49:22 54:6 59:2 64:6,15 65:15,16 65:17 67:13 70:6 74:3,18 80:12,15 80:18,21 93:6 103:11 115:18 118:6 121:6 143:19 144:21 155:17 169:1,6 174:11 177:18 204:10 209:19 221:19 227:7,14 227:21 235:15 237:2,3,13,14 241:11 252:16 258:8 261:4 278:11,14 305:1 321:2
**aspect** 288:22 289:5
**aspects** 101:19 140:16 174:19 261:6
**assert** 30:21 103:6 103:10,16 163:20 324:2
**asserting** 164:13
**assertion** 121:2 125:13
**assertions** 118:7 136:7
**assessing** 233:20
**assessment** 6:11 31:20 32:11 249:1 252:7,12 344:13
**assessments** 26:15 33:4 36:9 246:19 246:22
**assist** 126:9 132:8 133:11 198:21
**associated** 39:21 199:1 283:6,10 295:5 344:14 357:4 358:9,18
**assume** 175:7 227:18 237:18
**assumed** 331:15 333:19
**attached** 361:18
**attempt** 275:15 276:3,11,18 290:7 290:17 291:4,11
**attempts** 296:9 297:3
**attention** 108:17 131:18 190:1
**attorney** 170:11,13 295:22 321:9 362:15
**attorneys** 8:17 103:20 351:14
**attorney-client** 63:13,16
**August** 240:5,14
**authored** 220:15
**authoritative** 135:14
**authorities** 6:13 15:13 124:14 279:16 280:8
**authority** 27:18 28:16 29:8 163:18 164:13 167:2 179:1 232:3 234:6 234:18
**authorized** 206:6
**authorizing** 294:20
**available** 20:17 38:4 70:12,14,18 74:5 135:6 203:15 320:3
**Avenue** 2:7 4:8
**average** 146:18 147:4
**avoid** 96:5 105:5 189:2 296:9 297:4
**aware** 102:6 106:15 108:1 137:7 138:4 138:14 139:1,10 145:3,9 170:14,17 170:18 174:1 213:10 235:5,15 236:12 240:4 242:1,8 243:8 244:2 248:7 249:8 249:15 295:18 299:3 315:16 317:7 325:7 327:4 350:10 353:1
**Awesome** 347:14
**awful** 104:9,12
**a.m** 2:5 53:20,21 62:20,21 75:20,21 110:20,21
**a[n** 250:22

## B

**B** 5:21 27:10 213:16
**back** 24:12 39:7 53:5,10 55:14 56:8 68:6 72:16 72:19 73:1 95:3 102:12,13 111:1,2 120:19,22 127:13 127:15 132:14,16 133:21 134:1 140:1 143:5 149:3 153:15 157:2 158:2 167:14,15 171:18,20 175:16 177:9 180:7,8 183:21,22 185:13 187:14 189:3,19 197:9,21 198:12 207:19 214:16 216:22 217:13,16 218:18 231:22 236:2 244:16 245:1,2 260:16,18 260:19 262:2,11 262:14 267:1,2,8 271:5 272:16 277:12,14 284:15 284:16,18 286:10 286:11,17,18

287:3 297:11,12 298:19,20 303:15 303:16 308:6 310:3,5,6,16 315:18 323:6,12 323:13,15 325:2 325:12 335:3,6 338:21 339:1 341:11,12 344:18 347:13 348:2,13 350:17,19 352:10 354:6 356:6 357:9 357:10,19 358:1 359:8
**backbone** 46:18 47:4,10,13,17 48:1 49:5,15,22 50:14 51:2 52:21 54:10,22 61:7 62:14 63:4,10 64:2,7,19,22 66:22 68:1,16 69:5 73:5 78:11 79:7,17 80:7 121:19 122:7,8,22 123:9 124:21 125:16 145:15 146:11,19 147:5 147:13,22 148:20 148:22 149:12,19 150:4,11,18 151:3 151:11 152:2,9,16 153:1 157:12 163:4 199:3 258:18 259:9 260:1 261:17 263:13,18 266:7
**back-and-forth** 105:10
**baffled** 230:21
**baffling** 231:11
**bandwidth** 46:19 47:19 48:2,17 49:4 50:21 55:4 62:15 146:18 147:4,13,22 151:10 152:1,8,16 153:1
**barrier** 308:16,19 309:2,4 314:14,19
**barriers** 307:7 309:14,19 313:17 313:19
**based** 15:5 17:8 70:18 175:1 218:6 251:2,8 284:6 288:22 289:3,10 307:18 327:9,19 339:9
**basically** 261:11
**basis** 51:16 71:13 77:4 118:7 238:2 260:5 265:13
**Bates** 5:21 142:6 155:16,18 159:16 159:19 160:12 161:21 174:14 221:7
**bearing** 32:7
**Becky** 84:7,15
**beginning** 199:21 226:8 250:21
**begins** 108:21 160:1 185:15 187:16 194:6 221:12 312:17 343:16
**behalf** 3:2,18 4:2 9:18 103:8
**belief** 71:16
**believe** 16:11,15 55:11 68:7 71:20 73:6,9 94:17 97:5 108:15 118:12 142:3 158:5,17 164:4,15,19 174:13,22 176:5 177:21 189:6 203:5 226:6 227:15,20 232:15 251:15 265:18,19 289:17 316:11 356:12
**believed** 179:18 233:9
**believes** 15:6,12 16:6,10 114:13
**belong** 301:19
**best** 17:12,16 32:9 138:1 141:10 172:2 198:16 214:2 221:3 270:10 272:2 273:1 344:9
**better** 37:5,14 39:12,14 47:11 89:9 137:21 159:4 236:20 238:20
**beyond** 37:10 55:20 56:9 64:5 66:7 69:8,11 76:12,17 77:3 83:20 84:3,20 85:19 86:11 87:8 88:1 89:4 90:21 91:16 94:2 99:3 102:14 115:2 118:3 128:15 165:8 168:10,20 170:16,20 171:21 172:12 173:11 179:1 190:19 224:15,18 232:16 242:6 243:4 245:13 247:14 248:11 250:8 255:9 256:17,22 264:16,19,21 265:19 268:7 269:15,18 277:16 283:11 285:16 286:19 295:4 297:18 304:8 307:9 308:18 309:14 315:4,14 317:4 319:15,16 321:18 322:2 325:20,20 327:16 331:11 333:6 337:5 342:19 345:18,20 346:22 348:21 349:11 352:21 358:15 359:4,16
**big** 92:20
**binders** 23:16
**bit** 49:11 156:13 197:12 219:9 320:1
**black** 233:4
**board** 5:13 26:19 95:16 96:17 99:2 131:7 172:15 210:12
**Board's** 20:9 105:3
**bomb** 218:20
**bottom** 33:12,13 108:21 109:9 110:5 221:11 280:15 282:20 312:16
**box** 361:15
**Branch** 2:6 4:7 176:5,14 179:12 343:13
**Brand** 218:8,12
**break** 14:4 29:17 30:7,17,20,21 52:3 53:15 62:18 62:20 110:17 122:15 128:9 133:17 153:7,10 153:12 187:10 190:8,10 202:14 207:19 216:16 257:22 258:2 284:22 352:7,9
**breaks** 14:3 351:20
**brief** 199:8
**briefing** 6:7 220:10
**briefings** 27:2 316:8
**briefly** 32:10 185:14 187:14
**briefs** 198:7
**bring** 217:16
**bringing** 61:8
**broad** 41:10 101:17 157:19
**broadly** 96:8
**broke** 111:1 289:4
**browsing** 223:19
**budget** 314:9
**bulk** 270:16 271:11 271:11,13,17 272:1,7,12 273:5 273:9 274:9,18 275:3,9
**bullet** 333:22
**bunch** 93:2 229:11

C

**C** 8:1 27:11
**CA** 3:14
**cable** 56:16 59:8 60:2,11 61:22 62:7 78:4,22 79:6 79:16 80:1 81:6 81:19,22 157:11
**cables** 60:21 61:13 78:18 182:12,19 183:4,11
**California** 3:13
**call** 96:1 118:18 155:2 156:4 188:6 228:17 232:20 240:6
**called** 2:3 12:7 33:10 34:17 38:15 199:9
**calling** 51:6 53:3 255:10 257:1 352:21
**calls** 16:16 40:15 46:21 48:5,20 49:6 50:5 51:5 55:9,17 56:18 58:5 59:12 60:6 61:1,15 62:11 63:13 65:10 66:5 66:19 67:10 68:4 68:19 69:7 70:22 71:20 76:11 78:9 79:9,19 81:10 82:4,22 83:12

84:19 86:10 87:8 89:3 90:4,21 91:15 94:1 97:16 111:5 116:1 118:10 121:21 123:11 126:11 127:18 129:3 135:17 145:19 154:12 156:3 157:4 158:10 161:2 162:7 166:8 168:19 173:10 174:6 178:22 194:18 196:19 201:5,21 202:21 204:6 205:18 206:21 207:22 217:8 219:15 222:17 223:21 225:17 242:13 243:2,3 245:4,13 253:20 254:13 258:19 260:21 262:16 264:12 266:8 267:10 268:1,19 269:8 270:2,17 272:18 274:11 281:5 282:11 283:12 284:20 285:3 286:20 289:18,22 290:10 294:3 296:2 297:14 298:22 300:4 305:16 307:10,17 308:20 310:11 311:2,14 313:22 317:5 321:6,18 322:3,20 323:17 325:4 326:4 327:1 328:18 331:21 333:13 335:8 337:5,15 345:19 347:6 349:22 357:12

**capabilities** 251:1

**capable** 104:13

**capacity** 69:12,13 76:14,15 83:22 84:1 103:7 210:20 242:7 248:16 253:3 277:18,19 285:18 286:22 308:22 309:11 333:8 337:7 342:21 346:18 353:1

**caps** 58:17

**caption** 362:8

**capture** 199:5 200:17

**care** 14:14 136:17 137:3 177:12 303:1

**careful** 136:6

**carried** 61:13,21 62:7 150:17 151:2

**carries** 113:7 190:4 272:6

**carrying** 109:9 110:5 115:9 258:15

**carryover** 112:8 119:21 190:15

**case** 1:5 8:5 9:18 17:4 18:16 19:15 23:9,18,21 62:14 65:2 91:7 107:19 227:18,21 235:16 277:4 278:3 338:12 339:5 356:13 361:4 363:4

**categories** 42:15 148:6,13

**Cathleen** 9:8

**causing** 260:4

**caveats** 352:1

**CD** 11:7

**certain** 6:18,21 65:17 140:16 170:17 174:17 192:5 194:8,12,15 221:22 222:6,11 233:22 263:17,20 264:1 316:12 318:7,20 319:3 320:15

**certainly** 27:7 36:8 47:2 48:22 59:17 61:17 63:17 97:14 103:7 169:13 248:14 309:12 343:1

**CERTIFICATE** 362:1

**Certifications** 7:10 355:1

**certify** 362:4

**chance** 45:10 190:13 211:12

**change** 105:8,15 125:10 298:11 299:22 353:18

**changed** 50:7 63:20 107:9,15 140:16 247:2 294:22

**changes** 26:21,21 105:2,8 293:20 361:18

**characterizing** 158:7

**charge** 31:19

**check** 112:22 187:9 270:18 361:15

**chief** 32:15 37:19 37:19

**chokepoint** 183:19

**chokepoints** 184:8 184:15,22 185:7

**chosen** 143:5

**circuit** 57:22 78:5 78:11,22 79:6,16 80:2,6,9,17,19,22 81:1,7,11,12 82:2 82:16,19 83:5,6,7 83:9,15 84:17 85:16,20 86:2,5,9 86:19 87:2,5,18 87:22 88:11,18,22 89:10 91:12 92:3 92:4,10,13,18,19 92:21 93:6,7,12 93:15 94:9 121:19 122:7,8,22 123:9 125:16 152:15,22 154:3 157:11 158:7,17,22 163:4 198:8 322:18 324:10,18 326:16

**circuits** 49:9,16 58:4,8,10 87:1,2,4 87:6 91:12,20 93:20 94:6,7,17 124:20 125:9 145:15 146:11,19 147:5,13,22 148:6 148:13 198:22 322:19 324:10

**circular** 94:7 237:7

**circumstance** 82:7 82:8

**circumstances** 90:17 192:5 194:8 194:12,16 322:8

**cited** 124:15

**civil** 2:6 4:6 5:13,17 8:9,11 20:7,9 24:16 25:3,6,9 26:19 28:7 95:15 101:6 109:21 120:14 130:4 131:7 170:11 192:2 209:13 210:11 219:3 258:13 299:10 314:10 325:14 360:1

**claims** 16:3 41:3

**clarification** 155:10 215:14

**clarified** 53:22

**clarify** 25:15 26:5 67:12 77:17 157:5 212:13 221:18

**clarifying** 213:5 305:3

**classifiable** 178:18 179:9,20

**classification** 22:13 39:3 51:16 71:14 74:8 97:2 98:22 99:6,10,11,22 100:3 101:2,14 111:14 116:18 130:9 141:9 163:17 164:12 176:5,14 179:1 215:16

**classifications** 177:1 351:20

**classified** 10:2,9,15 11:16 15:11,20 16:6,10,13,16 18:1 20:18 21:1,1 21:2,5,9,14 22:9 22:16 23:3 30:7 30:10 39:22 41:13 41:18 42:5 50:8 50:16 51:7 52:12 54:16 63:14 70:22 71:17,20 72:9,10 73:14 75:3 76:6 97:3,19 98:1,5 99:4 101:3,5,12 105:12 110:9,12 110:13 111:5 112:2,17,21 113:13,20 114:3 114:16 116:2,14 116:15 117:5,16 118:18 121:21 122:3 123:1,3,11 124:13 126:12 127:18 128:16 129:4 131:14 133:3 134:4,21,22 139:5,21 140:4 141:12 144:12,17 145:12,20 151:15 155:2 156:4,10,12 156:12 161:2,22 174:7 175:10,11 175:20 178:20 179:10,18 180:10

188:7,11 190:20 193:10,11 194:18 196:20 199:14 201:6,22 202:22 204:6 205:18 206:22 208:1 209:12 214:17 215:1 216:10 217:8 219:5,16 222:17 223:22 226:11 228:6,18 232:20 233:2,3 234:10 235:19 236:21 239:4,6,9 239:17 241:7 242:13 243:2 245:4 248:1,12 254:14 256:8,14 256:16 258:20 260:5,21 261:7,12 262:3,16 264:6,12 265:2,5,20 266:1 266:9 267:10 268:1,12,19 269:8 270:2,18 272:18 273:12,17 274:11 277:21 278:8,17 281:5 282:12 283:13 284:20 285:3 287:14 288:2,19 289:8,9 289:13,17,22 290:10 294:3,12 294:16 295:20 296:2,14 297:14 298:3,22 299:14 300:4 302:8 303:18 304:6,21 305:8,17 307:18 309:8,9 310:11 311:2,14 313:22 317:5,10 322:21 323:17 325:4 326:4 327:1,18 328:19 331:21 332:14,15 333:13 335:8 337:15 339:7,19 340:13 347:7 349:12,18 350:1 351:17,19 357:12

**clean** 145:1 289:20

**clear** 13:12,15 16:5 17:12,14 22:12,12 27:16 29:20 30:16 35:22 36:20 40:21 55:2 69:10 78:15 80:13 86:17 149:10 202:15 205:1 249:16 294:7 308:13 358:22 359:13

**clearer** 13:17 41:14 134:9,18 320:9

**clearly** 16:13,18 104:4 118:6 144:6 197:11

**clicking** 156:11

**closely** 37:18 106:8 106:9

**CLR** 2:8 362:19

**CNCI** 253:5

**coffee** 14:7

**colleague** 177:4 307:22

**colleagues** 8:8 118:2

**collect** 206:6 219:12 228:12 229:21 230:10 232:4 234:4,6,19 284:5

**collected** 242:3,10 295:1 355:20 356:18

**collecting** 233:21 273:5 274:6 296:10 297:4

**collection** 6:19 107:10,11,16,17 111:19 140:9 195:7 196:1 197:16 204:17 209:17 212:6,17 213:1 214:20 215:9 217:6 218:2 221:14 222:1,7 223:15,18 224:1 230:14,20 234:21 235:9 236:15 238:6 244:10 253:20 271:18,21 272:2 293:21 294:22 295:2 307:8 308:9,11,13 308:17 309:5 313:2,11,20 315:1 315:11,19 316:21 317:14 318:7 319:9 320:18 321:15 322:1,11 347:19

**collections** 218:4

**collects** 206:7,9

**college** 36:2

**Collyer** 6:17

**Columbia** 2:9 8:4 362:3,20

**combined** 147:12 147:21

**combining** 149:10

**come** 41:17 121:11 146:5 187:9 189:3 222:4 259:14

**comes** 47:9 199:8

**comfort** 239:16

**comfortable** 161:15 203:4

**coming** 211:2 311:20

**commencing** 2:4

**comment** 131:8 214:22

**comments** 104:22

**Commerce** 33:22 34:4

**commission** 34:3,5 362:21

**committee** 38:3 316:10,12

**common** 91:11 94:16 254:6,22

**commonly** 157:12 256:20 257:6

**communicated** 231:22

**communicating** 212:3 231:3,5,8

**communication** 91:10,15 93:18 126:8 160:6,7 188:17,18 232:4 243:9 266:18 267:21 274:5,6 305:10 339:19 352:15 353:9,13 353:21

**communications** 39:17 67:15 124:20 132:10 133:12 170:10 196:7 198:22 205:15 206:5 222:15 223:15 225:14 227:17 228:12 229:21 230:11 231:12 233:22 234:4,7 242:20 243:17,18 255:8,18 256:21 258:17 259:8,22 261:16 263:13,18 266:6 268:16 270:15 271:11 272:11 273:5,9 274:9,18 275:3,9 275:17 276:5,12 276:19 277:5 278:5 279:2 280:19,21 281:3 281:17 282:3,7,9 282:21 283:4,9,19 284:6 285:11 290:7,18 291:4,12 291:18 292:4,10 292:17 293:4,12 296:10 297:4 298:12 300:1,21 301:10,11,19 302:4,16 320:7 322:18 324:9,18 324:21 325:17 326:1,16,18 328:16 329:4,12 329:20 330:6,14 331:18 334:2,15 335:14,22 336:15 337:3,11,22 338:13,16 339:14 340:9 341:3,14 342:3 355:20 356:12 357:4 358:2,12 359:2,10

**communication's** 352:16 353:10

**Community** 142:21

**Community's** 104:22

**companies** 34:4

**compared** 221:13 226:9

**Compartmented** 10:13

**compel** 6:14 75:5 279:17 280:9

**compelled** 126:8 132:8 133:10 198:21

**complete** 16:20 139:6 293:19 297:2 298:10 299:21 300:12 361:16,19

**completely** 324:20

**compliance** 26:1,10 26:12,20 31:13 246:17 312:19

**component** 289:9

**compound** 151:14 151:17 342:3

**comprehend** 44:2

**comprehensive** 6:9 142:13 249:9 250:16 252:17 319:1

**compress** 270:7
**computer** 35:9,9 36:14,21,21 37:7 40:11,11 46:22 66:2,10,15 67:7 67:17 343:12
**computers** 39:16
**concedes** 160:2,5 185:16 187:17
**concept** 44:13 246:4
**concepts** 43:4 44:8
**concern** 35:4 41:8 42:2 215:17 240:17 241:6
**concerned** 102:20 156:8,9 215:15 236:21 238:15 239:3,22
**concerning** 16:5 24:3,7 171:12 172:7
**concerns** 17:4
**concluded** 360:4
**conclusion** 65:10 76:7 118:2,10 173:11 286:21 307:11 308:20 321:6,19 322:3
**conduct** 11:15 27:19 28:16 29:8 37:14 121:17 122:20 123:7 165:6,16 167:2 175:4 180:2,16 181:2,10 186:12 272:7 280:17
**conducted** 26:15 99:10 120:1 145:6 145:16 146:12,20 147:6,14 148:1 181:19 182:12,18 183:4 184:7,14 185:1,8 187:19 228:11 234:18 244:20 246:22 264:21 319:5
**conducting** 26:22 100:6 107:21 250:21 321:15
**conducts** 182:6 183:11 185:21
**confer** 10:12 215:10 216:17 229:11 260:2
**conference** 97:16 240:6
**conferring** 53:1 72:13 76:22 102:10 113:2 124:9 132:13 133:15 138:9 170:7 171:16 175:14 177:3 180:6 186:21 193:6 202:13 223:10 228:15 235:11 238:12 244:14 251:11 254:9 256:1 261:21 266:21 270:20 277:7 285:14 294:1 296:15 297:6 298:14 301:3 302:20 303:8 307:15 309:21 313:12 315:3,13 317:2 319:11 326:21 331:9 334:19 347:21 349:9 352:19 356:1 357:7
**confident** 71:3
**configuration** 282:5 283:3
**configured** 283:7
**confined** 88:4
**confirm** 76:19 77:4 80:18 128:17 132:7 133:10 134:11 178:8 187:17 188:14 193:14,20 240:20 304:13
**confirming** 236:19
**confusion** 177:9
**Congress** 308:7 309:13 315:10,22 321:14,22
**congressional** 316:10
**connect** 81:7
**connected** 66:10
**connecting** 48:15 54:14 80:17
**connection** 271:14 282:6 283:3
**connects** 78:5,22 79:6,16 80:1
**consider** 42:16 51:17 52:17 82:16 82:18 83:5,6 179:19 229:9 230:8 308:15 315:18
**considerable** 320:2
**consideration** 314:16
**considerations** 32:2 314:15
**considered** 67:16 80:7 104:22 178:19 179:10 314:11
**considering** 247:7
**considers** 16:13 50:21 108:11 314:9
**consistent** 154:6 355:11 356:13,22
**consolidate** 294:8
**constitute** 10:18 16:20 62:8 67:6 91:10 223:19 247:6 254:5,21
**constitutes** 80:17
**constraints** 319:2
**construed** 10:18
**consult** 37:13 76:4 261:20
**consulted** 247:16
**contain** 205:15 266:18 285:11 322:10
**contained** 219:14 230:13,19 234:21 264:10 269:5
**containing** 160:7 188:18 195:8 196:2 197:17 199:6 200:17 344:8
**contains** 231:4,19 239:8 269:22
**contemplates** 118:6
**contend** 277:3
**contending** 278:21
**contends** 278:3 279:1
**content** 261:9 263:4 289:13 304:5
**contents** 242:20 243:9 244:3 258:17 259:7,21 300:21 301:10 302:4,16 303:6 304:14 305:10,14 351:13
**context** 86:2 157:20,20 183:17 195:13 218:17 221:16,20 222:15 224:1,19 226:3 235:21 236:3 239:15 240:2 255:7,17 274:4 288:1 319:13
**Continued** 4:1 6:1 7:1
**continues** 101:17
**contributed** 235:8
**contributing** 288:7
**contributors** 288:14
**conversant** 42:17
**conversation** 39:4 85:18 94:8 101:9 101:13 105:6 176:17 228:4 344:17
**conversations** 351:14,16
**conveyed** 136:19
**Cook** 3:11 5:6 8:10 110:16 232:5 328:8,9 329:2,10 329:18 330:4,12 330:20 331:5,14 332:6 333:1,10,18 334:7,14 335:13 335:21 336:7,14 337:1,10,20 338:7 339:13 340:2,8,18 341:2,9,19 342:8 342:13,16 343:5 343:14 344:7 345:2,9 346:2,10 347:2,12 348:5,11 348:15 349:4,19 350:6 351:2,9,12 352:5,8
**Cooley** 3:12 8:10
**copied** 11:10 340:10
**copies** 279:18
**copy** 248:2 251:18 275:3,9 301:9,17 329:11,19 344:2,9 345:4,16 346:5,12 347:5
**corner** 14:7
**correct** 14:12 18:13 18:14 19:19,20 21:7 38:13 39:11 43:12,13,15 70:3 73:10 85:13 89:20 94:17 97:9 98:9 98:10 99:20 100:1 100:9 103:2 112:17,18 113:10 136:3 140:14,15 154:9 158:6,7 166:18 173:6

189:5 199:19,20 200:1 208:22 217:20 253:19 256:13 257:20 265:9 289:2 305:5 322:1,12,14 328:2 347:15 348:14 355:21 356:19 357:5 358:13 361:16,18
**correcting** 192:13 192:16
**correctly** 76:17
**counsel** 2:3 7:7 9:1 9:6,9,21 10:4,10 11:7,12,18 12:10 13:1,19,22 15:3 17:14 21:16 30:10 53:1 72:13 76:4 76:22 102:10 113:2 118:6 124:6 124:9,15 132:13 133:15 138:9 170:7 171:16 175:14 177:3 180:6 186:21 187:1 193:6 202:13 211:15 214:6 223:10 228:15 235:11 238:12 244:14 251:11 254:9 256:1 258:4,12 260:4 261:21 266:21 270:20 274:2 277:7 285:14 294:1 296:15 297:6 298:5,14 301:3 302:20 303:8 307:15 309:21 313:12 315:3,13 317:2 319:11 326:21 328:7 331:9 334:19 343:9 347:21 349:9 352:19 356:1 357:7 362:11,15
**counsel's** 203:11 304:10 327:11,19
**counterterrorism** 27:1
**countries** 157:8,17 162:6
**country** 162:18 163:5
**couple** 169:12 287:11
**course** 101:22 258:15 259:6,20 261:15 266:16 270:14 272:10 274:8,16 275:2,8 275:14 276:2,10 276:17 328:16 329:4,12,20 334:16 335:15 336:1,16 337:12 337:22 340:10 341:5 355:20 356:18 357:5 358:10
**court** 1:1 5:20 6:16 11:1,6,12,19 23:22 27:19 28:10 29:9,12 46:8 160:20 162:16 163:15 165:5,13 165:15 166:1,11 166:17 167:2,11 167:20 168:14 169:14 170:4 171:12 172:7,10 174:4,20 220:11 220:12 279:14 312:5,10,22 319:8 319:14 320:10,17 320:21 321:2,3,4 361:1
**Court's** 6:7 173:8 220:10
**covered** 120:21 232:18
**co-op** 34:17
**create** 345:4 346:11
**created** 82:2
**creating** 288:14
**creation** 345:16 346:4
**CSR** 2:8 362:19
**CT** 142:21
**current** 22:20 24:14 31:5,11 117:5 319:2
**currently** 250:21 284:22
**cyber** 251:5
**cybersecurity** 6:10 249:9 250:17 252:17

**D**

**D** 8:1
**data** 34:6 46:19 47:19 48:2,13,17 49:4 50:2,21 52:18 55:4,16,20 56:5,6,14 57:1,7 57:10,12 58:1 59:3,4,9,22 60:11 60:18 61:9,10 62:8,15 67:21 68:14,20 69:3,21 73:3 80:16 93:3 261:16 263:12,17 263:22 266:6 301:18 306:3
**databases** 206:4
**date** 108:1 128:3 193:21 251:12 361:22 363:4
**dated** 130:6 233:14 252:10 280:9 312:10 318:6 320:16 343:13 355:1
**Dawn** 1:21 2:8 110:18 153:11 251:19 328:13 348:11 362:2,19
**day** 328:10,14 363:19
**days** 322:6
**De** 211:2,10,13,18 212:2,18 214:7 215:5 217:2,21 218:15
**deal** 36:12 41:6 234:2
**decide** 27:9 92:21 173:16 280:20
**decided** 319:4 320:4
**decides** 286:1 314:12
**decipher** 280:19 281:17 282:3,9
**decision** 226:3
**decisions** 27:8
**declassification** 175:5
**declassified** 105:14 142:2,4,8 177:10 177:14,21 227:4 232:13 284:22 339:6
**declined** 214:22 289:10
**deem** 283:19
**deemed** 282:21 342:2
**deems** 9:22 10:7
**deep** 244:12,21 245:10 247:10 348:16 349:2,7
**Defendant** 30:2
**defendants** 1:8 4:2 5:11 6:14 9:4,18 19:15 45:3 361:7
**Defendant's** 279:17 280:8
**define** 88:11 89:8 93:5,7 255:13
**defined** 78:6
**defines** 57:20
**definitely** 209:12
**definition** 47:8 49:17,22 54:11,19 56:1 61:7 64:6,11 64:12,18,21 65:22 66:1 68:1,16,21 69:4,22 70:1 73:5 78:16 81:12 82:11 83:2 85:19 87:17 89:10 153:22 154:2 155:11 157:6 225:20 239:9 256:11,15 257:5,6,19 271:10 271:19
**definitions** 63:18 161:18 191:2,7
**deliberately** 275:15 276:3,11,18 277:4 278:4
**deliberations** 103:12
**deliberative** 96:2,5 96:9 102:20 103:14,17
**delving** 104:8
**deny** 76:19 77:4 128:17 134:11 193:14
**denying** 236:19
**Department** 2:5 4:5 8:21 26:16 31:13 32:1,18 33:5,22 34:3,5 36:10,19 37:12,22 103:4,20 166:22 167:19,21 168:7 168:17 170:10,12 172:19 176:21 220:19 222:10 246:15 247:16 248:7 249:5 252:9
**depend** 92:5,7,8,9 93:5,10 353:4,5
**depending** 27:11 52:8 92:2,15 228:20
**depends** 92:1

**depicting** 240:16
**deployment** 343:10
**DEPONENT** 361:9
**deposed** 12:20 18:13
**deposition** 1:12 2:1 5:9,10 6:3 7:3 9:20 10:11,22 11:4,5,10 12:13 13:3 14:4,9 19:1 19:14 20:20 23:5 44:16 63:11 65:1 65:6 69:9,11 85:16 95:7 104:6 120:12 129:15 159:8 210:2 220:1 250:1 251:20 273:2 279:11 312:1 317:21 318:12 331:3 342:6 351:20,22 354:15 360:4 361:12 362:4,10 362:13 363:1
**describe** 35:8 36:17 40:9 49:11 54:13 108:14 117:18 118:16 137:10 140:13 143:3,9 202:7,17 269:3,20 293:18 296:9 297:1 298:9 299:20 300:11 318:17 320:20 337:9 354:19
**described** 13:1 47:16 86:13 96:17 99:13 138:7,17,21 140:9 145:11 155:15 161:21 162:4 192:10,11 196:17 197:6 199:11 200:11,14 201:2 240:8 244:9 244:19 251:2 253:9 257:4 309:19 310:19 313:18 314:20
**describes** 109:17 109:18 117:5 139:13 272:1
**describing** 119:2 119:13,16 139:21 141:18 199:15
**description** 47:14 98:15 101:17 102:18 106:5 107:2,4 109:11,20 110:3 111:12,16 111:19,22 124:3 130:21 131:10 137:18 140:3 141:11 142:13 143:11 144:7 145:5 198:16 200:3 246:12 272:5
**descriptions** 110:2 143:7 157:10 191:9 311:7
**designated** 18:19 58:17 77:15
**designed** 196:9 199:14 204:18,21 205:3,9,12
**designee** 19:18 65:18 69:13 84:1
**destination** 90:2,12 91:11 94:16 254:6 283:5,9
**detail** 44:2 293:19 297:2 298:10 299:21 300:11 324:19 326:1,17
**detailed** 19:12
**details** 40:16 104:8 126:13 145:21
**detection** 248:8 343:11
**determine** 110:11 202:8,9,18 239:5 239:17 264:9
**determined** 266:17 269:4
**determines** 269:21
**determining** 351:16
**developed** 251:3,8
**developing** 31:19
**device** 11:4 195:7 196:1,9,16 197:5 197:16 200:11,13
**devices** 204:16 282:6
**Devon** 3:11 8:10 328:9
**De's** 236:2
**dhanleycook@co...** 3:16
**DHS** 37:4 38:9,12 38:16 39:5,10 248:14 250:21 343:3
**differ** 17:8,11
**difference** 83:2 119:13 159:1 213:2,9 261:19
**differences** 107:14 158:16,17 213:11
**different** 20:5,11 22:22 36:11 38:1 50:12 65:21 73:21 86:22 88:17 91:10 91:12,19,20 92:3 92:17 93:18,20 94:6,6,9,15,16 96:12 112:1 119:16 138:22 142:2 144:20 162:3 174:19 179:6 199:10,15 214:15 225:9 226:1,1 236:5 257:10 259:14 274:6 284:7 287:12 318:10 353:17
**differentiating** 54:17
**differently** 132:18 143:4
**difficult** 18:6 41:9 41:17 139:22 238:15
**difficulties** 319:3
**direct** 10:5 131:18 190:1 195:15
**direction** 116:10 123:17 124:3 129:8 146:3 182:2
**directions** 146:16 302:12 327:11
**Directive** 271:19
**directly** 25:2
**Director** 5:16 24:16 25:2,4 30:3 31:12 45:4 130:3 163:18,19 235:6 236:12 239:13 240:5,7 242:2 246:16
**Directorate** 252:8
**disagreed** 172:19
**disagreement** 178:6
**disagreements** 178:12
**disavowed** 314:22
**discard** 300:22
**disclose** 16:12 71:17 72:9 117:16 123:21 175:9 226:11 256:8
**disclosed** 14:20 20:13 131:13 136:1 175:22 226:20 312:18,21 339:3
**discloses** 124:13
**disclosing** 16:2,9 42:5 76:5 164:4
**disclosure** 10:2,8 10:15 15:7 141:1
**discovery** 6:14 269:19 279:17 280:9
**discrete** 223:15
**discriminates** 271:22
**discuss** 22:16 30:7 30:9 39:4 139:20 207:15 271:7 338:15 351:21
**discussed** 20:22 22:14 33:19 64:10 86:1 119:5 120:2 120:10
**discussing** 50:3 124:12 187:16 203:19 325:13
**discussion** 228:6 235:20 312:16
**displayed** 11:1,3
**disposal** 171:7
**dispositive** 126:4
**dispute** 176:21
**disregard** 280:21 281:2
**disrupt** 345:12 346:13
**distinct** 56:2 225:4
**distinction** 48:8 214:6 263:1
**distinctions** 93:2
**District** 1:1,2 2:9 361:1,1 362:3,20
**divide** 86:22
**Division** 2:6 4:6 170:11,12 220:19
**DNI** 321:9
**document** 14:17 19:6 32:22 45:9 45:15,19 58:21 68:10 95:12 96:22 97:2 98:22 99:11 99:14,21 100:3 108:10 111:11 129:20,22 130:2,3 130:8 132:3 143:16 145:10 155:9 159:13,18 176:3,19 177:10 178:6,11 191:20 198:3 210:8,10 212:1 220:6,15

224:2,12,19 235:13 236:19 237:17,18 238:19 239:7,13 240:15 249:20 250:6,7,13 251:13 252:6 272:1 279:10,20 280:3,4,6,15 312:7 317:20 318:4,5,10,16 332:8,10 333:4,7 342:10,18,21 343:22 344:16 345:3,5 354:14,19 355:16
**documentation** 96:18 97:6,21
**documents** 14:22 20:4,5,19 21:3,6 21:10,14 23:17 99:1 176:7,13 226:20 227:3,10 338:8,9,10,11 346:20 355:5
**doing** 12:1 33:2 105:9 107:9,16 137:22 141:10 196:8 221:4 310:16
**DOJ** 9:4
**domestic** 160:5 188:16,17 196:7 199:4 200:5 201:19 202:10,20 204:2,19 205:4,16 325:17
**dot** 281:17,17,17 281:19,19,20
**double** 171:19
**doubt** 104:7
**draft** 46:5,6 129:22
**drafted** 136:1
**drafting** 45:20 95:20 96:13 97:8 246:18 252:12
**drafts** 167:9,18
**drawing** 214:6
**drawn** 351:18
**drive** 11:8
**drugs** 18:5
**duly** 12:8 362:6
**duty** 241:6,7
**D-E** 211:3
**D.C** 1:14 2:8 4:9

**E**

**E** 8:1,1 363:2
**earlier** 128:13 138:20 162:5 219:5 257:9
**easier** 41:20 53:7
**effort** 221:21
**Einstein** 6:11 246:22 247:1,10 248:1,6,9 249:1,8 249:17 251:1,7,17 252:9 260:7 343:11,17 344:1 344:14,14 345:11 345:15 346:4,11
**either** 26:16 101:1 201:1 238:21 295:4 327:5
**electronic** 11:4 126:7 132:9 133:12
**eliminate** 199:4 200:5 201:19 204:11,18 205:12
**eliminated** 204:3 266:19 267:21
**eliminating** 205:3
**else's** 11:3
**elucidate** 228:4
**email** 3:9,16 4:12 97:16 243:9,18 268:16
**emailing** 218:12
**employ** 192:6 194:9
**employed** 362:12 362:15
**employee** 21:20,21 34:18 362:14
**employees** 25:12 43:19,22 210:16 210:20
**encompass** 50:2 286:6 288:5
**encompasses** 225:13
**encrypted** 280:19 291:18 292:3 293:3,12 352:15 353:9,21
**encryption** 353:4
**ends** 108:22
**engineering** 35:9 36:21 40:12
**ensure** 28:5 32:15 32:19 37:6 38:5 63:19 97:2 105:1 105:10 106:8,10 136:6,18 141:1 191:13 192:7 194:10 196:8
**ensuring** 31:21 99:3
**entire** 42:1 97:1 99:21 100:3 111:11 210:1 305:10,14 306:22
**entirely** 319:21 325:11
**entirety** 343:3,4
**entity** 280:17
**equipment** 280:21 281:2 283:3,8
**erode** 32:16
**errata** 361:18 363:1
**error** 311:9 313:9
**Esq** 3:3,11,19,20 4:3,4,16,17,20
**essence** 50:12 98:14
**essentially** 157:17 227:15
**establish** 75:1
**establishment** 104:1
**et** 1:7 361:6 363:4
**EU** 34:7
**European** 34:3
**evaluation** 320:3
**event** 277:22
**everybody** 105:10 328:14
**everyday** 257:16
**evidently** 239:22
**ex** 170:9
**exact** 97:14
**exactly** 22:12 23:2 130:7 142:1 171:2 188:21 189:4 193:11,14 195:12 209:18 235:17 270:9 344:21
**examination** 2:3 5:4,5,6 12:10 19:9 258:4 328:7 352:13
**examined** 12:9 361:11
**examining** 246:7
**example** 15:19 47:3 47:21,22 49:1 56:16 59:16,17,17 60:9 61:5,18 62:13 66:14,21,22 80:6,9,10 81:14 81:14 82:10 191:19 192:4,21 193:18 194:7 200:7,8 231:8 240:9
**examples** 49:3,9 50:13 61:6 80:22 91:2,4 191:17 193:12 233:1
**exception** 91:6 340:21 351:15
**exceptions** 354:12
**exchange** 218:18
**exchanges** 97:17
**exclude** 282:7
**excuse** 124:6 167:13 244:11
**executive** 142:20 176:4,13 179:12 343:13
**exercise** 250:22 251:1
**exhaustive** 143:10 144:8,12,14
**exhibit** 5:9,10,11 5:13,16,19 6:3,4,7 6:9,11,13,15,18 6:20 7:3,4,5,7,9 19:1,5,19 44:16 44:20,21 45:7,15 58:15 77:13,13,19 95:6,7,11,14,21 96:14 97:8,12 98:8,17 99:19 102:4 105:21 106:17 108:18,22 109:10 110:6 112:9 113:8 115:10 119:22 124:13 126:21 129:14,15,19 131:3,17 135:4 137:8 138:5,15 139:12 140:19,20 140:22 141:1 143:10 145:3 159:7,8,12,16,22 163:15 174:2 175:5,22 176:10 177:1,19 185:14 187:15 188:1 189:19 190:14,16 190:20 192:4 193:22 194:6 195:16 197:7 198:18 199:18 200:12,16 201:4 203:17 204:3 209:8,14 210:2,8 211:9 212:19 214:8 217:3 220:1 220:5 221:6,7 224:20 226:8,15 233:7 250:1,5

251:20 252:3,22 252:22 273:3 279:10,11,15 280:13 281:14 282:19 312:1,4 313:18 317:20,21 318:3,11,12 320:2 320:13 331:6,7,12 331:15 332:7,9 333:3,19 342:6,9 343:16 344:1 354:15
**Exhibits** 331:3 334:8
**existed** 35:7
**existence** 248:17
**existing** 325:14
**expect** 56:10 66:7 78:13
**experience** 36:8,12 37:10 38:1
**experienced** 240:10
**expert** 20:22 21:6 21:20 22:2,3 46:22 47:1 48:6 48:21 49:7,18 50:5 51:5 53:3 54:12 55:9,18,21 56:10,13,18 58:6 59:13 61:1,15 62:11 64:12 66:5 66:8,19 67:10 68:4,19 69:7 76:11 78:9,12 79:10,19 81:10 82:4,15,22 83:3 83:12 84:20 86:3 86:11 87:8 88:4,7 89:3 90:4,21 91:16 94:1 96:16 154:13 156:3 157:4 158:10 161:19 169:15 225:17 243:4 245:14 255:11 257:2 337:5 352:22
**expertise** 38:2,8 178:22
**experts** 37:21 52:17 55:1,3 59:11 60:7 63:5 64:1 73:22 85:15 87:17
**expires** 362:21
**explain** 17:10 32:10 39:13 44:13 119:12 238:22 309:1 324:19 325:22 326:17
**explained** 44:3
**explaining** 44:8 101:1 218:16,21 222:9
**explanation** 218:14 228:7
**explanations** 167:8 168:5
**explosive** 218:20
**explosives** 218:12
**expound** 346:20
**extensive** 42:11 106:13
**extensively** 37:4 106:10 120:13 121:16
**extent** 21:4 26:20 40:15,20 42:13 50:9 54:9,14 55:8 60:5,8,22 61:15 62:10,12 63:13,15 65:9 66:4,18,20 67:10 68:4,18 69:7,8,10 70:11 70:13,22 71:6,7 73:10,19 74:9,14 78:8,17 79:9,18 80:8 81:8 82:3,20 82:22 83:1 87:7 88:14 89:3 90:4 90:21 92:19 93:22 96:1 99:1,12 107:11,18 111:3,5 111:8 117:4 121:21 122:3 123:2,3,11 127:18 127:22 128:19,19 131:13 132:21 134:3,6 137:15,20 139:2 140:7,16 141:5 142:17,18 144:12,15 155:1 156:2,3 157:4 158:9 164:1,10,11 166:10 169:10 170:21 174:6,9,17 174:21 193:9,11 194:18 198:19 199:12 204:5 205:17,19 217:7 217:10 222:17 223:22 227:5,22 230:6 232:18,20 243:2,3 253:4 260:21 261:2 262:15,18 264:11 264:13 265:22 267:10,12 268:11 269:7 272:17,21 273:11 277:20 278:16,19 285:18 288:17 289:21 294:3 296:1 297:14 298:22 299:3 303:18,21 304:18,20 307:17 308:3 309:2,7 310:10,14 311:2,5 311:13,16 313:21 314:8 317:5 325:4 325:7,16 327:21 333:6 344:12 348:20 349:11 353:1,15 357:12
**extenuating** 322:8
**external** 37:21 38:2
**extracted** 355:11 356:11
**extracts** 355:19 356:17
**e-commerce** 34:1
**E-Government** 32:13
**e-mail** 206:13
**E-X-H-I-B-I-T-S** 5:8 6:2 7:2
**E3A** 6:12 252:10

**F**

**F** 45:4
**FAA** 308:4 322:5
**fabulous** 210:6
**FACA** 38:3
**face** 57:18 212:10 212:18 236:1
**Facility** 10:13
**fact** 44:14 96:21 98:11 112:14 124:17 125:9 126:3 134:13,21 145:11 166:6 170:15 173:2,14 173:15 178:2 187:18 188:15,16 192:13,18 219:1 227:19 234:3 238:7 242:19 243:8 244:2 264:21 317:7
**facts** 104:10 107:5 108:14 124:13,13 141:6 174:21,22 259:14
**factual** 96:22 98:8 98:17 99:8 100:11 105:22 106:16 136:7 138:5,14 139:11 140:22 145:4 172:20 173:6 179:16 277:3 278:3
**factually** 109:3 137:7 241:3
**fair** 141:16 142:11 143:9,20,22
**faith** 9:22 10:7
**fall** 200:2
**familiar** 21:13 24:6 24:9 28:17 165:3 242:19 245:10,22 248:5,14 252:14 255:6 256:10 312:6 318:16,18 354:20 355:4
**familiarity** 36:5
**fantastic** 171:3
**far** 32:6 33:19 186:5 239:20
**fast** 91:7 92:2 130:16 324:4
**federal** 2:6 4:7 31:8 32:18 33:8,18,20 34:4 35:2 38:3 46:8 65:5 345:12 346:13 359:22
**feel** 94:7 187:5
**felt** 43:6 44:2,6
**fiber** 56:16 79:22 80:8 81:6,18,21 151:10 152:1,8
**fiberoptic** 59:8 60:2,11,20 61:9 61:13,22 62:7
**fibers** 60:1 93:19 148:19,22 149:11 149:18 150:3,11 150:18 151:3
**figure** 75:14 214:2 221:12,13 226:8
**figures** 222:11
**filed** 23:18,22 46:8 167:10 338:11 339:4,5 355:16
**Filing** 6:7 7:9 354:21
**filter** 191:13 192:6 192:9 193:3,21 194:10 196:6 200:2,6,8,9 202:10,20 275:16 276:3,12,18 277:21 290:7,18 291:4,11,18 292:3 292:10,16 293:3 293:11

**filtered** 199:4 200:4 267:15 325:17
**filtering** 190:22 191:12,16,19 192:10,21 193:2 193:13,16 195:5 195:21 196:17 197:5,14 198:2 199:9 201:2,14 244:8,18 278:20 279:1 298:12 299:9 325:15 341:4
**filters** 277:4 278:4
**final** 127:1
**Finally** 11:14
**financially** 362:16
**find** 74:10 110:10 112:22
**fine** 43:2 74:22 171:18 187:12 246:12 252:15 303:1
**Fingerprints** 7:5
**finish** 201:17 304:17
**first** 3:4 8:4 12:8 16:8 29:21 30:4 37:2 47:9 48:12 67:2 69:6 77:20 108:19 131:18 137:19,22 143:19 189:22 199:3 200:4 212:3,4 229:19 237:4 243:16 273:3 281:15 287:15 300:20 309:18 310:7 312:15 318:22 333:22 343:19
**FISA** 28:17,18
**FISC** 7:9 20:10,11 20:12,19 142:2 171:5,6,6,7,8 172:15 175:11 176:3,6,15,22 178:18 179:9,11 179:15 219:11 222:11 295:8,10 308:6 309:12 310:15,19 313:9 315:22 316:20 317:13 321:4,11 321:11,12 322:7 339:5 354:22 355:16
**FISC's** 176:11,18 221:21 222:5
**fits** 353:7
**five** 10:22 253:7 352:9
**five-minute** 62:18 110:17 257:21
**fix** 102:3 105:22
**fixed** 106:1
**flash** 11:8
**Floor** 3:13
**flow** 255:6,7,16,17 256:11,13,15 257:14,14,15
**focus** 259:4
**focused** 217:22
**focusing** 112:8
**folder** 210:1
**follow** 51:11 72:3,4 77:8,10 116:7,9 123:16 126:17 129:7 146:2 162:11 180:14,21 181:7,15 182:1,9 182:15 183:1,8,15 184:3,11,18 185:4 185:11 195:2 197:1 201:9 202:4 203:11 207:3,11 208:10 219:19 224:7 234:14 235:2 242:16 245:7 255:3 256:4 259:1,5,12,17 266:12 268:22 270:11 274:1,21 275:6,12,20 276:8 276:15,22 281:10 282:15 283:16 284:2 285:7 290:3 290:13,22 291:8 291:15,21 292:7 292:13,20 293:7 293:15 300:17 301:6,14,22 302:11 305:20 306:7 307:4 323:2 323:21 324:14 326:7 327:11 328:22 329:8,16 330:2,10,18 332:4 332:20 333:16 334:5,12 335:11 335:19 336:5,12 336:20 337:18 338:5 339:11,22 340:6,16 341:17 347:10 350:22 351:7
**followed** 254:18
**following** 9:19 124:2 146:15 147:1,9,18 148:4 148:11,17 149:16 150:1,8,15,22 151:7 152:5,13,20 153:5 162:21 163:8 304:10 317:10 340:22
**follows** 12:9
**follow-up** 218:9 289:12
**footnoted** 142:7
**force** 34:1
**forced** 237:11,15
**foregoing** 362:3,5
**foreign** 5:15,18,20 6:6,16,18 24:3 27:18 28:9,18 29:9,11 95:17 130:5 160:9,19 162:16,17 163:5 163:14 165:5,13 165:22 166:16 167:1,10,20 168:13 170:3 171:12 172:6,9 173:7 174:3 191:14 210:14 220:11 228:12 229:22 230:1 233:11,12,21 234:7 283:20 285:12 286:5 287:16 288:5,14 312:9 318:7 320:5 320:7
**foreigner** 230:11 230:15 231:2,16 232:1 234:19
**foreign-intelligen...** 283:1
**forgive** 144:20
**form** 21:11 22:8 35:13 41:2 42:19 43:7,14 44:4 46:1 48:5 50:4 53:2 56:18 58:5 61:14 64:8 67:9 68:3 70:21 79:8 82:22 86:10 90:3,20 91:13 98:19 106:2 106:18 109:4 113:22 118:1 124:22 141:3,20 165:7 193:7 212:7 220:17 222:16 226:22 228:16 239:15 242:5 296:12 302:6
**formal** 35:21 36:13 37:10
**forms** 221:22 222:6 244:12,20
**forth** 19:19 140:1 177:9 218:18 236:3 262:11 341:15 355:13
**forward** 37:5 308:8 314:17 321:10 324:1
**found** 134:19
**foundation** 1:4 8:6 12:14 91:14 258:5 258:13 279:22 344:11 345:21 346:16 361:3 363:4
**four** 10:17 22:20 24:20 25:1 31:5 35:18 36:2,19 40:10 42:14,17 130:7 211:21 247:3
**Fourth** 198:8
**fragmentary** 197:12
**frame** 17:13,15 34:16 168:22 169:2 316:5 336:9
**framed** 52:12
**frames** 17:11
**Francisco** 3:14
**Freedom** 169:18,19 177:11,14
**frequency** 312:21
**frequent** 37:17
**front** 19:4 44:19 95:10 129:18 159:11 210:7 220:4 250:5
**full** 8:14 9:14 17:7 17:17 22:10 34:20 105:15 107:3 195:12 211:17 221:8
**fully** 16:9 17:20 19:10 27:13 38:5 44:13 59:21 88:7 88:11 110:12 186:4 202:22 269:3,20 325:22 326:18
**full-time** 34:18
**function** 103:20 287:22
**functions** 26:13

71:9 142:22
**further** 39:4,22 40:2 50:7 57:16 71:12 89:7 93:4 112:3 161:22 178:14 203:12 228:3,5,7 233:4 264:5 304:4,6 349:16 352:5,13 359:20 362:14
**furthered** 219:2
**future** 315:1,11 316:6,22 317:15

**G**

**G** 8:1
**game** 227:13
**general** 9:1,6,9 22:6 47:13 74:5 96:6 107:1,13 108:11 140:3 153:21 154:2,6 162:4 169:1,5 176:18 187:5 211:15 245:15 256:20 257:4 272:5 312:18 321:9 348:19 349:1 353:3
**generally** 21:13 33:12 49:17 53:11 54:10 55:10 63:8 86:1 90:14 94:18 102:7 105:22 106:1 120:10 139:1,18 161:19 223:14 224:11,18 230:20 243:17 248:6 249:3 353:16 354:4,10 358:3
**generic** 227:16
**getting** 38:8 56:4 107:10 121:14 177:5 211:11 309:12 310:18 345:20
**Gilligan** 4:4,11 9:3 9:3 53:18 103:19 104:10 124:6 151:18 230:21 231:5,10 237:7 241:13 253:12 260:8 273:15,19 312:12 319:15 323:4,7 331:1
**give** 12:13 13:7 42:8 49:3 71:13 74:13 76:14 172:1 172:21 192:4 204:9 211:12 215:11 223:1 228:6 229:8 239:21 247:18 248:15 271:10 273:1 285:2 288:11 299:21 300:11 308:7 319:22 327:7
**given** 14:11 18:15 36:12 48:18 68:1 68:16 69:5 80:9 117:4 171:4 186:6 203:7 241:4 264:16 268:3 324:18 326:16 361:16,19 362:11
**gives** 101:16 229:5
**gleaned** 251:4
**go** 13:2,20 27:10 30:15 39:3,22 40:1 50:7 53:19 56:8 57:16 68:6 72:22 73:14,18 74:19 75:16,18 108:5,7 110:18 112:2 120:19 125:18 128:6 138:10 145:8 151:16 153:11 156:18 158:2 161:17 170:18 172:15 185:13 187:8 189:2,19 190:9 198:9 207:14 213:4 216:13,17 217:16 217:17 228:5 229:11 232:5 233:4 241:16 247:21 260:8,10 262:6 264:5 267:3 267:5 270:21 271:7 272:13 277:8 284:11 286:13 287:5 297:7 298:15 303:9,11 304:4 309:22 310:3 314:4,13,17 323:7 323:12 327:7 328:3 338:18 342:11 344:18 348:3 350:12 352:10 358:1
**goal** 16:1
**goes** 24:12 26:2,7 218:15
**going** 15:11 51:11 55:14 72:3,4 77:3 84:22 89:2 92:16 92:21 102:18 103:11 104:14 110:11,14 116:7,9 117:22 118:17 120:17 127:16 138:21 140:4,18 144:17 155:1,7 156:10 157:5 198:17 222:22 223:11 227:5 229:10 232:16 235:19 258:7 260:16 280:14 281:14,22,22 282:18 308:6 310:16 315:18 318:21 324:1 328:12 347:13 355:8 359:22
**good** 8:2 9:22 10:7 13:19 96:7 153:7 173:6 191:2 218:9 351:10
**Gorski** 3:20 8:11
**gotcha** 227:14
**gotten** 137:21
**governing** 9:19
**government** 9:21 10:4,11 23:9,18 23:20 27:17 28:15 29:7 31:8 33:8,19 33:20 35:2 104:1 109:18 135:6,15 141:18 142:13 143:6 160:1,4 165:4 173:18,19 175:2 176:4,13 178:19 179:10 185:16,21 187:1 187:17,18 198:21 220:14 339:3 359:22
**government's** 6:7 7:9 109:20 165:15 165:21 166:11 176:10 220:9 354:22
**graduate** 36:3
**grammatically** 208:22
**great** 9:11 15:3 36:12 44:15 136:17
**greater** 312:21
**ground** 11:20
**grounds** 96:9
**group** 26:12
**groupings** 57:1
**groups** 257:10
**guess** 50:6 57:17 70:13 92:7 114:19 114:20 115:1 144:3 157:14 176:18 178:9 197:22 346:8
**guessing** 143:15
**guideline** 118:5
**guys** 216:17

**H**

**half** 31:5
**halfway** 160:2 250:20
**hand** 12:2
**handed** 279:14 312:5
**handful** 97:13
**Hanley** 3:11 5:6 8:10 110:16 232:5 328:8,9 329:2,10 329:18 330:4,12 330:20 331:5,14 332:6 333:1,10,18 334:7,14 335:13 335:21 336:7,14 337:1,10,20 338:7 339:13 340:2,8,18 341:2,9,19 342:8 342:13,16 343:5 343:14 344:7 345:2,9 346:2,10 347:2,12 348:5,11 348:15 349:4,19 350:6 351:2,9,12 352:5,8
**happening** 107:12 193:15
**happens** 28:8
**happy** 15:1 53:15 106:21 107:7 108:8 139:3 268:8
**Harbor** 34:2
**hard** 57:19 91:7 92:2 238:3
**harm** 117:20 118:13,16 119:2,3 119:17 121:11 163:11 164:5,15 164:20
**head** 13:10 91:2 156:11 251:16
**hear** 137:13 188:8 197:20 229:5 323:4 358:6

**heard** 12:22
**hearing** 6:4 210:12 210:17 212:19 214:7 215:6 217:2 316:16 338:9
**held** 33:20 240:6
**help** 14:8 27:9,9 43:9 141:11 212:13 228:3
**helpful** 14:18 29:4 53:17
**helping** 34:1
**helps** 342:2
**hereof** 362:8
**Hi** 328:9
**high** 49:4
**high-bandwidth** 52:18
**high-speed** 46:18 47:19 48:2,17 49:4 50:21 52:18 55:3 62:15
**historical** 141:7
**History** 98:15
**hitting** 39:2 140:2
**hold** 29:13 31:10 161:9 170:6 357:6
**holding** 33:7
**holds** 205:14
**Homeland** 31:13 32:1,13,18 33:5 36:10,19 37:13,22 246:15 247:17 248:7 249:5 252:9
**honestly** 247:12
**hope** 230:7
**hopefully** 54:3
**hours** 347:13
**HTTP** 7:4 219:12 225:13 334:1,15 335:14
**HTTPS** 225:13 280:19 281:2,17 282:3,7,9 290:7 290:18 335:22 352:16 353:10,22
**human** 311:9 313:9
**hypothetical** 94:1 288:15

I

**idea** 277:20 278:16
**identical** 158:15
**identification** 19:2 44:17 95:8 129:16 159:9 210:3 220:2 250:2 251:21 279:12 312:2 317:22 318:13 331:4 342:7 354:16
**identified** 45:8,16 105:20 175:20 295:13 296:8 313:10,18
**identifiers** 313:1
**identifies** 172:5
**identify** 25:6,7 29:21 167:21 168:4 173:9 175:10 196:10 198:22 199:21 304:1
**ignore** 283:4,8
**III** 173:17
**imagine** 173:5 178:5,9 [redacted] 4:17 9:8 9:9
**impact** 6:11 31:20 32:11,20 36:9 37:15 38:6 246:19 246:22 248:22 252:7 314:10 344:13
**impediment** 309:5
**implementation** 5:17 27:5 130:5 168:6 319:4
**implemented** 230:9 249:17 253:10 293:20 344:22
**implications** 37:6
**important** 13:6 101:4 112:14 131:2,12 204:15 204:20 217:13 263:21 281:19
**improper** 277:16
**inaccuracies** 102:2 102:3 106:16,16 108:2 138:5,15 139:1,11,11 145:4 145:10 168:4 174:1
**inaccuracy** 99:8,9 100:4,8,19 105:20 106:1 172:5,10
**inaccurate** 14:11 101:1 106:5 110:4 114:12 115:10,18 115:21 145:10 174:13 226:7
**incidences** 26:21
**incident** 26:11
**incidents** 26:1
**include** 46:18 59:20 60:1,20 61:12,20 66:15 169:7,14 191:12 192:18,19,19,20 193:2,4,17,20 195:6,22 197:15 320:6 321:4
**included** 47:3,16 59:18 60:9 66:21 104:5 115:8
**includes** 48:2 55:3 114:11
**including** 346:16
**incomplete** 14:11 101:8 111:13,21 112:14,16,19 113:8,18 114:2,8 114:9,11,14,15 115:1,3,16,20 132:22 133:2,3,7 137:17 138:4 139:20 141:13 144:16 265:4
**incompleteness** 138:14 145:2
**inconsistent** 125:12 125:20
**incorrect** 137:8
**independent** 103:22 142:19
**independently** 90:2 90:12,19
**INDEX** 6:1 7:1
**indicate** 265:16 331:16 333:20 346:3
**indicated** 289:8 311:8 312:20 315:9 316:20 317:13
**indicates** 345:20
**indicating** 33:13
**indication** 134:15 312:15
**individual** 21:22 22:7 61:12 148:19 148:21 149:11,18 221:4 285:22 322:18 324:10
**industry** 64:13 88:19 89:1,11 154:8 256:21
**information** 10:3,9 10:13,16 11:16,17 15:5,12,18 16:2,5 16:9,12,19,22 21:5 22:14,17 26:2,7 27:2 30:8 30:11 33:2 37:8,9 37:19,19 38:7 40:22 42:6 50:8 50:10,11,15 51:7 51:7 54:1,8,16 63:14 70:13,18 71:1,17,18,20,21 72:10 74:4,13,15 74:20 76:6,18 77:2 81:13 97:19 99:3 101:2,8 105:14 107:1,15 111:6,6,14 112:20 113:11,19 114:3 114:10,11,16,21 114:22 115:4,8 116:2,16 117:1,15 117:16 118:19,19 120:4,16,20 123:3 123:11 126:12 127:19,19 128:14 128:18 129:4 131:14 133:3 134:5,21 135:6,15 137:16 138:4 139:5,17 141:17 144:13,13,16 145:12,20 156:4 161:2,2,22 162:8 165:12,20 166:6 166:12 168:15 170:4 171:4 174:7 174:8,12 175:10 175:21 178:14,19 179:10,19 180:10 191:15 193:10 194:19,20 196:20 201:6,6,22,22 202:22 203:12,13 203:15,21 204:6,6 205:18 206:22,22 208:1,1 209:20 217:8,9 219:16,16 223:22 226:12 228:3,18,18 233:5 233:11 235:18 236:1 238:16 239:8,21 240:18 241:5,8,9 242:13 242:13 245:4,5 249:21 251:4 253:5 254:14 256:8 258:20 260:5,21,22 262:16,16 264:15 264:18,21 265:2 265:13 266:1,9 267:10,11,18 268:12,19,20 269:8,9,15 270:2

270:2,18 272:7,18 272:19 273:1 274:11 281:5,6 282:12 283:13 285:4,12 286:6,6 287:17 288:5,6,15 289:7,10,13,17,22 289:22 290:10 294:3,4,10,13,15 294:16,19 295:3,4 295:5,12,14,20 296:2,4,7,22 297:14,18,22 298:2,3,8,22 299:1,9,14,19 300:4,4,10 302:8 303:18,19 305:17 305:17 309:9 310:11,12 311:2,3 311:14,15 313:22 314:1 322:21,21 323:18 325:4,5,21 326:4,4,14 327:1 327:1,3,11,14,16 327:18 328:19 335:8,8 337:15,16 339:6 340:13 346:21 347:7,7 349:12,17,18 350:1,1 351:17,19 356:14 357:12

**informed** 27:9

**ingested** 205:10 206:3 267:18

**ingests** 206:10

**initiative** 6:10 249:10 250:17 251:2 252:17

**inquiry** 218:10 221:21 222:5

**inside** 66:17

**inspection** 244:12 244:21 245:11 247:11 348:17 349:3,7

**Inspector** 312:18

**instance** 227:8

**instances** 105:13

**Institute** 3:4 8:4

**instruct** 51:9,15 71:22 77:5 116:4 118:20 123:14 126:15 129:5 146:1 161:5 162:9 180:12 194:22 196:22 198:1 201:8 207:2 208:3 219:18 224:5 234:12 238:17 242:15 245:6 254:16 258:22 259:16 266:2,11 268:21 270:4 272:20 273:14 274:13 281:8 282:14 283:15 285:5 290:1,12 300:5 302:10 304:7,21 305:18 323:1,20 326:6 327:8 328:21 332:2 333:15 335:10 337:17 339:8,21 340:15 341:15 347:8 349:12 350:2

**instructed** 117:1 265:15 289:14 332:18

**instructing** 188:9 240:21 241:12 294:9,11,17

**instruction** 51:12 72:5,6 77:9 116:8 117:20 124:1 146:14,22 147:2,8 147:17 148:3,4,10 148:11,16,17 149:15,16,22 150:1,7,8,14,15 150:21,22 151:6,7 152:4,5,11,12,13 152:19,20 153:4,5 162:20,21 163:7,8 164:8,22 180:20 180:21 181:6,8,14 181:15,22 182:8,9 182:14,22 183:1,7 183:8,14,15 184:2 184:4,10,11,17,19 185:3,4,10,11 186:15 197:1 202:2 203:11 205:8 207:10,12 208:9,11,17 213:7 219:20 224:8 235:1,3 255:2 256:3,5 263:15 264:4 265:13 274:20,22 275:11 275:19,21 276:6,8 276:14,15,21 278:7 284:1,2 287:10 288:10 289:1,4 290:14,21 291:1,7,8,14,15 291:20,22 292:6,7 292:12,13,19,21 293:6,8,14,16 295:17,22 298:4 299:16 300:16,18 301:5,7,13,15,21 302:1 304:11 306:8,17 307:3 317:17 324:13 327:20 329:7,9,15 329:17 330:1,3,9 330:11,17 332:12 332:13 334:4,11 335:18 336:4,6,11 336:13,19,21 337:19 338:4,6 340:1,5,21 341:22 342:4 351:6 353:14 354:3,8 357:21

**instructions** 147:10 147:19 162:12 182:16 201:10 202:5 207:4 209:5 234:15 242:17 245:8 254:17 255:4 259:2,11,18 266:13 269:1 270:12 274:2 275:5,6,12 277:1 281:11 282:16 283:17 285:8 290:4 305:21 306:6 307:5 317:10 323:3,22 324:15 326:8 329:1 330:19 332:5,21,22 333:17 334:6,13 334:21 335:12,20 339:12 340:7,17 341:1,18 347:11 349:17 350:21 351:1,8

**instructs** 13:22

**instruments** 81:13

**intelligence** 5:15,18 5:20 6:6,16,19 24:4 27:18 28:10 28:18 29:9,11 95:18 104:22 130:5 142:21 160:20 162:16 163:14,19 165:5 165:13,22 166:17 167:1,10,20 168:14 170:3 171:12 172:6,9 173:7 174:3 191:15 210:14 220:12 233:11,12 233:21 235:6 236:13 239:14 240:5,8 242:2 283:21 285:12 286:5 287:16 288:5,14 312:9 314:9,13 315:20 316:12 318:7 320:5,8 331:17 334:1

**intends** 317:14

**intention** 314:22

**intentionally** 290:6 290:17 291:3,11 291:17 292:3,9,16 293:2,11

**interacting** 42:14

**interception** 132:9 133:11

**interchangeable** 159:3

**interchangeably** 226:20 227:16,20

**interconnected** 66:2,15 67:7,17

**interest** 146:5 149:9 285:13 315:10 316:21 331:18 334:1 358:11 359:1,14

**interested** 7:4 106:5 358:17 362:16

**interests** 103:21 319:3

**interim** 232:12

**interlocutor** 26:18

**intern** 34:10

**international** 78:4 78:21 79:5,15 80:1 81:6,19,22 154:11,15,17 155:11 157:7 158:3 160:8,21 162:15 163:3,13 180:3,17 181:3,11 181:18 182:5,12 182:19 183:19 184:7,14,22 185:7 185:22 186:13,19 187:4,20 188:19 219:12 275:16 276:4 322:17 324:9,17 326:15

**internet** 36:11 46:18,20 47:3,10 47:13,17,20 48:1 48:4,14,15,18

49:5,14,22 50:14 51:1,2 52:20,21 54:9,21 55:5 61:7 62:14 63:3,10 64:2,7,18,22 66:16,22 67:6 68:1,16 69:5 73:5 78:10 79:7,17 80:7 89:22 90:1 90:10,11,18,19 91:9 111:19 121:18 122:7,8,16 122:21 123:8 124:21 125:16 145:15 146:11,19 147:5,13,22 148:20,22 149:12 149:19 150:4,11 150:18 151:3,10 152:1,8,16 153:1 153:17,20 154:11 154:17 155:12 157:7,7,11 158:3 158:3,4,16 160:8 160:21 162:15,17 163:3,3,13 180:3 180:17 181:4,12 181:18 182:5 185:22 186:13,19 187:4,20 188:19 191:13 192:6 193:3,21 194:9 195:7,8 196:1,2 196:10 197:16,17 199:1,2,3 200:4 201:14 204:2,17 206:19 222:15 223:15,19 225:1,3 225:5,15,21 226:21 227:17,17 233:22 234:4 242:20,22 243:11 243:17 244:4 253:22 254:1,2,4 254:5,20,21 255:8 255:15,17 257:5 257:11 258:18 259:9 260:1 261:9 261:17 263:4,6,7 263:8,13,18 264:9 266:7 267:15 269:5,22 280:18 282:4 283:2 291:4 291:11 300:12 302:22 303:6 304:1,2,14 305:2 305:11,14 306:4 306:11,22 313:1 313:11 320:6 341:8,21 347:18 348:18 355:11 356:11,18 358:2,9 358:13,18 359:10 359:14

**internship** 34:11

**interrogatories** 5:12 45:5 77:18 77:21 86:14 189:22 203:18 264:19

**interrogatory** 45:8 45:11,17,21 55:15 57:7,21 58:16 60:20 61:12 62:9 64:6 70:2 78:6 85:21 86:20 87:19 88:2,13 119:14 190:16 192:11 195:16 196:4,6,18 197:6 198:4 200:12 204:1 265:17 327:5

**interrupt** 28:21

**introduce** 8:17 258:9 311:20

**intrusion** 248:8,8 343:11

**intrusions** 251:5

**invocation** 41:2 119:5 120:4,11 121:10

**invoke** 103:18 163:20 359:22

**invoked** 96:3

**involve** 97:18 213:6 247:10 322:17 324:8 347:4

**involved** 23:5 24:2 25:17 27:4,20 32:3 33:3 96:13 125:15 129:1 236:15 246:21 349:6

**involvement** 28:2

**involves** 43:11 124:19 345:15 346:4

**in-boxes** 235:8 236:16 238:7 240:9 242:4,10

**IP** 191:20 192:18 200:2,6,8 283:5 283:10 354:1

**irrespective** 74:4

**issuance** 33:3 120:14

**issue** 74:8 215:16 215:16 218:7

**issued** 135:3 136:15 141:16 142:4,12,15 145:6 160:12 171:14 172:8

**issues** 25:4,9 176:6 310:18,22 311:9 311:10,12 313:9 343:9

**issuing** 33:11 120:21 130:18,20 131:2

**I-N-D-E-X** 5:1

**J**

**J** 1:12 2:2 4:4 5:3 9:16 12:6 361:10 363:5,17

**James** 4:4 9:3

**james.gilligan@...** 4:13

**January** 7:7 343:13 362:22

**Jaques** 1:21 2:8 11:22 13:6,8 95:5 110:22 129:13 133:22 156:22 159:6 209:7,22 260:17 279:9 284:16 286:16 323:13 362:2,19

**Jason** 4:16 8:22

**Jewel** 24:13

**Joan** 9:15

**job** 1:22 13:15 32:3 32:7 35:1,4 37:17 41:21 42:13 43:3 43:11 166:11

**jobs** 33:18,20

**John** 5:21 [redacted] 4:20 9:5 9:5

**joined** 8:8

**joining** 35:11 36:6 40:5

**judge** 5:21 6:17 142:6 155:16,18 159:19 160:12 161:21 173:17 174:14,18

**judgment** 172:18

**July** 5:13 95:18 107:22 109:12 128:3

**June** 145:18 146:20 147:14 148:8,21 149:20 150:12 151:4,12 152:10 152:17 175:1 181:12,19 182:19 183:5 184:13 185:1 186:8 190:22 193:1 201:13 205:16 208:7,15 209:3 216:6 228:11 229:20 230:9 233:14 234:5 244:12,20 259:4,7 259:21 261:14 262:19 263:11 264:8 265:8,10 266:15 269:4 270:15 272:10 273:8 275:15 276:11 290:16 291:10 292:2,15 293:10 324:7 326:10,15 329:19 330:13 335:14 336:8 337:21 347:3,16 349:6 351:3

**jury** 76:8

**Justice** 2:6 4:5 8:21 26:16 103:4,20 167:22 168:7,18 170:11,12 172:19 176:22 220:19 222:10

**Justice's** 167:1,19

**K**

**Kafka** 336:15 337:2

**KATHLEEN** 4:17

**keep** 28:22 177:5

**keeping** 101:11

**keeps** 289:20

**keimbri@nsa.gov** 4:19

**kept** 287:12

**key** 217:22 218:2 244:22

**kind** 270:9

**knew** 23:2 74:7 332:21

**Knight** 3:4 8:3

**knock** 34:12,13

**know** 13:14 14:5,13 32:6 33:1 36:2 41:20,21 45:18 63:7 69:16 70:5,6 70:7,8,10,15,16 70:17 73:6,8 74:8 85:1,3,4,8,10,11 87:11,14,15 89:14

89:16,18 97:10 104:3,4 106:9 107:13 110:14 116:11,16 121:5 132:1 139:17 140:6 142:22 161:19 169:5 170:9,22 171:4,10 172:13 173:14 176:6,20 177:13 177:20 178:4 203:10 211:13 213:10,14,17 214:12 220:14 221:16,19 224:19 227:2,9 236:4,6,7 236:16 237:3,5,8 237:12,14,17,21 238:1 239:11 241:3 251:15 256:13 257:11 278:2 279:2 287:19 288:16 307:22 315:20 316:2,9 328:13 337:2 343:3 344:21 345:15
**knowing** 203:3 239:6
**knowledge** 32:9 74:3 168:13 170:3 170:20 172:1,3 178:1 221:3 226:18 250:11 344:9 355:10
**known** 10:13 71:7 145:10 242:21 245:17 248:9
**knows** 41:22 65:6 73:3 237:8,9 247:17 315:6

**L**

**labeled** 190:5 211:2
**lack** 344:10 346:16
**lacked** 281:16 282:2
**lacks** 91:13 279:21 280:18 345:21
**language** 187:22 188:22 217:17
**laptop** 11:2,7,12
**large** 66:2,9,14 67:7,14 101:4 226:21 338:9
**largely** 120:20
**largest** 152:15,22
**late** 328:12
**law** 169:11,17
**lawful** 132:9 133:11
**lawsuit** 12:14 24:11 32:8 46:10
**lawyer** 171:3 265:14 299:16 317:11
**lawyer's** 51:11 72:4 77:8,10 116:7,9 117:19 123:17 124:3 126:18 129:8 146:3 289:1
**layer** 242:22 243:10 244:4 246:8 261:16 263:6,9,12,22 266:6 301:18 306:3,22 347:18 348:18
**Leadership** 25:5
**leads** 52:12
**learn** 42:12 43:4,6
**left** 217:1
**legal** 15:13 65:10 118:1,10 173:11 286:21 307:10 308:20 321:6,18 322:3 343:9
**let's** 40:8 95:4 198:9 207:14 259:4 260:10 271:18 286:13 303:11 307:22 310:3 323:12 328:3 330:21,22 331:6
**level** 26:10 137:3
**liberties** 5:13,17 8:9,11 20:8,9 24:17 25:3,7 26:19 28:7 95:15 101:7 109:21 120:14 130:4 131:7 192:3 209:13 210:12 219:3 258:14 299:10 314:10 325:14
**Library** 3:6
**light** 61:13,21 62:4 62:7 150:17 151:2
**limit** 355:13
**limited** 58:2
**line** 8:8 22:16 30:10 41:21,22 54:2 59:7,9 60:1,12,19 61:9,9,11 62:8 80:16 82:13 93:2 93:3 211:6 218:9 239:18 273:3 351:18 363:6
**lines** 22:13 46:19 47:20 48:3,13,18 49:4 50:2,22 52:19 54:1 55:4 55:16,19 56:5,14 57:8,10 58:2,3 59:3,5 62:16 67:22 68:15,21 69:4,21 73:4 140:2 211:1,7,20 211:21 218:16 271:21
**link** 153:17,21 154:11,17 155:12 157:7,8,17 158:3 158:4,4,16,22 160:8,21 162:5,15 162:17 163:3,14 186:19 187:4,20 188:19
**links** 180:4,18 181:4,12,18 182:5 185:22 186:13
**listed** 65:1
**listening** 149:6 261:18
**litigation** 21:9 23:6 24:3,6,9,13
**little** 24:20 33:17 33:17 49:11 57:16 141:17 156:13 320:1
**LLP** 3:12 8:10
**local** 118:5
**located** 191:15 192:7 194:11 233:10
**location** 261:12
**locator** 207:7
**logical** 56:22 57:18 157:6
**long** 24:18 31:15 33:15 34:11 84:5 161:14 328:14
**longer** 107:10,16 107:18 140:8,17 295:1 320:6
**look** 68:6 106:20,22 118:4 153:20 190:14 196:4 204:14 226:2 237:20 250:18 253:8 312:4 318:2 318:15 342:9 344:18 354:18
**looked** 141:8
**looking** 29:14,22 30:1,7,9 42:8 58:13,14 69:16,17 122:12 144:22 153:21 155:11 180:4 209:8 217:12 231:14 233:7,16 238:3 252:3
**looks** 236:1
**lost** 84:14
**lot** 101:9,12 104:9 104:12 262:10
**loud** 127:3
**love** 294:14
**low** 3:6 282:22 283:20
**lunch** 153:10,12,15

**M**

**M** 6:17
**main** 26:18
**major** 46:20 47:20 48:3,14,15,18 51:1 52:19 55:5 66:16 67:6
**making** 17:14 48:7 262:22
**man** 34:13
**managing** 251:4
**March** 6:4,13 210:15 215:6 217:3 280:9
**mark** 251:19 279:10 311:21 312:12 317:19 318:10 354:13
**marked** 19:2,5,6 44:17,20 95:8,11 95:20 97:12 98:8 98:17 99:19 102:4 105:21 106:17 108:18 126:21,22 129:16,19 131:17 143:10 145:3 159:9,12,16 195:17 210:3,7 220:2,5 221:11 250:2,4 251:21 252:3 279:12 312:2 317:22 318:13 331:4 342:7 354:16
**marking** 95:5 129:13 159:7 209:8 210:1
**Mary** 4:20 9:5
**MARYLAND** 1:2 361:1

**Massachusetts** 2:7 4:8
**matching** 22:22
**material** 23:16 97:3 99:4 107:11 144:17
**materials** 23:14 28:5 344:18
**matter** 20:22 21:6 21:20 22:3 63:22 64:12 85:14 87:16 88:4,7 97:11 107:1,13 108:11 176:18 277:4 278:4
**ma'am** 12:3
**mean** 18:4 25:16 39:13,16 47:6 49:12 51:21 55:20 55:22 61:5 66:3 70:15 73:20 78:13 88:17 92:12 95:4 158:14,15 160:20 173:16 178:10 191:5 192:8 203:22 204:11 205:2 213:17 221:1 222:14 224:18 225:11,21 225:21,22 231:5 239:20 246:2 264:1 271:10,17 278:9 309:2,2,4
**meaning** 56:9 63:10 64:1 66:7 78:11,12 83:4 85:15 87:18,21 88:21 154:4,21 155:21,22 162:4 213:16 223:14 224:10 257:4
**means** 34:17 42:13 56:6,15 84:6 88:12 163:14 205:12 228:20 267:17 349:3
**meant** 86:2 92:20 134:20 162:16 199:9 217:2 225:8 231:11 250:22
**measurement** 338:15 339:15
**mechanism** 190:22 191:12,16,19 192:10 193:2,13 193:16 195:6,22 196:17 197:5,15 198:3
**mechanisms** 192:22 199:9
**medications** 18:5
**meet** 21:16 68:21 315:21 328:10
**meeting** 22:16 25:9
**meets** 286:2
**mejoh18@nsa.gov** 4:22
**member** 315:9
**members** 97:7 99:2
**Memorandum** 5:20 6:13,16 7:7 159:19 174:14 279:16 280:7 310:20 311:8 312:8 343:8
**memory** 18:10 22:19 78:2
**mentioned** 21:19 36:15 43:18 51:8 107:3 111:11 141:7 142:6 161:4 219:3 221:6 266:10 362:8
**met** 8:7 20:21,21 21:19 22:4 315:20 315:20
**metadata** 274:17 304:5 352:17 353:11 355:10,19 356:10,17 357:3 358:8,9,12,18 359:2,14
**method** 233:20
**methods** 40:15 101:12 121:14,15 126:12 127:19 140:5 145:20 164:2
**Michael** 30:3 45:4 119:7
**middle** 355:9
**mind** 12:1 62:17 95:5 110:22 129:13 133:21 156:22 159:6 190:6 209:7,22 221:5 296:16 297:10 348:11
**mine** 41:7 221:9
**minimization** 20:7 313:3 355:14
**minimum** 28:3
**minute** 155:8 156:18 190:9 260:11
**minutes** 75:19 146:7 214:21 352:9
**mischaracterize** 348:21
**mischaracterizes** 81:9 110:8 112:12 187:22 228:1 304:19
**misheard** 180:9
**mislead** 136:13
**misleading** 114:12
**misperception** 218:1
**missing** 244:1
**mission** 25:19 26:22 319:1
**misstatement** 94:19 172:20
**misstatements** 173:7
**misstates** 73:19 111:4 264:2
**mistakes** 167:18,21
**mitigate** 25:8 32:21
**mixing** 22:21
**mixture** 101:10
**Mm-hmm** 131:21 194:14 263:21 343:18
**modify** 208:21
**moment** 77:14 124:7 132:12 133:14 138:8 158:2 160:14 171:15 185:19,20 202:12 207:13 238:11 241:1 251:10 255:19 266:20 277:6 293:22 301:2 302:17,19 309:20 326:20 338:17 349:8 355:22
**moments** 214:9
**Monday** 1:13 361:12
**monitor** 39:17
**monitored** 160:8 188:20 232:2
**monitoring** 322:19 324:11
**month** 221:15
**morning** 8:2
**Motion** 6:14 279:17 280:8
**move** 40:8 51:18 65:21 75:5 95:4 252:16 308:8 318:9
**moved** 37:8,9
**Moving** 219:9
**multiple** 83:10,15 84:17 86:6 87:2,5 88:16 126:7 144:21
**multiplexed** 82:1
**multiplexing** 82:2
**multi-communic...** 240:12
**multi-communic...** 238:9

## N

**N** 8:1
**name** 8:3,14 9:14 89:15 211:17 218:21
**narrative** 102:18 122:14
**narrow** 96:4
**national** 1:7 4:15 6:9 9:1,6,9 30:2 45:3 117:21 118:13 119:3,17 163:19 164:6,15 164:20 170:12 220:16,18,20 233:8 235:6 236:13 239:14 240:5,7 242:2 250:16 252:8,17 361:5 363:4
**nature** 22:6 28:1 29:3 30:22 40:4 41:16 92:9,12 117:5 121:9 163:11 265:5 289:9 353:5
**NDA** 240:2
**necessarily** 15:19 101:6 107:3 110:3 111:13,21 112:1 132:22 137:17 139:20 141:12 144:15 174:20 265:4 299:7
**necessary** 10:1,7 293:19 297:2 298:10 299:21 300:11 324:20 326:1,18
**necessitate** 172:21
**need** 14:4,7 16:4 30:14,20 38:18 39:3 40:1 53:5 77:14 78:1 103:7 110:10 133:16 156:15 197:19 213:4,12,14

214:15 216:13 236:19 261:20 268:10 271:6 303:9 326:11 334:21,22 335:2 342:11
**needed** 38:7,9
**needs** 314:9,13 315:20,21,22 319:1
**negotiate** 34:1
**neither** 76:19 77:4 128:17 193:14 238:14 362:11
**network** 35:10 36:22 37:11 38:10 38:14 39:10,13,18 40:13 56:13 59:10 60:3 66:3 67:5,8 67:17 246:9 247:8 247:9 255:7,17 256:21 257:14,15
**networks** 35:10 36:22 40:12 46:20 47:20 48:3,14 50:22 52:17,19 55:1,3,5 60:3 66:10,15,16 343:12
**never** 44:6,12
**new** 3:7,7 169:11 169:17 199:8 299:8 363:2,2
**newspaper** 240:15
**nice** 328:10
**nod** 13:9
**nonclassified** 22:14
**nonprofit** 33:9,10
**nonpublic** 77:2
**Non-Disclosure** 239:19
**non-foreign** 231:1
**non-objection** 65:13
**non-targeted** 230:11,15 231:2 231:16,22
**non-United** 233:9
**normal** 257:16 345:12 346:13
**Northwest** 2:7
**Notary** 2:8 12:8 362:1,2,20 363:21
**note** 88:15 103:12 107:8
**noted** 47:8 51:17 55:21 99:15 310:15 361:18
**notice** 2:4 5:10 6:7 7:9 19:14 65:1 69:9,11 76:12 102:1 242:6 307:10 308:7 312:17 354:21
**noticed** 99:8 100:3 100:19
**Notices** 31:21
**notification** 315:22 322:6
**notified** 99:9 100:8
**notify** 99:14 172:9
**notifying** 309:13
**notwithstanding** 124:17
**November** 355:2 355:17
**NSA** 5:16 6:18,18 6:21 8:21 10:20 11:7,11,12,14,19 12:14 15:6,12 16:5,10,12 18:20 19:18 20:7 21:20 21:21 22:1,4,20 24:15 25:2,11 26:3,22 35:11,19 36:6 37:11 40:6,9 40:16 42:12 43:3 43:11,12,18 44:1 45:18 49:16,16 50:20 54:12,18 55:12 56:2 57:22 60:13,19 61:6 62:8 63:5,9 64:1,5 65:4,19 67:8 68:2 68:17 69:5,13 70:9,16 71:9,9 73:3,6,7 74:3,7 75:2 77:2 78:5,11 82:18 83:2,6 84:8 85:4,11,15,20 86:19 87:13,17 88:7,10,12,17 89:9,19 96:13,16 97:6,10,14,22 98:7,16,21 99:2,6 99:9,10,18 100:7 100:15,18,22 101:6 102:1 105:20 107:9,21 108:11 109:21 114:13 120:14 121:17 122:20 123:7 126:9 130:3 130:8,10 131:2,10 132:9 133:11 137:20 140:21 141:5 143:1,6,17 143:20 154:4,21 155:20 156:1 160:5,8 161:16,20 163:18 165:12,20 166:13,15,22 167:21 168:17 171:10 172:5,9,19 173:6 174:20 175:4,10,19,20 176:21 177:21,22 178:3,17 179:8,18 179:19 180:2,16 181:2,10,19 182:5 183:4,11 186:11 188:15,20 191:14 202:8,18 206:5,7 206:9,10 210:16 210:20 211:16 219:12 221:21 222:5,10 226:19 227:19 228:11 229:21 230:10 232:2,3 234:3,5 234:18 236:14 238:8 240:10 242:3,10 249:18 251:3,9 253:20 255:16 257:6,18 258:16 259:7,21 260:4 261:15 263:5,12 264:9 266:5,16,17 267:18 268:15 269:4,21 270:15 271:13,16 272:6 272:11 273:8 274:9,17 275:3,9 275:15 276:3,11 276:18 277:3 278:2,3,22 281:1 281:16 282:2,8,21 283:7,19 284:4 285:13 290:6,17 291:3,10,17 292:2 292:9,15 293:2,10 293:20 294:22 295:6 296:9 297:3 300:20 301:9,17 302:3,15 303:5,22 305:9,13 306:2,11 306:21 307:7,12 308:16 312:18,19 312:22 313:19 314:8,11,15,22 315:9 316:20 317:13 318:6,7,19 319:4,8 320:4,14 320:14,18 321:14 322:1,19 324:10 328:15 329:3,11 329:19 330:5,13 331:17 333:22 339:4,16 347:16 349:20 350:7 351:3 355:14,19 356:17 357:3,22 358:8,11,17 359:1 359:13
**NSA's** 5:17 20:10 45:21 55:14 65:16 65:18 71:8 73:12 77:19 87:19 88:1 95:19 100:10 130:4,22 143:1 154:5 162:2 164:5 189:21 190:16,21 192:5,11 194:8 195:15 196:18 197:6 200:11 204:1 205:11,11 221:22 222:6 233:20 269:19 313:2
**NSA-developed** 253:6
**NSA-specific** 257:10
**NSA-WIKI** 5:21 6:8 159:17,17,22 221:8,9,11
**number** 10:10 20:5 47:15 97:14,15 114:9 128:14 142:1,3,7 145:14 145:15 146:10,11 180:5 181:17,18 182:4 183:3,4,10 183:11 184:21,21 185:6,6 206:16 225:8 354:11
**numbered** 159:16
**numbers** 134:21
**N.W** 4:8

## O

**O** 8:1
**oath** 12:4,18
**Obama** 249:10
**object** 13:19 35:13 35:13 42:19 43:7 43:14 44:4 46:1 53:2 56:17,17 58:5 61:14 64:8 65:9 67:9 68:3 69:6 70:19,21 73:18 79:8 82:21 86:10 89:2 90:3 90:20 91:13,14,15

93:22 96:8 102:14 103:13 106:2,18 108:4 109:4 113:22 117:22 118:17 121:20 123:10 124:22 127:16,17 141:3 141:20 155:1 157:3 158:9 163:16 165:7 171:21 174:6 180:9 193:7 194:17 204:5 205:17 216:8 222:16 223:11 224:14,14 225:18 226:22 227:22 228:16,17 232:19 242:5,12 243:1 245:3,12 247:13 250:7 260:5 264:11 267:9 268:18 277:15 284:19 285:3,16 289:21 294:2 296:12 297:13 300:3 302:6,7 307:18 310:10 311:1 315:4 317:4 325:3 326:3,22 331:10,20 333:5 333:12 335:7 337:4 348:20 352:20 353:12 357:11

**objected** 13:21 170:15 214:17

**objecting** 28:22

**objection** 23:10 25:20 27:6 28:11 29:3 36:7 38:17 38:20 40:14 46:21 48:5,20 49:6,13 50:4 51:4,5,6,17 55:8,17 56:7 59:12 60:5,14,22 62:10 63:12 65:11 66:4,18 68:18 71:19 72:11 78:8 79:2,9,18 80:3,4 81:8,10 82:3,12 82:21 83:11,12 84:3,19,20 85:22 87:7 95:22 96:1 96:15 98:19 100:12,21 104:2 110:7 111:3,4 112:11 115:11 116:1 118:9 121:4 123:22 125:17 126:11 129:3,10 130:15 134:2,3 135:8,17 136:4,9 136:21 137:4,12 137:14 138:19 139:14 142:16 143:13 144:9 145:7,17,19 146:13 148:9 149:14,21 150:6 150:13,20 151:5 151:14,15,17 152:3,18 153:3,18 154:12 156:2 157:18 158:19 161:1 162:7,19 163:6 164:7,21 165:8 166:2,8 168:1,9,19,20 172:11 173:1,10 174:5 176:2 178:21 179:13 180:19 181:5,13 181:21 182:7,13 182:21 183:6,13 184:1,9,16 185:2 185:9 186:14 187:21 188:21 196:19 198:13 201:5,15,21 202:21 205:7 206:21 207:9,22 208:8,16 209:4 212:7 213:15 217:7 219:15 220:17 223:21 224:3,21 225:6,16 225:17 234:22 236:9 244:13 248:11 252:22 254:7,13 255:1,9 256:2,17,22 258:19 260:20 262:15 263:14 264:2 266:8 267:22 269:7 270:1,7,17 271:6 272:17 273:10 274:10 275:4,10 275:18,19 276:13 276:20 279:4,21 281:4 282:10 283:11,12,22 286:19 290:9 291:19 292:5,11 292:18 293:5,13 295:16 296:1 298:21 300:15 301:4,12,20 303:17 304:18 305:16 306:5,16 307:2,9,14 308:1 308:18 311:13 313:21 315:14 317:1,3,16 319:12 321:16 322:2,20 323:16 324:12 328:18 329:6,14 329:22 330:8,16 332:11,12 334:3 334:10,20 335:17 336:3,10,18 337:14 338:2 339:18 340:12,13 341:13,14 342:2 342:19 343:7 344:10 345:5,18 347:6 349:10,22 350:9 351:5 354:2 354:7 356:2,7,20 357:20 358:14 359:4,16

**objections** 5:11 9:22 15:5 30:1 45:2 57:3 62:1 76:10 77:20 83:18 83:19 90:13 92:6 92:14 93:14 123:2 125:3 126:1 128:5 128:12 146:21 147:7,16 148:2,15 165:17 166:3,19 167:4,12 169:9 170:8 179:21 189:21 206:8 243:12 244:5 246:3,10 249:2,12 249:19 259:10 264:3 274:19 276:7 278:6 279:5 287:4,9 288:9 290:20 291:6,13 309:6 320:19 321:5,17 322:13 340:4,20 344:4 346:6,15 350:20 353:14

**obligation** 65:5

**observed** 251:5

**obstacle** 309:4

**obtain** 191:14

**obtains** 253:20

**occasion** 13:11

**occur** 233:3

**occurred** 177:16 235:9 240:14

**October** 5:19 159:20 174:3,12 186:11 187:18 188:15 189:5,10 189:18 312:17 316:4

**ODNI** 26:3,8,16 235:17 237:19 240:16 339:4

**ODNI's** 20:17 176:7

**offer** 142:18 356:9

**office** 5:17 9:1,6,9 20:8 24:17 25:1 25:22 26:9,14 27:20 29:10 31:14 38:15 101:7 109:21 120:15 130:4 192:3 209:13 219:4 235:5 236:12 240:4,7 242:2 246:17 299:10 312:19

**officer** 32:15 37:19 37:20

**offices** 2:5

**office's** 25:13,19 28:1

**official** 163:17 210:20

**officially** 339:2

**oh** 19:16 57:13 58:22 190:3 194:20 210:6 211:10 249:13 259:12 273:19 348:19

**okay** 12:22 14:14 15:1,14 18:12,18 22:15 24:14 30:13 35:1,17 40:1,3,7 44:12,15 45:19 51:20 55:14 57:13 58:22 59:8,8,20 61:4 62:17 65:21 67:21 68:12 74:2 77:12 79:5,22 80:14,20 81:2 83:9 84:2,16 86:8 91:9 93:20 105:19 106:15 108:17 109:2 111:10 113:16 121:1,17 122:19 128:8 129:9,12 132:3 140:18 143:9 144:19 146:18 153:10 154:10

155:19 156:19 157:16 158:2 159:3 160:16 167:16 173:5 175:4 177:7 178:13,17 180:2 182:11 183:17 185:17 187:7 188:13 189:12,19 191:10,21 193:9 195:18 196:15 198:15 199:17 200:10,20 201:12 203:9,22 210:6 211:8 212:1 215:19 216:16 217:12,16,17 219:8,22 220:22 221:10 229:14 230:7 232:7 238:6 240:20 242:19 243:8,20 248:5 249:8 252:11,14 253:11,18 254:20 256:15 257:21 273:19 284:10 314:19 321:8 339:14 342:13 350:12
**old** 130:7
**omits** 112:19 113:11,19 114:3 114:10,15 133:3
**omitted** 145:12
**omitting** 115:2,4
**once** 108:21 195:19 223:1 308:5
**ones** 20:13 169:12 226:1
**on-the-job** 36:12 36:17 38:11 39:9 39:21 40:10
**open** 292:10,16 337:11,21
**operate** 273:4
**operated** 5:14 6:5 95:16 109:11 132:5 140:14 142:14 143:12 191:11 195:5,21 197:14 200:21 210:13 244:11
**operates** 167:9 244:10
**operation** 25:18 105:1 112:20 113:12,20 115:13 115:21 117:11 126:9 127:9 133:4 135:7,16 136:14 137:9,10 138:6,16 139:12 141:18 144:8 165:14 168:5,15 170:5 174:2 179:17 312:19
**operational** 40:16 126:13 145:21
**operations** 345:11 345:12 346:13
**opinion** 5:20 6:16 7:7 50:5 55:9,18 154:13 156:3 158:10 159:20 160:13 172:6,8,20 173:11 174:4,14 176:9 177:19 178:18 179:9 225:17 243:4 245:14 255:11 257:2 295:5,8,10 310:20 311:8 312:8 343:8 352:22
**opinions** 20:10,12 20:19 99:2 142:2 171:11,13 173:8 174:18,19
**opportunity** 169:13 176:16
**opposed** 41:11 56:20,22 69:12 76:15 83:22 218:20 219:4
**optical** 56:16 60:1 79:22 80:8 81:5 81:18,21 93:18 148:19,22 149:11 149:18 150:3,10 150:18 151:3,10 152:1,8
**options** 114:6
**orally** 13:7
**order** 6:8,16 10:12 105:14 106:10 155:16 202:10,22 220:10 304:2 312:9 319:8,14 320:17
**ordering** 321:12
**organizations** 25:10
**original** 94:14 95:1 119:20 179:1
**originally** 73:2 155:15
**ought** 144:22
**outcome** 362:17
**outline** 101:18 108:12 133:1 352:10
**outlined** 15:4
**outset** 221:7
**outside** 90:5 100:4 100:5 169:15 224:19 233:10 240:1 241:14 245:17 253:1 257:11 282:10 287:13 351:15
**outstanding** 241:19 242:1
**overclassifying** 260:6
**overcollection** 235:7 236:14 238:7 240:8,10
**overseas** 191:15 192:7 194:11
**oversight** 5:13 20:9 25:14,16 26:1,19 95:15 131:7 142:20 210:12

**P**

**P** 8:1
**pace** 151:18
**packet** 90:1,11 244:12,21 245:11 247:10 348:16 349:2,7
**packets** 90:18 91:9 91:11,19 92:16 93:12,17 94:8,15 242:22 243:11 244:4 246:8 254:4 254:20 301:18 348:18
**Padgett** 4:16 8:22 8:22 52:2 53:17 72:16 76:21 127:13 132:14 149:3 167:13 180:7 197:19,22 198:6 207:14 213:5 244:22 261:22 262:6 266:22 286:9,12 347:22
**page** 5:2,9 6:3 7:3 45:6,8,12,14,16 58:12,15,17 77:12 77:13,16,21,22 86:14 96:17 98:12 98:14 99:15 104:21 108:18,20 108:22 109:1,9,10 109:14,16,22 110:3,5,6 117:3 119:14,15,21 126:20 127:1 131:16,19 139:4 159:21 160:2 185:13 187:14,22 190:1,14,14 192:4 194:1,4,6 195:16 198:17 199:18 200:15 201:3 203:17,18 204:4 209:12,14 210:22 211:7,21 217:13 217:14,18 221:5 221:10 233:3,16 233:19 250:19 273:3 280:11,16 281:13,15 282:19 282:20 312:11,16 320:2 333:21 343:15 346:1,3 355:6 363:6
**pages** 7:6 98:12 112:9 113:8 115:10 124:12 190:15 197:7 361:11 362:5
**paid** 34:17
**paper** 88:5 347:1
**paragraph** 45:15 108:20 127:1 131:19 190:4,15 222:4 273:4 280:15 281:15 282:19 318:22 343:16 355:9
**paragraphs** 58:20 77:15
**parens** 134:10,18 134:19 196:13
**part** 16:17,17 25:19 26:2,6 32:3 37:2 37:17 38:2 43:3 43:17 49:5 50:13 51:1 52:1,20 62:13 67:3 77:2 85:18 93:17 98:14 99:8,11,15,18 131:8,8 136:12 161:13 173:18,19 192:10 196:16 197:5 200:16 202:18 242:11 249:9 261:8 263:3 287:15,21 316:7 316:15 325:18 347:18

**parte** 170:9
**partially** 110:12
**participated** 246:18 252:12
**participates** 171:11
**particular** 38:21 56:9 80:16 106:19 106:21 107:6 108:9,13 119:9 139:3,19 177:9 224:2 226:1 232:15 239:11 245:17 259:15 285:22 286:1 314:14 320:10 321:6 339:5 346:21
**particularly** 101:13 333:21
**parties** 9:18 15:4 362:12,15
**passage** 281:14 282:1,18 308:4 318:21 322:4
**passed** 169:11
**passes** 232:1
**path** 73:1 91:19
**paths** 83:10,16 84:18 86:6 91:11 92:17 93:11 94:9 94:15
**patience** 328:11
**Patrick** 3:19 8:8 258:12
**Patton** 4:3,10 8:16 8:20,20 9:17,17 13:1 15:3,17 17:22 23:10 25:20 27:6 28:11,21 29:15,18 30:16 34:12 35:13,16 36:7 38:17,19 40:14 41:5,15 42:19 43:7,14 44:4 46:1,21 48:5 48:20 49:6,13 50:4 51:4,19,21 52:6,22 53:2,22 55:8,17 56:7,17 57:3 58:5 59:12 60:5,14,22 61:14 62:1,10,19 63:12 64:8 65:9,13 66:4 66:18 67:9 68:3 68:18 69:6 70:1 70:19,21 71:19 72:11,15 73:17 74:19 75:13,22 76:8 77:1 78:8 79:2,8,18 80:3 81:8 82:3,12,21 83:11,19 84:5,19 85:6,22 86:10 87:7 88:14 89:2 89:12,15 90:3,13 90:20 91:13 92:6 92:14 93:14,22 94:4,10,19 95:2 95:22 96:15 98:19 100:12,21 102:9 102:11,14 103:3 103:15 104:7,12 106:2,18 108:4 109:4 110:7 111:3 112:11,22 113:14 113:22 115:11 116:1 117:22 118:9,17 119:8 120:6 121:4,20 122:9,14 123:1,10 123:22 124:22 125:3,17 126:1,11 127:2,16 128:5,8 128:12 129:3,11 130:15 132:12 133:14,16 134:2 135:8,17 136:4,9 136:21 137:4,12 137:14 138:8,10 138:19 139:14 141:3,20 142:16 143:13 144:1,3,9 145:7,17,19 146:8 146:13,21 147:7 147:16 148:2,9,15 149:2,6,14,21 150:6,13,20 151:5 151:14 152:3,11 152:18 153:3,18 154:12,22 156:2 156:15 157:3,18 158:9,19 160:14 161:1,10,14 162:7 162:19 163:6,16 164:7,11,21 165:7 165:17 166:2,8,19 167:4,12 168:1,9 168:19 169:6,9 170:6,8 171:15,17 171:21 172:11 173:1,10 174:5 175:13,15 176:2 177:2,4,8 178:21 179:13,21 180:9 180:19 181:5,13 181:21 182:7,13 182:21 183:6,13 183:20 184:1,9,16 185:2,9 186:6,14 186:22 187:1,8,12 187:21 188:5,21 189:11 193:5,7 194:17,21 196:19 197:8 198:9,13 201:5,15,21 202:12,14,21 204:5 205:7,17 206:8,21 207:9,13 207:22 208:8,16 209:4 212:7 213:8 213:14,22 215:13 215:19,21 216:8 216:14 217:7 219:15 220:17 222:16 223:9,11 223:21 224:14,21 225:6,16 226:13 226:22 227:22 228:14,16 229:4 232:8,11 234:9,22 235:10 236:9 238:11,13 239:10 240:13 241:1 242:5,12 243:1,12 244:5,13,15 245:3 245:12 246:3,10 247:13 248:11,19 249:2,12,19 250:7 251:10 252:19,21 254:7,10,13 255:1 255:9,19 256:2,17 256:22 258:1,19 259:10,13 260:2 260:14,20 261:18 262:4,10,15 263:14 264:2,11 265:7,15 266:8,20 267:3,9,22 268:18 269:7 270:1,8,17 270:21 271:6 272:13,17 273:10 273:17,21 274:10 274:19 275:4,10 275:18 276:6,13 276:20 277:6,8,15 278:6,10,13 279:4 279:21 281:4,19 282:10 283:11,22 284:9,11,19 285:15 286:19 287:4,9 288:9 289:3,19 290:9,20 291:6,13,19 292:5 292:11,18 293:5 293:13,22 294:2 294:11,14 295:7 295:16 296:1,12 296:16,19 297:7 297:10,13 298:15 298:21 300:3,15 301:2,4,12,20 302:6,17,19,21 303:9,17 304:7,16 305:16 306:5,13 306:16 307:2,9,13 307:16 308:10,18 309:6,20,22 310:9 311:1,13 313:13 313:21 315:2,4,12 315:14 317:1,3,16 319:10,12,16 320:19 321:5,16 322:2,13,20 323:16 324:4,12 324:22 325:3 326:3,20,22 327:21 328:18 329:6,14,22 330:8 330:16 331:8,10 331:20 332:11,15 333:5,12 334:3,10 334:18,20 335:2,7 335:17 336:3,10 336:18 337:4,14 338:2,17,21 339:2 339:18 340:4,12 340:20 341:7,10 341:13,22 342:11 342:19 343:7 344:4,10 345:5,18 346:6,15 347:6,20 348:20 349:8,10 349:22 350:9,14 350:17,20 351:5 351:11 352:1,18 352:20 353:12 354:2,7 355:22 356:2,7,20 357:6 357:8,11,20 358:14 359:4,16 359:21
**pause** 52:22
**pausing** 114:18 141:22
**PCLOB** 6:4 27:3 47:10 96:3 97:7 97:15,22 99:9 100:8 102:2,7,19 103:1,22 105:21 105:22 106:4 109:15 120:15 132:21 135:13 136:13 138:16 198:18 199:11 273:2

**PCLOB's** 96:9 103:13 144:7
**penalty** 166:15
**pending** 76:1,3 77:5 265:21
**people** 42:14
**perfectly** 104:13
**period** 17:7,9,17 186:7 259:4 296:17 337:15 356:3
**periodic** 14:3
**periods** 138:7,17 187:3
**perjury** 166:16
**permissible** 218:13
**permit** 219:12
**permitted** 228:11 229:21 230:10 284:4
**person** 75:8,10 191:14 218:3 286:1,6 288:6 312:22 319:3
**personal** 69:12 76:14 83:22 170:20 171:22 242:7 248:16 250:11 253:3 277:17,19 286:22 309:11 333:8 337:6 342:21 346:18 353:1 355:9
**personally** 317:7 331:12
**persons** 196:12,13 233:9
**perspective** 130:22 287:18
**phone** 3:8,15 4:10 206:16
**phrase** 59:21 186:2 215:4 260:3
**phrased** 52:8 188:5
**phrasing** 259:15
**physical** 56:5,15 57:9 58:2 59:4,6 83:10,16 84:18 86:6 87:6 93:12 93:15 239:7
**PIA** 248:2 249:4 251:17
**piece** 88:5 140:10 209:20 261:12 288:1,18 346:22
**pieces** 99:13 288:12
**pilot** 251:1
**piloted** 251:8
**place** 13:3 16:3 17:5 109:19 131:1 153:20 322:5 362:7
**places** 206:4
**plaintiff** 1:5 8:5 12:10 19:14 46:13 361:4
**plaintiffs** 2:4 3:2,18 10:20 30:4 46:9 189:22 328:7
**plaintiff's** 5:11 11:18 45:4 77:20
**play** 227:13
**please** 8:19 13:20 14:21 15:22 16:17 17:10,10,16 29:21 45:6 73:9 75:12 77:12,15 79:14 94:17,22 108:19 110:19 126:20 132:1 158:5 169:5 183:21 202:7,17 214:13 223:3 247:21 260:18 262:13 269:3,20 271:3 273:7 279:10,19 280:6 280:10 284:16 286:17 289:16 293:18 296:9 297:1,11 298:9,18 299:20 300:10 303:14 309:17 311:21 312:4 317:20 318:2,10 318:15 323:5,7,13 324:19,22 325:22 326:17 330:21,22 338:22 342:9 343:15 350:5,18 354:13,18 355:6 357:9
**plural** 125:10 126:4 132:8 134:14
**plus** 352:2
**point** 14:5,8,10,16 30:17 57:1 58:7 104:20 105:5 107:6 109:13 110:14 111:16 117:2 128:17 134:15,16 178:1 206:10 217:15 232:15 235:12 239:2,11 249:5 299:6 311:19 333:22 344:13
**pointed** 118:2 196:5 297:18
**pointing** 117:14
**points** 6:13 13:20 20:11 279:16 280:7
**policies** 33:11 34:8
**policy** 33:14 271:19
**port** 291:5,12
**portion** 12:22 17:9 26:6 98:16 100:4 100:5,19 170:1 195:14 200:14 288:21 302:4,15 303:6,22 305:2 306:3
**portions** 21:14 99:7 101:5 108:13 300:12 304:13 306:10 343:2 347:17
**position** 24:14,19 24:22 25:18 31:5 31:10,15 33:7,15 34:9 36:18 103:10 241:2 246:14 315:21
**positions** 346:19
**possible** 52:11 117:4 144:16 166:12 239:22 269:4,21 285:10 287:20 288:13
**possibly** 287:16
**post** 306:13,15
**potential** 199:4 200:5 201:19
**potentially** 170:19 248:12 296:13
**practice** 173:6
**precisely** 135:22
**preparation** 63:17
**prepare** 20:3
**prepared** 19:21 232:14
**preparing** 20:19 21:17 23:4 63:11
**prepping** 227:12
**present** 3:18 4:15 17:5
**presentations** 96:19 97:7 98:4
**preservation** 103:16
**preserving** 103:5 252:21
**President** 7:8 343:9
**Presidential** 271:19
**press** 6:18 318:6
**pretty** 191:2 316:12
**prevent** 10:1,8 282:5 283:2
**preventing** 10:14
**prevention** 248:9
**previous** 20:7 125:10 158:8 169:12 216:5 260:18 298:9 342:3 346:19
**previously** 21:8 51:8 161:4 312:21
**primary** 22:15
**prior** 11:17 23:21 28:8 29:10 33:7 33:21 35:11,18 36:6 40:5 46:7,8 73:19 81:9 85:16 94:20 110:8 111:4 112:12 120:13 121:22 142:5 177:14 228:1 264:3 284:17 301:10,18 303:15 304:19 327:6 353:13
**PRISM** 29:1 208:14 209:2,16 212:5,16,22 214:10,19 215:8 216:6 217:5 218:6
**privacy** 5:13,17 6:11 20:8,8 24:17 25:3,7,11 26:19 28:6 31:12,14,20 31:21 32:2,11,15 32:16,20 33:11,14 34:2,8 36:9 37:6 37:15 38:6 95:15 101:7 109:21 120:15 130:4,22 131:7 192:3 209:13 210:11 219:3 246:16,17 246:19,21 248:22 252:7 299:10 314:10 319:3 325:14 344:13
**privately** 10:12
**privilege** 15:7 30:19,22 31:1 40:17 41:3 63:14 96:2,10 103:6,17 116:3 118:7 119:6 120:5,11 121:3,10 121:22 123:12,13 125:13 129:5

145:22 162:8 163:20 215:16 273:22 281:6 282:13 307:19 328:20 331:22 332:16 339:9,20 340:14
**privileged** 10:2,9 10:16 11:16 54:1 63:16 105:7 134:4 206:22 267:11 357:13
**privileges** 10:19 71:22 111:7 116:4 118:20 122:1 126:14 127:20 129:6 155:4 156:5 161:4 174:7 180:11 194:22 196:21 201:7 202:1 204:7 205:19 208:2 217:9 219:17 222:19 224:3 228:19 232:22 234:11 242:14 245:5 254:15 258:21 261:1 262:17 266:10 268:20 269:10 270:3 272:19 273:13 274:13 281:7 282:13 283:14 285:5 290:1,11 294:4 299:2 300:5 302:9 303:19 305:18 307:20 310:12 311:3,15 314:1 317:6 322:22 324:3 325:5 326:5 327:2,9 328:20 332:1,17 333:14 335:9 337:16 339:10,21 340:15 347:8 350:2 352:2
**probably** 122:9 134:17 144:3,14 187:6 247:6 350:11
**problem** 52:1 240:10
**problems** 236:14 238:8
**Procedure** 360:1
**procedures** 13:1,2 20:7 28:4 192:5 194:9 196:14 219:10 232:13 233:7 285:1 313:3 321:10,11 355:14
**proceeding** 103:22
**process** 15:4,10 16:3,4 26:17 27:21 28:2 31:20 32:17 37:3 96:2,5 96:9,20 100:2 102:21 103:14,17 105:3,16 165:3 176:12 195:7 196:1,6,17 197:16 198:16 199:11 204:18 209:15 246:7 267:14 325:15
**processes** 135:19 201:1 244:9,19 251:3
**professional** 225:15
**professionals** 55:1 60:4
**program** 5:14 6:5 95:16 101:5,18 105:1,11 107:4 128:20 131:11 133:1 140:4,5,17 141:12 210:13 212:5,22 214:19 215:8 217:5 248:9 248:14,18 251:8 265:5 273:4 280:20 320:3
**programmed** 281:1
**programs** 2:6 4:7 25:6 36:3 38:15 43:5,12,18,19 44:1 143:7 247:1 252:8
**prohibit** 321:14
**prohibited** 313:3 321:22
**prohibition** 322:11
**promise** 133:17
**properly** 28:6 351:18
**proposed** 28:4
**protect** 96:9 121:15 224:4 241:7 343:12
**protected** 10:2,8,15 11:15 15:7,13,19 16:2 28:6 40:17 41:13 51:7 71:1 71:18,21 123:12 124:14 127:20 204:7 208:1 217:9 228:19 242:14 245:5 260:22 262:17 268:20 269:9 270:3 272:19 281:5,6 282:12 294:4 303:19 305:17 310:12 311:3,15 314:1 322:21 323:18 325:5 326:5 327:2 335:9 337:16 340:13 350:1
**protecting** 251:4
**protection** 41:4 252:8
**protections** 10:19 130:22
**protocol** 89:22 90:11,18 191:13 192:6 193:3,21 194:10 201:14 206:19 225:12
**provide** 15:1 16:19 27:1 38:2 50:15 50:19 52:9,10 65:5 73:11 74:15 75:2,4 87:22 89:15 100:22 101:10 111:22 116:17 117:1 141:11 145:1 155:6 161:22 163:12 165:12 166:11 186:20 190:21 203:12 235:13 241:8 261:5 264:16 265:12 268:5 272:6 289:16 293:19 294:6,9,15 294:19 295:14 296:4 297:2 298:10 299:4,7 304:22 307:21 309:10 314:3,3 327:16 349:15,15 349:18 357:16
**provided** 23:15 45:17 46:12 53:15 63:19 64:5,18 73:5,12 74:21 76:18 85:20 96:16 96:18,19 97:6,11 97:22 98:4 111:17 134:20 141:6 157:10 178:15 187:6 203:14,21 233:2 241:5 264:19 273:11 289:6 296:22 298:8 299:20 300:10 311:7 316:3,9 325:21 326:14 327:5,17 346:22 356:14
**provider** 48:16,19 67:6,15 128:15 129:1 134:12,13 161:18 198:20
**providers** 46:20 47:21 48:4,14 51:1 52:20 55:6 66:16 126:8 127:12 132:8 133:10
**provides** 11:13 111:18 165:21 239:15 240:1 249:21
**providing** 27:9 62:15 72:8 114:6 128:14 140:3 238:16 240:19 268:12 295:22 298:4 299:15 327:19
**provisions** 323:19
**public** 2:9 6:4 12:8 33:1 70:12,14,18 71:7 74:5,11 111:12 130:21 135:12,14 136:13 141:17 175:12 176:1 210:12 232:13,17 238:19 285:1 316:17 338:8,8,10 362:1 362:2,20 363:21
**publicly** 14:20 20:14 73:11 131:13 226:20 339:4
**published** 237:19 248:3
**publishes** 74:14
**publishing** 25:9 31:20
**purport** 140:13
**purports** 137:10
**purpose** 10:14 22:15 30:17 130:18,20 141:9 233:21 346:8
**purposes** 51:2 215:1 272:7
**pursuant** 2:4 5:14 6:5 95:17 129:4

207:1 210:13
233:11 357:13
**put** 50:7 76:10
130:21 131:9
134:10,18,19
176:16 295:6
321:10
**puts** 322:5
**putting** 37:5 310:9
328:11
**p.m** 128:10,11
133:19,20 153:12
153:13 156:20,21
190:10,11 198:10
198:11 207:16,17
216:19,20 232:9
232:10 241:17,18
258:2,3 260:12,13
262:8,9 267:6,7
271:1,2 272:14,15
277:10,11 284:12
284:13 286:14,15
287:7,8 297:8,9
298:16,17 303:12
303:13 310:1,2
314:6,7 323:9,10
328:5,6 338:19,20
342:14,15 348:6,7
350:15,16 352:11
352:12 360:3

**Q**

**qualify** 59:9
**quasi-invocation**
103:13
**queries** 313:4,10
**query** 218:13 313:1
**question** 10:6,6
13:12,21 14:19
16:9,12,16 23:13
28:13 30:14 38:21
39:15 40:14,19
41:10,11,17 42:5
43:9 45:7,11
50:20 51:9,12,16
51:22 52:4,8,11
53:4,5,9,10 54:3
54:21 57:14 59:21
60:16 63:12 68:11
68:12 70:10,12,17
71:2,6,17 72:8,9
72:17,19,20,22
73:8,12 74:10,16
75:22 76:2,5,16
77:6 81:4,5 82:13
84:13,14 85:5,12
87:14 88:8,9 89:3
89:13 90:4,8
91:18 93:10,21
94:11,14 95:1,2
96:4,8,13 102:12
102:13,16,18
104:18,19 105:17
111:1,2 113:3,4
114:5 116:5,11,22
117:10,20 118:1,8
118:13,18,21
119:7,9,11,12,20
120:3,7 121:12,20
122:2,4,18 123:2
123:4,10,15,20,21
125:1,14 126:16
127:14,15,18,21
128:7 132:15,16
133:22 134:1
138:3,13 139:2,9
144:6,19 149:4
151:21 154:20
157:1,2,3 161:1,6
162:5,10 163:13
163:16,22 164:14
165:8 167:14
171:20 175:16
177:6 178:4,22
179:4 180:8,13
183:22 186:3,18
188:6 189:1 192:9
194:18 195:14,19
197:4,9,21 198:12
201:17 202:3
203:1,3 207:2,20
208:19 209:9,19
212:20 213:2,6
214:1,8,12 216:1
216:5,9 217:1
219:4,18 221:18
222:12,17 223:4
224:6 228:20
229:8 230:3,7,22
234:2,5,10,13
236:5,6,8,10,11
236:17 237:3,4,8
237:9,10,12,15,22
238:18 239:3
240:22 241:3,11
241:20 242:1,12
242:15 243:1,16
243:18 245:2,3,12
247:14 252:15
260:18,19,20
261:1,4,11,19
262:1,2,13,14,22
263:5,11 265:3,21
265:22 267:1,2,8
267:9,22 268:18
269:13 270:1
271:4,5 272:9,16
272:21 273:7,11
274:10 277:13,14
277:15,17 278:10
278:12,13,21,22
279:3 281:4,9
282:11 284:7,17
284:18,20 285:3
286:11,17,18
287:2,3,15,21
288:4,22 289:5,12
289:18,19,21
290:9,16 294:2
295:15,21 296:8
296:13 297:1,11
297:12,13 298:9,9
298:19,20,21
299:15,18 300:3,6
302:7,22 303:15
303:16,17,20
304:20 305:7,8,12
307:17 310:6,10
310:13 311:1,4
313:14 320:17
323:5,6,14,15,17
325:1,2,3,6,8,10
325:12 326:3,10
326:11,12,22
327:7,9,22 328:1
331:10,20 332:3
332:19 333:5,12
335:2,5,6,7 336:8
337:4 338:22
339:1,8 340:3,19
341:11,12 342:17
348:1,2,13 350:5
350:17,19 351:18
352:20 353:16
354:5,6,9 356:5,6
356:10,12 357:9
357:10,11,18,19
359:7,8
**questioning** 54:2
82:13
**questions** 7:9 13:4
13:5,14,15 14:17
16:1 17:6,19
27:11 38:5 41:20
48:12 54:6 80:15
96:19 104:13
106:21 122:10
140:19 149:7
214:15 215:12
232:19 250:9
253:1 259:5,15
270:9 328:12
352:6 354:22
359:20 361:17,19
**quick** 29:21 156:18
201:18
**quicker** 151:16
**quickly** 252:14
**quite** 24:12 250:13
**quote** 107:17
124:21 191:12
195:6,15,22
197:15 200:16
204:2 212:4 215:7
**quoting** 127:11
179:11

**R**

**R** 8:1
**Rachel** 218:12
**Raise** 12:2
**Raj** 236:2
**Rajesh** 211:18
**range** 98:12
**ranging** 20:6
**read** 19:10 23:16
45:7,11,15 53:5,8
53:10 58:19 59:1
72:16,18 95:3
102:11,13 108:19
109:9 111:2
126:21 127:2,13
127:15 131:22
132:14,16 134:1
149:3 157:2
159:22 167:14,15
171:17,20 175:15
180:7,8 183:21,22
195:18 197:9,21
198:12 211:13,20
212:10 214:16
221:12 222:22
227:11 244:15
245:1,2 253:15
260:17,19 261:22
262:2,14 266:22
267:2,8 271:5
272:16 277:12,14
280:5,14 281:14
281:22 282:18
284:16,18 286:9
286:11,17,18
287:1,3 297:12
298:18,20 303:14
303:16 310:5,6
318:21 319:22
320:1,12 323:6,13
323:15 325:2,9,12
335:3,4,6 338:21
339:1 341:10,12
343:19 345:10,13
345:22 347:22
348:2,13 350:17
350:19 354:6
355:8 356:6 357:8

357:10,17,19 359:8 361:11
**readily** 20:17 160:1 160:4 185:16 187:17
**reading** 63:6 111:1 133:21 190:6 194:4 195:10 199:18 200:15 201:3 286:7 297:10 348:12 360:5
**real** 159:1 201:18
**realize** 14:10 209:18
**realized** 247:5
**really** 57:5 137:19 149:6 173:18 176:18 239:10 253:8 328:14
**realm** 20:6 112:2 198:17
**reason** 13:6,13 17:18 113:18 114:17 121:10 133:7 226:6 234:3 256:7 344:20,21
**reasonably** 233:9
**reasons** 101:15 112:16 114:9 136:1 341:15
**reauthorization** 169:21,22 308:5 322:5
**Rebecca** 1:12 2:2 5:3 9:15 12:6 361:10 363:5,17
**recalling** 14:19
**received** 38:11 39:9 135:13
**rechanged** 247:5
**recipients** 353:22
**recognize** 19:5 44:21 95:12 129:20 159:13 204:21 210:8 220:6 250:6 252:4 318:3,5
**Recognizing** 332:9
**recollection** 14:18 68:10 238:22 272:2
**recommendation** 126:22 127:11
**recommendations** 27:10 102:2,8 104:11 105:4
**record** 8:14,18 9:14 13:8,9 15:18 16:5 16:14,18 29:22 41:7 53:19,20 69:15 73:18 74:20 75:18,20 76:11 88:16 103:1 105:15 106:13 110:18,20 128:10 130:21 131:10 133:19 135:3 153:11 156:18,20 167:15 170:19 190:9 192:17 194:3 198:9,10 199:17 207:14,16 211:17 215:14 216:17,19,22 232:6,9,17 238:14 241:16,17 252:2 252:11 260:9,10 260:12,17 262:7,8 267:4,5,6 270:22 271:1 272:13,14 277:9,10 284:11 284:12,15 286:13 286:14 287:6,7 289:20 297:7,8 298:15,16 303:10 303:11,12 309:22 310:1,4 314:5,6 323:8,9,12 328:4 328:5 338:18,19 342:12,14 348:4,6 350:14,15 352:11 359:22 362:10
**recorded** 13:5 361:17,19
**Records** 31:21
**redact** 11:17
**redacted** 20:16 142:5 226:13
**redactions** 176:9 176:10,11,15
**reduced** 362:9
**REF** 363:5
**refer** 15:12 55:16 56:5,14 143:5 153:17 154:11 195:11 223:7,13 223:17 264:14
**referred** 24:13 198:3 211:14 225:12
**referring** 81:18 98:12,13 132:4 143:16 169:17 198:2 203:16 206:4 236:20 237:17,18 239:12 241:4
**refers** 57:9 348:17
**reflective** 177:16
**reflects** 107:12
**refresh** 68:9 78:1 238:21
**refreshing** 14:18
**refuse** 71:13 212:20
**refusing** 265:12
**regard** 135:14 139:12 224:11 238:9 240:11
**regarding** 6:4 105:1 210:12 269:12 354:22
**regulated** 34:4
**relate** 334:8
**related** 30:21 48:13 96:12 187:3 313:10 331:15 333:19 351:16 362:12
**relates** 26:22 131:1 142:21 174:18 193:15 233:19 310:18
**relating** 43:5 174:1 176:22 343:10
**relationship** 95:19
**relative** 362:14
**relatively** 135:5 141:17
**relaying** 222:11
**release** 6:18 11:17 175:11 318:6
**relevance** 35:14 38:21
**relevant** 17:11 114:10 138:6
**rely** 248:13
**remain** 101:5 107:5 342:5 352:17 353:11
**remainder** 115:5
**remains** 125:5 140:6 299:11 344:22
**remember** 58:9 97:13 101:4 142:1 247:12,22
**remind** 260:14 334:22
**reminder** 334:21
**repeat** 60:15 79:13 113:4 222:2,3 229:14,16 262:12 268:7,10 271:3 324:22 348:8,10 359:6
**repetition** 144:21
**rephrase** 103:15 115:6 151:21 160:11 175:18 186:17 216:4 223:3 296:18 302:21 303:3 356:16
**rephrasing** 186:9 296:16
**report** 5:13,17 20:8 20:9 25:2 95:16 95:20 96:18 97:12 98:8,17 99:7,18 100:11,20 101:6,7 101:16 102:1 104:5 105:21 106:16 108:1,2,18 109:15,21 120:15 120:16 128:4 130:4,19,20 131:3 131:9,13,17 132:22 134:20 135:3,10,13 136:2 136:7,15,18 137:10 138:7,15 138:18 139:13 140:10,13 141:15 142:12,15 143:10 144:15 145:3,4,6 192:3 198:18 209:13 219:4 273:2 299:10,12 312:19 325:14
**Reported** 1:20
**reporter** 11:19 12:2 53:10 102:13 111:2 127:15 132:16 134:1 157:2 167:15 171:20 180:8 183:22 197:21 198:12 245:2 260:19 262:2,14 267:2,8 271:5 272:16 277:14 279:14 284:18 286:11,18 287:3 297:12 298:20 303:16 310:6 312:5 323:6,15 325:2,12 331:2 335:6 339:1 341:12 348:2,13 350:19 354:6 356:6 357:10,19 359:8
**reporters** 240:6

**reporter's** 11:2,7 11:12
**reports** 25:9 26:1,2 26:15 120:21 142:7
**repository** 205:11 205:14 267:19
**represent** 96:3 103:1,4,21
**representation** 101:11 106:11
**representative** 18:20
**representatives** 168:17
**representing** 8:5 8:21 9:4
**request** 68:7 69:18 69:18 109:16 111:17 119:15 131:8
**requests** 30:4 73:13
**require** 117:15 192:6 194:9
**required** 43:4 194:13
**requirement** 32:12 308:5,16 322:6
**requires** 32:14 120:4
**reserve** 360:1
**reserved** 360:5
**resolved** 178:12
**resource** 207:6
**respect** 17:17 36:1 39:9 40:10 54:21 59:2 117:8 119:6 119:8,22 128:2 191:10 195:4,20 197:13 200:20 243:16,18 244:9 289:19
**respond** 76:5 87:10 186:3 202:22 221:21
**responded** 186:5
**responding** 10:6 62:9 222:5,12
**response** 6:7 16:11 16:16,21 30:18 45:16,17,21 46:5 46:6,7,12,13,15 50:10,19 52:9,11 54:3 55:15 57:6 57:21 58:16,18 60:20 61:11 64:5 67:3 69:18 70:2 71:12 74:13 75:3 75:5,6 77:16 78:2 78:6 85:20 86:15 86:20 87:19 88:1 88:12 101:1 109:16 110:9 111:18 116:17,22 117:3,10 123:20 123:20 125:14 155:2 161:11,13 162:5 186:4,20 190:5,16,19 192:11 195:15,17 196:5,18 197:6 200:11 203:2,6 204:1,15 220:9 232:20 240:1 254:11,14 268:13 269:12 271:8 294:5 296:8,22 298:8 299:5,15 309:8 325:20
**responses** 5:11 7:9 30:2 45:2 73:13 77:20 189:21 203:19,20 238:16 239:20 265:18 269:20 327:5 354:22
**responsibilities** 24:22 31:18 32:7
**responsible** 25:13
**responsive** 265:3 351:17
**rest** 136:18 341:14
**restarting** 307:8 308:16 309:5 313:19 322:1,11
**restate** 72:19,22 84:13,16 88:9 122:18 214:14 305:11 326:11,12
**restroom** 62:18
**result** 118:13 119:3 285:2 330:6,14 339:16
**resulting** 105:2
**results** 313:1,10
**resume** 53:21 62:21 75:21 110:21 128:11 133:20 153:13 156:21 190:11 198:11 207:17 216:20 232:10 241:18 258:3 260:13 262:9 267:7 271:2 272:15 277:11 284:13 286:15 287:8 297:9 298:17 303:13 310:2 314:7 317:14 323:10 328:6 338:20 342:15 348:7 350:16 352:12
**resuming** 315:1,10 316:21
**retain** 339:16 358:9
**retains** 357:3,22 358:8
**retention** 355:13
**reveal** 103:11 131:14
**revealed** 178:18 179:9,18
**revealing** 116:22 351:10,13
**review** 11:15 20:18 21:2 23:17,20 25:6 26:10,17 28:3,4,5,8 29:10 31:22 32:19 37:3 38:16 95:20 98:16 98:22 99:7,10,12 100:6,10 101:3,22 107:7 130:8,13 140:22 166:22 167:7 171:11 172:15 175:5,7 176:14 258:16 259:7 302:3,7 305:9 312:18 319:1 344:16 360:2
**reviewed** 20:4,12 20:15 21:9,10 22:9 23:8,14 32:1 46:13 63:18 96:22 96:22 97:1 98:7 99:18,21 100:4,6 100:15 137:2 142:5 232:11 249:6 252:13 253:7 284:21 338:10 344:13 346:19
**reviewing** 10:21 21:6 25:18 33:11 37:15 43:5,12,17 45:9,19,21 58:21 85:19 99:3 100:2 132:3 155:9 191:20 212:1 343:22
**reviews** 25:22 171:10 176:5
**revise** 39:20 191:21 191:22
**re-read** 77:15
**re-reading** 157:1
**re-remind** 140:8
**re-reminding** 140:15
**RFA** 74:13,17 76:19 77:3 109:16 109:17 111:17 117:3
**Richards** 1:12 2:2 5:3 8:2 9:13,15,16 12:1,6,12 42:4 44:19 45:10 51:15 63:2 76:3 84:7 104:17 129:18 153:8,16 159:11 159:18 190:13 210:5 214:5 217:2 220:4 229:3 250:5 258:7 279:15 361:10 363:5,17
**right** 12:2,15 14:13 14:14 18:20 39:11 43:20 48:10 52:6 54:20 55:6 70:2 80:12 97:8 99:19 99:22 103:16 106:9 135:7 136:2 144:4 154:2 155:14 175:18 177:18 190:9 191:3 213:8 215:2 233:22 310:3 335:16 344:3 345:4,13 347:19 348:18 349:7 359:19,20 360:1
**rise** 172:21
**risk** 248:20 314:9
**risks** 25:7
**Rodney** 4:3 8:20 9:17 29:5 41:1 51:14 53:13 84:2 103:1 129:9 146:4 187:1 241:11 270:6 294:7
**rodney.patton@...** 4:12
**Rogers** 30:3 45:4 119:7 120:2,12 315:17 316:2
**role** 21:22 26:2,6 27:4 45:20
**roles** 24:21 31:17 32:6
**roll** 217:13
**room** 351:15
**Rosemary** 6:17

**roughly** 141:8 217:13 271:21 316:4
**routed** 90:1,11,19 92:17 93:12 160:7 160:9 188:19
**rule** 91:5 92:2 360:1
**rules** 9:19 11:20 65:5 118:5 282:4 283:2
**runs** 101:18
**R-E-B-E-C-C-A** 9:16
**R-I-C-H-A-R-D-S** 9:16

**S**

**S** 8:1 30:3 134:10
**Safe** 34:2
**San** 3:14
**satisfy** 67:22 68:15 69:4,21 73:4
**save** 330:21
**saw** 343:2,4
**saying** 44:7 52:7 59:16 67:14 75:8 112:17 173:18 192:16 200:16 213:12 218:11 235:22 237:6 263:2 358:1
**says** 47:12 104:21 198:20 200:4 209:14 217:19,21 218:8 236:1 318:22 344:1,6 345:3,8,11 346:7 355:10
**scan** 196:9 259:21 261:8,15 263:12 263:17 266:5 270:15 274:9,17 300:21 302:15 303:5 305:13 306:2,22 328:15 329:3 344:2
**scanned** 263:3 266:16 267:16 272:11 273:8 300:13 304:14 324:19,21 325:18 326:2,17,19 334:16 335:15 336:1,16 337:11 337:22 345:17 346:5,12 347:5,17
**scanning** 196:8 263:6,8 271:11 274:5 300:1 301:10,19 305:3 322:17 324:8 325:16 346:8 347:4 348:17
**scans** 303:22 306:11
**scenarios** 16:7 17:2
**science** 35:9 36:14 36:21 40:11
**SCIF** 10:14 128:7 189:3 213:13,15 215:10 216:18 230:8 271:7
**scope** 30:22 83:20 84:4,20 86:11 87:9 89:4 90:5,22 91:16 94:2 102:15 118:3 165:9 168:10,20 170:16 171:22 172:12 173:12 179:2 224:15 242:6 243:4 245:13 247:14 248:12 250:8 253:1 255:10 256:18 257:1 277:16 282:11 283:12 285:16 286:20 307:10 308:19 315:5,15 317:4 319:15,17 321:18 322:3 337:5 342:20 345:19,20 348:22 349:11 352:21 358:15 359:5,17
**scratch** 185:19
**screened** 199:5 200:17
**screening** 195:6,22 196:9,16 197:4,15 200:10,13 201:2 244:8,18
**Screenshot** 7:4,5
**scrubbed** 141:6
**seals** 33:11
**second** 16:11 30:4 38:19 58:19 69:8 72:12,15 75:13 102:9 110:9 113:14 114:4 131:20 149:2 154:22 175:13 177:2 183:20 193:5 197:8 200:14,16 211:13 219:22 223:9 228:14 230:7 235:10 243:17 252:19 254:8 262:7 267:4 270:21 282:19 287:21 307:13 315:2,12 319:10 320:1 331:8 333:21 334:18 343:16 347:20 352:18
**seconds** 53:18
**secret** 351:19
**secrets** 15:7 40:17 41:2 116:3 119:6 120:5,11 121:2,10 121:22 123:12,21 125:13 126:13 129:5 145:21 155:3 161:3 163:20 164:13 180:11 194:22 196:21 232:21 258:21 273:15,16 273:22 274:12 281:6 282:13 283:13 285:4 290:11 302:9 307:19 324:2 328:19 331:22 332:16 333:14 339:9,20 340:14
**section** 5:14,18 6:5 6:19,21 7:10 24:3 24:7 28:17 32:14 95:17 96:21 98:8 98:11 100:11 106:6 130:6 131:1 131:9 141:7 199:2 206:6 210:14 218:5 221:14 233:12 313:3 318:8,20 319:5 320:4,15 355:1,12 355:13
**sections** 311:19
**Secure** 10:13
**security** 1:7 4:15 9:1,6,10 30:2 31:13 32:1,14,18 33:5 36:10,19 37:13,20,22 45:3 117:21 118:14 119:3,17 164:6,15 164:20 170:12 220:18,20 233:8 246:15 247:17 249:5 252:9 361:5 363:4
**Security's** 248:8
**see** 14:6 46:7 74:12 74:20 88:5 125:19 158:20,21,22 189:1 198:6 203:14 211:1 214:14 216:4 235:17 236:19 237:19 251:17 254:10 264:15 270:18 271:18 346:22
**seeing** 58:9 140:1 236:3
**seek** 215:13 268:15
**seeking** 120:3 167:2 180:10 280:17 302:8
**seeks** 118:1 123:2 134:3 165:4 191:14 303:18 323:18 340:13
**seen** 33:13 227:3,10 235:22 238:17 239:1 250:12 280:3,4 331:7,12 332:7,9 333:3,7 342:10,17,21 343:1
**Select** 316:11
**selector** 195:9 196:3 197:18 199:6 200:18 205:15 206:14,16 206:20 207:7,20 208:6 217:20 219:14 230:13,19 231:4,13,19,21 234:21 264:10 266:18 267:16 269:6,22 286:1 296:11 297:5 301:1 304:2 358:19,20 359:3 359:15
**selectors** 132:10 133:13 199:2 208:13 209:1,15 212:5,16,21 214:9 214:18 215:7 216:5 217:4 218:7 218:17,20,22 300:13,21 302:5 302:16 303:7 304:15 305:15 306:4,11 307:1 334:16 335:15 336:1,16 337:12

337:22
**Senate** 316:11
**senders** 353:22
**Senior** 25:5 31:12 246:16
**sense** 73:21 92:20 92:20 245:15 263:7 333:2 349:1 353:3
**sensors** 344:2 346:8
**sent** 46:9 90:1,11
**sentence** 100:16 108:19,22 109:3,8 109:14 110:4 111:10,15 112:7,8 113:7 114:13 115:9,9 117:9,10 119:14,21 124:11 124:16,18 131:18 131:22 132:4,7,19 133:9 134:8 137:2 139:3,6,19,22 159:22 160:10,12 160:17,22 185:14 187:15 188:13,22 189:9,17 194:5 198:20 199:21 200:3,15 201:3 204:16 211:12 212:3,4 215:20,21 219:2 221:12,17 221:20 222:4,9 226:3,7,7 250:21 280:14 312:17 319:6 344:5,8 345:8,10 348:9
**sentences** 106:20 107:6 108:7,9,14 138:22 139:9 343:20
**separate** 41:10 93:1,11 288:12
**September/Octo...** 316:6
**series** 250:9 253:1
**served** 19:14 338:11
**server** 160:9 231:18
**service** 46:20 47:21 48:4,14,16,19 51:1 52:20 55:6 66:16 67:6 126:8 127:12 128:15 132:8 133:10 134:12,13
**SERVICES** 363:1
**sessions** 97:10
**set** 19:19 25:1 34:7 48:12 54:6 77:20 92:6 93:1,14 157:13 189:22 225:20 249:2 309:6 321:10,17 322:13 341:15 355:13
**Sets** 30:4
**setting** 138:3,13 143:20 145:2
**Seven** 11:9
**shake** 13:9
**sheet** 361:18 363:1
**she'll** 69:11 238:22
**short** 41:1 53:15 133:17 318:21
**shorten** 41:6,7 69:14 84:3 273:18 324:2,4
**shortened** 146:5
**shortening** 129:10
**shorthand** 15:16 15:20 28:18 362:7
**show** 227:5 238:20
**shy** 31:16
**side** 239:17
**signature** 360:2,5 361:22
**signed** 171:14 239:19
**signing** 173:17
**similar** 74:12 140:18 154:3 158:6,13,14 212:9 288:4 299:18
**Similarly** 169:15
**simple** 241:11
**single** 26:10,11 83:9,13,15 84:17 86:5 91:10,15 254:5,21
**sit** 139:10 176:7
**sites** 287:17
**situation** 173:15
**Six** 11:5
**slight** 107:14,14 261:19
**slightly** 143:4 179:6 208:21
**small** 33:9 92:20 135:5
**smallest** 151:9,22 152:7
**society/non-gove...** 25:10
**solely** 100:5 296:10 297:4 300:22 320:7
**solidify** 251:3
**somebody** 65:6 73:3,7 75:1,4,9 85:11 178:3 229:22 288:13
**somewhat** 353:16 354:10
**sorry** 18:4,4 19:16 26:8 29:13 45:13 46:8 48:12 53:9 65:12 67:4,15 68:22 69:2 70:8 76:21 77:13,17 78:18 90:7 100:5 102:6 108:4 119:12 124:8 130:16 137:13 154:14 156:13 159:15 169:7,19 175:15,19,21 188:8,16 190:14 191:18,20,21 197:19 200:22 201:17 208:18 211:6 213:4 217:16,18 219:22 221:8,9 231:2 233:6 237:5,16 243:2 244:15,22 246:5 247:21 249:13 252:20 253:12 254:1 263:8 279:17,18 287:1,6 294:12 295:9 310:9 312:12 314:4 316:5,5 341:7,10 354:5 357:8 358:6
**sort** 37:7 47:11 50:2 54:17 57:19 63:7,8 80:19 91:6 105:7 111:12 161:19 173:15 235:19 238:2 247:3 257:9 261:4 261:6
**sorts** 16:3 33:4
**sound** 14:14
**sounded** 243:22
**sounds** 75:7
**source** 40:15 135:14 254:22 283:5,9
**sources** 101:12 121:14,14 126:12 127:19 140:5 145:20 164:2 241:6
**span** 83:9,15 84:17
**speak** 13:7 36:13 96:6 173:3 248:3 285:21 344:15
**speaking** 53:12 90:14 139:18 249:3 353:17 354:4
**speaks** 345:6
**special** 49:18,21 54:18 56:1,9 61:6 78:14 83:4 154:4 155:20 156:1 199:10 257:19
**specific** 17:9 26:15 27:11 29:2,14 35:18 41:11,19 47:12 49:16 66:7 71:8 78:11 86:4 98:12 101:19 108:7 114:20 143:16 153:19 154:18 157:21 161:21 169:2 173:3,14,15 178:1 180:5 187:3 228:3 245:16,19 248:6 253:6 257:5 260:3 349:3
**specifically** 13:22 26:11 104:21 117:8 119:18 120:19 177:18 194:1 217:15 225:12 238:9 243:19
**specificity** 193:16 319:20 344:16
**specifics** 199:12 248:3
**specified** 17:16
**specify** 128:2 296:17
**speculation** 135:18 166:9 168:20 173:11
**speculative** 285:17 285:20 286:20
**speed** 149:10
**spell** 9:14
**spelled** 159:17 211:3
**spelling** 8:14
**spend** 314:12
**spent** 328:9
**sphere** 71:8
**spoke** 120:13
**spot** 41:19
**SSCI** 316:11

**stamped** 221:7
**stand** 174:22 299:8
**standard** 177:11
**standards** 286:2
**start** 8:13 42:9 67:4 87:4 109:7 175:21 241:22 281:22 312:11 322:7 331:6
**started** 73:1
**starting** 140:10 198:20 312:16
**starts** 108:20 131:19 204:16
**state** 9:13 15:6,17 16:13,18 40:17 41:2 50:20 102:22 116:3 119:6 120:4 120:11 121:2,10 121:22 123:12,21 125:13 126:13 129:4 145:21 155:3 161:3 163:20 164:13 180:11 194:21 196:20 197:11 209:11 232:21 238:13 258:20 273:15,16,21 274:12 281:6 282:12 283:13 285:4 290:11 302:9 307:19 309:17 318:16 324:2 328:19 331:22 332:16 333:14 339:9,20 340:14 351:19
**stated** 18:12 115:19 126:2,3 194:1
**statement** 6:20 114:8 178:10 179:8,11,16,18,19 187:5 189:4 211:2 212:18 213:3 214:7,17 215:5 232:14 318:19 320:14 355:15
**statements** 137:8 178:17 221:1 339:3
**states** 1:1 5:19 6:15 66:17 67:16 103:5 103:21 104:1 124:18 163:4 214:18 228:13 230:2,12,17 231:3 231:18 233:9,10 234:8,20 273:4 319:2 320:2 361:1
**stating** 8:13 123:19 253:5 318:6,19
**stations** 78:5,22 79:6,16 80:2,17 81:7,12 83:10,16 84:18
**statute** 322:10
**statutes** 51:8 207:1 357:14
**statutorily** 134:4
**statutory** 41:3 71:21 111:7 116:3 118:20 122:1 123:13 124:14 126:14 127:20 129:6 145:22 155:3 156:4 161:3 162:8 174:7 180:11 194:22 196:21 201:7 202:1 204:7 205:18 208:2 217:9 219:17 222:19 224:3 228:19 232:22 234:10 242:14 245:5 254:15 258:21 260:22 262:17 266:10 268:20 269:9 270:3 272:19 273:13 274:12 281:7 282:13 283:14 285:5 290:1,11 294:4 299:1 300:5 302:9 303:19 305:18 307:19 308:15 310:12 311:3,15 314:1 317:6 322:22 323:19 324:2 325:5 326:5 327:2 328:20 331:22 332:16 333:14 335:9 337:16 339:9,20 340:14 347:8 350:2 352:2
**step** 39:7 241:14
**stood** 131:10
**stop** 10:6,11 313:6 319:4,8,13 320:18 321:12
**Stops** 6:18,21 318:7 318:20 320:14
**stored** 231:18
**stores** 206:5
**strategic** 26:9,14
**strategically** 66:2,9 66:14 67:7,16
**Street** 3:5,13 363:2
**strike** 102:6 127:7 305:11 352:8
**striking** 77:1
**student** 34:17
**study** 144:11,14
**subdivision** 62:3 151:9,22 152:7
**subdivisions** 61:21 62:6 82:1 150:3 150:10
**subject** 10:20,20 15:6 20:21,22 21:5,20 22:3 30:19 63:22 64:12 85:14 87:16 88:4 88:6 97:11 104:5 111:6 116:2 118:19 121:22 126:13 145:21 148:7,14 155:3 161:3 162:8 180:10 194:21 196:20 201:6,13 201:22 219:16 222:18 224:2 232:21,21 234:10 254:14 258:20 266:9 273:12,21 274:11 283:13 285:4,5 290:1,10 298:12 299:1 300:1,5 302:8 317:6 328:19 331:21 332:15 333:13 338:13 339:19 341:4 347:7 352:1 355:12
**subjected** 148:20 148:22 149:12,19 150:4,11,19 151:4 151:11,12 152:2,9 152:16 153:1 201:14
**submarine** 78:4,18 78:21 79:5,15 80:1 81:6,19,22 182:12,19
**submission** 28:9 29:11 175:1
**submissions** 20:10 23:9,21 143:2,6 166:16 167:1,9,19 175:3
**submitted** 20:4 131:6 220:16
**Subscribed** 363:18
**subsequent** 175:2
**subset** 218:6
**substance** 211:11 351:21
**substantially** 164:19
**substantive** 105:3
**substantively** 105:9
**suggest** 109:15,19 176:15 241:14
**suggested** 227:14
**Suite** 363:2
**sum** 81:1
**supervision** 362:9
**supplement** 14:12
**support** 6:14 165:14,21 249:18 279:16 280:8
**suppose** 93:17 143:14 231:16
**supposed** 166:1
**sure** 17:13,14 22:10 22:18 25:15,17 27:12,13 28:15 29:14,17,18 32:12 38:20 39:16 42:7 43:11 54:5 57:19 58:8,13 60:16,18 64:14 67:2,13 68:14 69:20 73:16 78:14,19 79:15 90:10 91:2,4 94:8 99:16 103:9,10 104:3 105:19 112:5 114:4 115:1 115:4 133:17 140:2 149:5 153:9 154:19 155:8,19 171:19 177:15 179:3 189:16 192:1 194:5 195:12,14 208:21 209:20 212:12 218:10 221:19 223:5 229:5 235:18 244:18 247:15 249:22 258:1 262:20,21 280:7,12 284:9 296:18 303:3 308:4 313:7 319:21 320:14 325:10 332:21 343:2 348:9 350:7 352:9 355:7 358:8 358:22
**Surely** 248:17

**surveillance** 5:14 5:15,18,20 6:5,6 6:16 14:21 17:4 24:4 25:14,19 27:5,19,20 28:10 28:16,19 29:8,9 29:12 32:4 35:5,7 35:11 37:1,11 38:10,15 39:10,14 40:13 43:12 44:1 51:3 95:16,18 107:22 109:11 112:21 113:12,21 115:14,22 117:12 120:1 121:18 122:21 123:8 124:19 125:15 126:10 127:10 130:6 132:5 133:4 135:7,16 136:14 137:9,11 138:6,17 139:13 141:19 142:14 143:11 144:8 145:5,16 146:12,20 147:6 147:14 148:1,7,14 148:21 149:1,13 149:20 150:5,12 150:19 151:4,12 151:13 152:2,9,17 153:2 160:20 162:16 163:15 165:5,6,13,14,16 166:1,17 167:2,3 167:8,11,20 168:6 168:14,16 170:4,5 171:12,13 172:7,8 172:10 173:8 174:2,4 179:17 180:3,17 181:3,11 181:19 182:6,11 182:18 183:5,12 183:18 184:6,13 185:1,7,21 186:12 187:19 191:11 195:4,20 197:13 200:21 201:13,20 202:11,19 206:14 206:17,20 207:8 207:21 208:7,14 208:15 209:2,3 210:13,15 214:11 216:6,7 219:11 220:12 228:10 229:20 230:1,9 232:3 233:13 234:17 236:15 238:8 240:11 242:4,11 244:11 244:20 245:19 247:7,8,9 258:16 259:6,20 261:15 266:17 268:17 270:14 271:14 272:11 274:5,8,16 275:2,8,14 276:2 276:10,17 280:18 280:20 281:2 282:7 283:4,8 284:5 286:7 288:7 290:8,19 298:13 300:2 312:9 320:5 322:16 324:8 328:17 329:5,13 329:21 330:7,15 331:16 333:20 334:9,17 335:16 336:2,17 337:13 338:1,14 339:17 340:10 341:5 347:4 349:6,21 350:8 351:4 355:21 356:19 357:5

**surveillances** 140:14

**surveilled** 286:7 288:6

**sustains** 32:15

**switch** 50:11

**sworn** 11:22 12:8 362:6 363:18

**system** 31:21 343:11

**systems** 31:22 37:7 345:12 346:14

**S's** 134:19

T

**Tab** 330:21

**take** 13:3 14:4,13 15:22 29:15,16 30:7,15,20,21 39:7 52:2,22 53:13 58:19 62:18 73:15 91:10,19 92:17 94:9 110:16 118:4 128:9 133:16 136:17 153:10 155:7 156:18 190:8 216:16 221:14 248:19 257:21 303:1 312:4 314:16 318:2,15 342:9 349:17 352:7,9 354:18

**taken** 17:5 62:20 93:11 153:12 177:12 190:10 258:2 361:12 362:4,7,13

**takes** 83:3,4

**talk** 29:16 30:18 42:12 43:18 63:9 63:22 64:4,17 85:14 87:16 108:9 110:2 156:15 213:13,15 286:12 289:6,7 323:7 350:11,13

**talked** 21:4 22:7

**talking** 17:9,13,15 29:1 43:22 63:6 128:3 135:4 144:4 185:15 213:9 217:15 218:19 223:14 265:7 306:13 320:21

**target** 192:7 194:10 228:12 229:22 230:1 231:1 234:7 267:17 304:3 320:8

**targeted** 196:12,13 285:22 358:19,19 359:3,15

**targeting** 196:14 232:12 233:2,8 285:1 286:2 321:10

**targets** 268:16 284:5 285:10 349:20 350:7 351:3 357:4 358:12

**task** 34:1 132:10 133:12 195:9 196:3 197:18 199:2,6 200:18 230:20 231:19,21 234:21 304:1

**tasked** 108:21 230:13

**tasking** 209:16

**TCP** 291:5,12

**Team** 25:5

**technical** 35:21 40:5 43:4 44:2 167:7 168:5 282:4 283:2 313:9

**technically** 42:17

**techniques** 86:22

**technological** 249:17 311:9 319:2

**technologists** 37:14

**technology** 32:15 32:19 37:4 251:2 251:8 253:6 320:4

**tele** 55:20

**teleco** 161:19

**telecom** 49:18 161:18

**telecommunicati...** 127:12 128:15

**telecommunicati...** 35:10 36:22 39:17 40:12 46:22 52:17 54:12,22 55:2,21 56:10,13 59:10,13 60:3,6 63:8 64:13 66:8 73:22 78:12 82:15 83:3 86:3 88:3,6,19 89:1,11 153:22 154:7 157:9,13 257:1,7

**telecom-like** 61:8

**TeleGeography** 74:14

**tell** 14:21 20:2 30:6 41:16 75:15 94:22 121:2 128:22 163:10 183:18 193:17 194:3,15 229:16 237:20 241:13 246:14 250:15 266:1 279:19 312:6 318:3 338:12 343:20 354:19

**temporally** 128:16

**temporary** 344:2,8 345:4,16 346:5,11 347:4

**ten** 31:16

**term** 15:11 41:13 41:13 46:17 47:12 50:1 54:9,21 55:2 55:15 56:4,14 57:6,7,22 58:1 59:3,9,22 60:2,12 60:18 61:10,20 62:9 63:3,10 64:1 64:18,22 65:7,22 66:1,3,14 67:8 78:6 85:15 86:9 86:18 87:18,22 88:11,18 91:14 153:16 154:6,7,10 154:20 160:21 161:20 162:3,4,15 163:13 164:5 185:18 186:18 190:22 191:11

193:1,12 195:5,21 197:14 199:8 200:22 224:11 225:8,15 226:18 227:16,19 245:10 255:6 256:20 257:19 271:13,17 286:5 288:4 319:13 339:19 341:8,21 353:12
**terminates** 162:17
**terms** 22:13 40:9 41:9 53:3 64:17 64:22 65:17 96:6 127:17 144:1,2 157:11 161:17 194:16 221:17 264:8 272:21,22 302:22 304:4
**terrestrial** 49:8,15
**territory** 236:21
**test** 267:16
**testified** 12:9 88:16 315:17 347:15 348:16
**testify** 19:21 210:16
**testifying** 83:21 84:6,7 210:19
**testimony** 10:17 12:13 18:15 46:22 47:10 48:6,21 49:7 51:5 53:3 56:18 58:6 59:13 60:6 61:1,15 62:11 66:5,19 67:10 68:4,19 69:7 73:19 76:11 78:9 79:10,19 81:9,10 82:4,22 83:12 84:20 86:11 87:8 89:4 90:5,21 91:16 94:1,20 96:17 97:6,11,18 100:7 110:8 111:4 112:12 117:14 120:18 157:4 158:8 228:1 264:3 304:19 316:3,10 316:17,18 327:6 337:5 338:9,12 348:21 351:22 362:5,6,10
**testing** 343:10
**text** 195:17 219:13
**text-based** 322:18 324:9,18 326:15
**thank** 11:21 209:22 232:8 261:14 266:4 269:18 270:10 280:10 299:18 316:14 318:9 328:3,11,13 343:15 348:5 355:3 359:19
**thanks** 29:4 31:2 84:9 133:18 232:7 270:7 296:19 348:12
**thereto** 362:16
**thing** 42:1 134:9 186:10 209:11 236:2 244:22
**things** 29:21 47:15 53:9 143:4 170:13 170:17 225:9 287:12 294:8 304:6 353:18
**think** 8:7 9:11 14:6 14:17 17:18 28:6 30:13,14 33:16 39:19 40:1 41:15 42:4 43:2 52:3 53:11,14 54:20 67:13 69:20 70:20 72:14 73:1 74:16 82:9,10 90:17 94:10 104:14 105:18 108:8 114:18 143:22 144:5,10,11,22 146:4 157:8 171:18 172:14 173:13 176:16 177:8 186:22 187:2 189:8 198:15 204:3,14 212:9 213:4,18 217:22 219:7 225:7,19,20 226:2 226:16 230:5 238:20 241:2 250:22 255:20 260:4 261:3 303:9 332:10 347:15 353:17
**thinks** 314:16
**third** 16:15 355:8
**thorough** 100:11 130:13 175:7
**thought** 135:18
**thoughtful** 173:20
**threat** 316:7
**three** 10:10 16:7 17:1 33:16 37:2 157:13,20 339:17 340:11 341:6
**throwing** 52:4
**tied** 101:14
**time** 10:5,12 15:22 17:11,13,15 23:11 29:15 30:15,20 33:10 34:16,20 36:6 37:12 38:12 38:16 39:10 40:8 46:2 51:15 53:9 57:19 68:13 69:3 69:14 79:11 98:20 109:7 115:12 125:1,4 127:17 128:2 129:2 134:3 134:16,16 135:2 136:14 137:9,22 138:7,17 141:15 142:11,14 145:6 153:7 160:12 166:12 168:22 169:2 174:6 186:6 186:9 187:3 197:20 211:16 213:15 215:7 235:7 238:3 240:17,21 250:13 287:2 289:4 290:17 296:13,17 314:9 316:4 325:10 330:22 334:15 335:22 336:8 337:15 338:3,14 348:9 354:5 355:16 356:3,8,21 357:18 362:7
**times** 88:16 97:15 137:20 235:22
**timing** 142:9
**tired** 345:20
**title** 280:5 320:12
**titled** 279:15
**today** 12:13 14:22 17:20 18:10,19 19:17,21 65:19 75:3 111:20 115:22 117:12 120:1 139:10 146:12 147:6 148:1,14 149:1,13 150:5,19 151:13 152:2 153:2 181:3 182:6 183:11 184:6 185:8 186:1 186:8 191:1 196:12 202:9 257:9 266:5 268:15 269:21 274:9,17 275:9 276:3,18 284:5 290:6 291:3,17 292:9 293:2 299:11,20 300:10 307:8 322:16 324:17 325:22 326:14 328:12 338:12 345:1 349:20 350:7 351:15,21 357:3
**today's** 20:20 120:18
**tomorrow** 309:15
**Toomey** 3:19 5:5 8:9 258:6,11,12 259:3,19 260:10 260:16 261:13 263:10,19 264:7 265:1,9,11 266:3 266:14 267:5,20 268:9 269:2,17 270:13 271:3,12 273:6 274:3,15 275:1,7,13 276:1 276:9,16 277:2,12 278:1,18 279:9,13 280:1 281:12,21 282:17 283:18 284:3,14 285:9 286:4,16 288:3,20 289:15 290:5,15 291:2,9,16 292:1 292:8,14 293:1,9 293:17 294:7,12 295:11,19 296:6 296:18,20 297:20 298:18 299:13 300:8,19 301:8,16 302:2,13,18 303:3 303:4,11,14 304:9 305:4 306:1,9,15 306:20 307:6 308:2,14 309:3,16 310:3,21 311:11 311:21 312:3 313:5,16 314:18 315:8 316:1 317:12,19 318:1 318:14 319:18 320:11 321:1,13 321:21 322:9,15 323:11 324:1,6,16 325:19 326:9 327:12 328:3 352:7,14 353:8,20 354:13,17 356:15 357:2 358:5,21 359:12,19
**top** 91:1 199:18

209:14 251:16 281:15
**topic** 38:11 65:1 104:4 279:8
**topics** 19:9,18,22 35:18 36:2,6,14 36:20,20 38:1
**total** 81:1 221:13
**Trade** 34:5
**traditionally** 349:2
**traffic** 227:17 344:2 345:16 346:5,12
**training** 35:8,18,22 36:1,13,18 38:12 39:9,21 40:5,10
**transaction** 160:6 188:14,18 202:9 202:19 254:5,21 255:15 257:5,12 264:10 266:15 267:15 269:5,22 300:13 302:22 304:1,3 305:2 306:11 358:3
**transactions** 195:8 196:2,10 197:17 199:1,3,5,6 200:4 200:5,17 201:12 201:20 204:2,19 205:6 230:10 234:19 238:10 240:12 253:21,22 254:1,2 261:9 263:4 303:7 304:14 305:14 306:4 307:1 340:3 340:19 341:4,8,21 342:4 347:5,18 355:11 356:11,18 358:10,13,18 359:11,14
**transcribe** 13:8
**transcribed** 212:19 214:7 217:3 338:10
**transcript** 6:4 10:21 11:1,6,9,15 11:18 211:1 361:12
**transcription** 361:16,19
**transfer** 34:6
**transferred** 11:3,6
**transit** 258:17 259:8,22 261:12 261:17 263:13,18 266:7
**transiting** 124:20
**transmission** 46:19 47:19 48:3,13,18 49:4 50:2,22 52:18 55:4,16 56:5,6,14,15 57:8 57:12 58:2,3 59:3 59:4,7,9,22 60:12 60:19 61:9,10 62:8,16 67:22 68:15,21 69:3,21 73:4 80:16 93:3 219:13
**transmit** 55:19
**transmitted** 11:11 57:1 353:6
**transmitting** 57:10 57:11 81:13
**transparency** 24:17 25:4,8 32:22
**TRANSPERFECT** 363:1
**Transportation** 34:6
**transported** 242:21 243:10 244:3
**traverse** 87:5 93:18
**traversing** 91:12 94:15,16 246:9
**treat** 178:17 179:8
**trick** 16:1
**tried** 144:20 239:21
**tripping** 57:17 58:9 216:12
**trolled** 287:19
**true** 61:4 89:21,22 90:10 97:21 98:3 107:14 112:7 124:17 127:9 140:7 160:10,12 166:17 189:9 214:22 215:6,6 251:7 299:11 344:22 354:11 357:1 358:4 361:16,18 362:10
**TRUSTe** 33:10,21
**trusted** 33:14
**truthfully** 18:6
**try** 13:16 23:19 27:16 35:22 52:10 52:13 69:19 80:13 86:17 87:3 93:9 141:10 186:9 270:6 294:8
**trying** 27:14 57:5,8 57:15 58:1 75:1,8 75:14 82:9 114:5 114:12 115:5 129:11 156:10 158:15 193:3 196:15 206:2 212:12,15 213:1 214:1 227:13 238:15 254:10 273:18
**turn** 45:6,14 58:12 58:15 77:12 108:17 126:20 131:16 159:21 210:22 221:10 250:19 280:10 281:13 309:14 343:15 355:6
**turning** 203:5 221:5 332:7
**turns** 47:12
**two** 10:4 29:20 33:18,20 41:3 54:18 58:20 76:12 77:15 78:5,18,22 79:6,16 80:1,17 81:7,12 83:10,16 84:18 93:17 94:5 94:6,8 112:1 119:16 149:10 157:8,17 162:6 190:5 211:20 214:14 288:12 309:19 311:6 317:4 343:19
**twofold** 317:3
**two-part** 261:4
**two-thirds** 250:20
**two-year** 355:13
**type** 27:1 169:14 218:17 308:8,10 308:12 353:4
**types** 26:12 27:2 37:4 50:13 218:19 218:22 247:3
**typewriting** 362:9

**U**

**Uh-uh** 254:12 255:21
**ultimately** 206:5
**ultra-high** 46:18 47:19 48:2,17 50:21 55:4 62:15
**unable** 43:6 44:2
**unauthorized** 10:1 10:8,15
**unclassified** 16:17 16:19,21 20:6,15 21:10 22:7,10,17 30:8,11 40:9,20 40:22 41:8,19 50:19 52:9,10 54:7 71:3,6 73:21 74:21 76:17 85:7 89:13 97:19 98:2 98:6 106:12 107:5 108:12 110:13 111:9 121:9 122:11 124:16 127:22 131:10 133:18 134:7 135:5 136:20 137:16 139:22 141:11 144:1,2 155:5 156:7 161:11,12,15 163:11 164:1 174:10 186:4,20 191:6,8 192:15 194:16 198:17 203:2,6,10,15 204:8 205:20 213:19 214:3 216:10,15 217:11 219:1 221:17 222:21 227:4 228:21 229:2,6 230:5 239:13,21 240:19 241:9 247:15,18,19 248:1,15,18 250:10 254:11 259:13 261:2,5 262:5,19 264:8,13 264:20 265:17 267:13 268:2,5 269:12,15 271:8 272:21 273:1 285:2,19 287:14 294:5,10,15,18 295:5,13 296:21 297:21 298:1,7 299:4,19 300:9 303:21 304:8,21 307:20 309:10 310:14 311:5,6,17 314:2 317:8 325:7 325:21 326:13 327:13,15 343:12 349:14 350:10 357:15
**unclear** 170:19
**underlying** 310:18 310:22
**undersea** 49:9,15
**understand** 12:12 12:17 13:13,14,16 13:17 14:1 15:20 17:1 18:18 29:13

32:20 33:1 37:14 40:4 43:6,8 44:7 46:15 50:18 55:22 57:5,9,14,15 58:1 59:2 64:21 65:4 65:15 67:13 71:11 74:2,6 75:9 76:3 76:16 83:17 84:5 84:10 87:3 93:9 99:16 104:2 112:5 114:13 115:1,2,5 120:16 127:7 133:9 135:2,12 139:4 158:15 160:19 162:2 179:4 187:15 188:13 193:4 196:5,15 204:15 206:2 211:4,5 212:2,15 213:1,22 214:5 217:14 219:7 223:6,17 224:10 225:4,11 225:14,15 230:3,4 233:19 236:20 241:10 253:8 271:16 319:21
**understanding** 22:11,21 27:13 37:5 38:6 46:17 47:18 50:1 52:16 56:12 57:11 63:3 64:14 65:7,17,18 72:7 81:3 86:8,18 86:21 90:15 111:20 154:5,6 155:17,18 157:16 161:20 162:3,14 163:2 164:5 190:21 199:7 262:22
**understands** 89:10 218:11
**understood** 37:6 54:10,22 59:10 60:12,16 63:19 64:11 67:2 88:19 88:22 105:11 114:4 157:12 170:21 173:22 192:20 205:1 206:13 212:20 253:11 255:16 257:6 266:4 349:2 359:1
**undoubtedly** 82:15 354:11
**unencrypted** 352:17 353:11 354:1
**uniform** 207:6
**Union** 8:9,12 258:14
**unit** 338:14 339:15
**United** 1:1 5:19 6:15 66:17 67:16 103:5,21 104:1 163:4 228:13 230:2,12,17 231:3 231:18 233:10 234:8,20 319:2 361:1
**University** 8:4
**unofficial** 241:6
**unpack** 261:5 287:13,14
**unrelated** 21:8
**untrue** 354:12
**upstream** 6:21 14:21 22:2,11,20 25:14,18 27:5,19 29:2,8 32:4 35:5,6 40:16 51:2 54:15 101:4,11 107:17 107:22 108:13 109:11 110:2 111:12,19 112:21 113:12,20 115:14 115:22 117:6,11 119:22 121:18 122:21 123:8 124:18 125:15 126:9 127:10 132:4 133:4 134:13 135:7,16 136:14 137:9,11 138:6,16 139:13 139:21 141:18 142:14 143:11 144:8 145:5,5,16 146:12,20 147:5 147:14 148:1,7,14 148:20 149:1,12 149:19 150:4,12 150:19 151:4,11 151:13 152:2,9,17 153:2 165:6,14,16 167:3,8 168:6,15 169:7,8 170:5 171:13 172:7 174:2 179:17 180:2,16 181:2,10 181:19 182:6,11 182:18 183:5,12 183:17 184:6,13 184:22 185:7,21 186:12 187:19 191:10 195:4,7,20 196:1 197:13,16 200:20 201:13,20 202:10,19 204:17 206:14,17,20 207:7,21 208:7,13 209:1,16 212:6,17 212:22 214:10,19 215:9 216:7 217:6 218:5,6 219:11 221:14 222:1,6 224:1 228:10 229:19 230:1,8 232:2 234:17 235:9 236:15 238:8 240:11 242:4,11 244:10 244:11,19 245:19 253:19 258:16 259:6,20 261:8,15 263:3 266:16 268:17 270:14 272:10 274:4,8,16 275:2,8,14 276:2 276:10,17 282:6 283:4 284:5 286:7 287:22 288:7,18 290:8,18 294:22 298:12 300:1 313:2,11 318:20 320:6,15 322:16 324:7 328:16 329:4,12,20 330:6 330:14 331:16 333:20 334:9,16 335:16 336:1,16 337:12 338:1,14 339:16 340:10 341:5 347:3,18 349:3,6,21 350:8 351:4 355:20 356:19 357:5 358:10
**URL** 207:6,20 208:6
**USA** 169:18,19 177:11,14
**use** 15:11 39:16 56:13 62:18 64:13 66:1 86:22 158:21 158:22 160:20 186:18 191:12 193:2,12 195:6,22 196:16 197:4,15 200:2,10,12 227:19 228:7 257:16 271:13 291:5 339:15 341:7 343:10 359:9,10
**uses** 57:22
**utilized** 204:17
**U.S** 4:5 230:16,18 284:6 312:22
**U.S.C** 15:8,9 40:18 40:18

**V**

**v** 363:4
**vague** 23:10 25:20 27:6 28:11,22 36:7 38:22 44:5 46:1 50:4 56:18 64:9 79:9 83:11 85:22 95:22 96:15 98:20 100:12,21 106:3,18 109:5 110:3 115:11 121:4 125:1,3 130:15 134:2 135:8 136:9,21 137:4 138:19 141:4,21 142:16 143:13 153:18 154:12 165:8 168:1,9 174:5 176:2 193:7 198:13 212:7 220:17 225:7 227:1 228:16 236:9 296:13 302:6 308:19 321:16,19 337:14 338:3 339:18 340:12 341:13 349:10 353:13,16 354:10 356:2,7,20 358:14
**vagueness** 91:14 127:17 216:9 223:12 308:1 319:13 340:5,21 342:2
**value** 283:1,21
**various** 13:20 99:2
**verdict** 76:9
**verification** 23:1 312:20
**verified** 220:20,22 221:1
**verify** 166:15
**versed** 42:17
**version** 146:6 221:9 232:13
**versions** 20:16,16 21:9 144:20
**versus** 12:14 22:13 30:8 48:8 83:3

193:4 257:10
**view** 123:19 124:11 125:12
**viewing** 231:17
**violating** 240:2
**virtual** 56:22 57:22 58:3,8,9 59:5 86:9 86:19 87:4,5,18 87:22 88:11,18,21 89:10
**visit** 231:7
**volume** 221:22 222:6 338:13,15 340:9 341:3
**VPN** 291:18 292:3 292:10,16 293:3 293:12 337:11,21
**vs** 1:6 361:4

**W**

**wait** 65:11 75:13 208:18
**waiting** 304:16
**waive** 103:8
**waiver** 10:19
**walk** 106:22 139:4 140:1 287:13
**want** 19:10 26:5 29:2,20 47:11 52:10 53:13 57:16 58:7,13,19 65:21 73:17 78:14,19 79:13 95:2 96:8 102:22 106:7 108:17 131:17 139:20 144:19 153:20 155:19 158:2 170:19 171:18 173:19 177:15 185:13 188:4 189:13 213:17 215:13 216:14 234:3 235:17 238:13,17 241:8 260:6 262:21 264:14 286:12 287:13 311:19 316:4 328:10,13 338:15 339:15 344:18
**wanted** 40:4 72:18 131:9 209:19 261:5
**wanting** 239:2
**warm** 177:5
**Washington** 1:14 2:7 4:9
**wasn't** 22:21 23:3 178:6 235:19 265:21
**water** 14:6
**wavelength** 61:21 62:6 93:4
**wavelengths** 61:12 150:17 151:2
**way** 14:13 32:4 35:4 39:12 52:11 52:14 54:5,7,15 86:21 115:7 117:5 126:5 167:8 173:3 177:11 179:7 186:2,17 214:2 215:4 223:14 238:1 241:14 250:20 294:22 344:19 346:21
**ways** 25:7 51:22 57:10,11 97:16 107:9 144:21 202:7,17 353:18
**web** 221:14 222:14 223:6,7,8,19,20 224:11 225:4,13 225:20,22 226:19 227:3,15 228:8 231:18
**webmail** 235:8 236:16 238:6 240:9 242:4,10
**website** 20:17 176:7 219:13,14 228:13 230:2,12 230:13,17,18,19 231:3,4,6,8,9,14 231:17,17,20,21 234:8,20,20 244:3 284:6 295:6
**websites** 33:12,13 282:22 283:20 286:8 287:20 288:8
**weeks** 227:11
**welcome** 68:9
**well-known** 61:8
**went** 34:16 76:4 97:15 105:9,16 178:7,11 236:2
**West** 3:5
**we'll** 13:4 14:3,13 74:19 75:18 211:12 281:21
**we're** 9:11 17:9,13 17:14,15 26:16 27:8 29:1 39:2 53:15 75:14 77:17 102:19 103:11 104:14 134:10 135:4 140:2 153:15 173:17 196:8,8 207:19 211:6 213:9 216:22 238:3 254:10 260:6,16 263:8 265:7 273:19 305:2
**we've** 53:22 55:21 112:7 124:11 126:2,2 134:12 137:21,21 140:16 187:15 203:19 227:11 235:22 251:18 261:7 264:16 327:17
**wholly** 110:13 160:5 188:16,17 196:7 202:9,20 204:2,18 205:3,16 325:17
**Wide** 223:7,8 225:13,22
**Wiegmann** 217:19
**Wiki** 159:17
**Wikimedia** 1:4 8:5 12:14 258:5,13 276:19 277:5 278:5,20 283:6,10 285:11 287:17,20 329:3,11,19 330:5 330:14 361:3 363:4
**Wikimedia's** 275:16 276:4,12 279:1 282:22 283:20 286:8 288:8 293:3,11 328:15 331:18 334:1
**willing** 115:3 248:19 346:20
**wire** 56:16
**withdraw** 30:14 151:17
**witness** 2:3 5:2 9:15 10:5,11,18 12:4,7 18:2 25:22 27:7 28:13 29:16 34:13,15 35:17 36:8 38:18,22 39:2 40:19 41:9 42:21 43:8,15 44:6 45:9,19 46:3 47:2 48:7,22 49:8 49:14 50:6 51:9 53:8,11 55:10,19 56:8,20 58:7,21 59:15 60:8,15 61:2,17 62:3,12 63:17 64:10 65:12 66:6,20 67:12 68:6,20 69:17 70:3,20 71:2,5,22 72:14,18 75:11,16 76:15 77:5 78:10 79:3,11,20 80:5 81:11 82:5,14 83:1,13,21 84:8 84:11,22 85:8 86:1,13 87:10 89:14,16 90:7,14 91:1,18 92:7,15 93:15 94:3,5,12 96:16 98:21 100:13,22 104:13 106:4,19 108:6 111:10 112:13 113:3,16 114:2 115:15 116:4 119:11 120:8 121:5 122:4,16 123:5,14,16 124:2 125:5,19 126:2,15 126:17 127:5,21 128:6,13 129:5,7 130:16 132:3 134:8 135:9,20 136:10,22 137:5 137:15 138:11,20 139:16 141:5,22 142:17 143:14 144:2,10 145:9 146:1,2,15 147:1 147:9,18 148:4,11 148:17 149:16 150:1,8,15,22 151:7 152:5,13,20 153:5,19 154:14 155:5,7,9 156:6,9 156:17 157:5,19 158:11,20 160:16 161:5,12,16 162:9 162:11,21 163:8 163:17 164:2,9,14 165:1,10,18 166:4 166:10,20 167:5 167:16 168:2,11 168:22 169:10 170:14 171:1 172:2,14 173:2,13 174:9,11 176:3 177:7 179:3,22 180:12,14,21 181:7,15 182:1,9 182:15 183:1,8,15 184:3,11,18 185:4 185:11 188:9,11

189:13 193:9
194:20 195:1,2
196:22 197:1
198:1,15 201:8,9
202:4 204:9,10
205:9,21 206:9
207:2,3,11 208:3
208:4,10,18 209:6
209:10 212:1,9
213:10,21 215:18
215:20 216:1,12
217:12 219:19
220:18 222:20,22
223:13 224:5,7,15
224:22 225:7,19
226:16 227:2
228:2 231:13
232:11 233:1
234:12,14 235:2
235:12 236:18
237:16 238:14,18
239:16 240:22
241:2,12,19 242:7
242:8,15,16 243:6
243:13 244:6
245:6,7,15 246:4
246:11 247:17,18
248:13 249:3,13
249:20 250:8,12
251:12 252:20
253:2,4,15 254:12
254:16,17 255:3
255:12,21 256:4
257:3 258:22
259:1,12,17 261:1
261:3 262:3,12,18
262:20 263:16
264:5,13,14
265:10 266:11,12
267:12,14 268:2,4
268:6,21,22
269:11,14 270:4,5
270:11 271:9
272:20,22 273:12
273:14 274:1,13
274:14,21 275:6
275:12,20 276:8
276:15,22 277:17
277:19 278:8,12
278:15 279:7
281:8,10 282:14
282:15 283:15,16
284:2,10,21 285:6
285:7,17,20
286:21 287:1,5,11
288:11 289:5
290:2,3,13,22
291:8,15,21 292:7
292:13,20 293:7
293:15 294:6,9,21
295:9,18 296:5
297:17 299:3,6
300:6,7,17 301:6
301:14,22 302:10
302:11 303:20,22
304:19 305:1,18
305:20 306:7,18
307:4,12,21
308:12,21 309:1,8
309:12 310:5,7,13
310:15 311:4,6,16
311:18 312:14
313:14,15 314:3,4
314:8 315:5,7,15
315:17 317:7,9,18
319:19 320:20
321:8,20 322:4,14
323:1,2,20,21
324:14 325:6,9,13
326:7 327:4,10
328:2,21,22 329:8
329:16 330:2,10
330:18 331:11,13
332:2,4,13,18,20
333:6,9,15,16
334:5,12,22 335:4
335:10,11,19
336:5,12,20 337:6
337:8,17,18 338:5
339:7,11,22 340:6
340:16,22 341:17
342:20 343:1,8,22
344:5,12 345:7,22
346:7,17 347:8,10
348:3,8,14,22
349:1,13,16 350:4
350:10,12,22
351:7 352:3,4,22
353:3,14,15 354:4
354:9 356:3,4,9
356:22 357:16,17
357:22 358:16,17
359:5,6,9,18
360:2 362:4,6,11
363:5
**witness's** 76:13
177:15 203:4
241:7 296:3
297:15
**word** 47:11 58:17
83:4 106:9 113:9
125:9 136:18
146:8 157:13
159:4 218:2 228:8
245:16 359:9,10
**words** 48:15 50:12
61:8 66:6 71:15
116:12 136:19
142:19,22 143:1
157:13,20 161:17
179:15,16 195:12
212:10 257:17,18
346:1,3
**work** 16:4 22:19
25:8 37:7,11 41:5
43:19 55:22 171:5
248:22 346:18
**worked** 22:11 33:9
33:22 37:18
105:11 106:7,10
131:11
**working** 33:21 36:9
36:11 177:21,22
343:3
**works** 101:11
111:20 117:6
133:1 193:11
198:16 282:5
299:9
**world** 223:7,8
225:12,21 239:7
245:17 257:11
**worried** 244:1
**wouldn't** 49:1
82:10 205:5
285:21 331:17,18
333:21 334:2
**written** 63:7
137:20 189:4,9
221:17 357:1
**wrong** 73:10 94:18
158:6 347:16
**wrote** 135:9 299:12
**W-I-K-I** 159:18

**X**

**x** 1:3,9 239:14
330:21,22 361:2,7

**Y**

**Y** 239:14 330:22
**yeah** 8:19 18:2 19:7
34:22 43:11 44:11
53:8 58:21 59:4
69:2 72:19 79:1
82:14 99:17 124:8
127:4 144:5 159:5
169:15 188:11
203:20 229:18
231:7,10 246:11
253:14 272:3
309:2 343:22
348:5 351:11
**year** 34:15,21
**years** 22:20 24:12
24:20 25:1 31:5
31:16 33:16 130:7
140:14 169:12
253:7 339:17
340:11 341:6
344:15
**Yep** 112:6
**yes-or-no** 122:10
189:5
**York** 3:7,7 363:2,2

**Z**

**Z** 239:14

**#**

**#903** 363:2

**0**

**00149** 5:21
**00229** 5:21
**00234** 6:8
**00277** 6:8

**1**

**1** 69:19 74:13,17
344:14
**1st** 175:1
**1:15-cv-00662-T...**
1:6 361:5
**10** 195:16
**10:02** 53:20
**10:05** 53:21
**10:06** 348:6
**10:11** 348:7
**10:14** 350:15,16
**10:15** 62:20
**10:16** 352:11
**10:25** 62:21
**10:26** 352:12
**10:36** 360:3
**10:38** 75:20
**10:47** 75:21
**10017** 363:2
**10027** 3:7
**101** 3:13
**103** 273:3
**11** 5:4 280:11
361:11
**11:30** 110:20
**11:56** 110:21
**116th** 3:5
**12** 45:8,12,17,22
55:15 57:7 60:20
61:12 62:9 64:6
70:2 126:20 127:1
281:13 282:19
**12:16** 128:10
**12:19** 128:11
**12:26** 133:19
**12:40** 133:20
**12:59** 153:12

**128** 5:18
**14** 312:11,16 362:22
**149** 159:17
**15** 312:11
**15th** 355:2,17
**158** 5:21
**16** 1:13 5:16 98:14 132:5,20 133:5 141:7 361:13 363:4
**16th** 130:6 132:11 133:13 193:22
**17** 45:6,12 211:1,7 211:8,21 218:16
**18** 5:10 45:14
**19** 6:4,11 210:15
**19th** 252:10
**191-page** 108:10
**193** 159:22
**1978** 233:13

**2**

**2** 5:13 7:6 19:18 58:16 65:1 69:19 78:7 85:21 86:15 86:20 87:19 88:2 88:13 246:22 247:10 248:1 344:14 345:15 346:4,11
**2nd** 95:18 107:22 109:12 128:3
**2.0** 343:11,17 344:1 345:11
**2:06** 153:13
**2:11** 156:20
**2:28** 156:21
**20** 2:7 4:8 211:1,7,8 211:21 218:17 363:19
**2002** 32:13
**2009** 7:7 343:13
**2010** 251:15 253:5 253:9
**2011** 5:19 6:8 7:10 159:20 174:3,12 186:9,11 187:18 188:15 189:5,10 189:18 220:10 355:1,2,17 356:22 357:1
**2013** 6:11 177:22 240:6,14 252:10 253:10
**2014** 5:13,16 6:4 95:18 107:13,22 109:12 111:15 112:10 115:14 120:22 121:17 122:20 123:7 125:2,14 126:7 127:10 128:3 130:7 132:5,11,20 133:5,13 140:7 143:12 193:22 210:15 215:6 217:3 233:14 299:11
**2015** 17:5 145:18 146:20 147:15 148:8,21 149:20 150:12 151:4,12 152:10,17 180:18 181:12,20 182:20 183:5 184:13 185:1,22 186:8 190:22 191:11,16 193:1,15 195:5,21 196:11 197:14 200:21 201:13 202:8,15,18 205:16 208:7,15 209:3 216:6 219:10 228:11 229:20 230:9 232:4 234:6,18 244:12,20 259:4,7 259:21 261:10,14 262:19 263:3,11 263:17 264:8 265:8,10 266:15 269:4 270:15 272:10 273:8 275:3,15 276:11 290:16 291:10 292:2,15 293:10 324:7 326:10,15 329:3,19 330:13 335:14 336:8 337:21 347:3,16 349:6 351:3
**2016** 312:17
**2017** 6:15,18,20 107:8 140:10 202:15 293:21 294:21,21 295:4,7 295:10 297:3 298:11 299:22 300:14,20 301:9 301:17 302:3,18 303:5 304:15 305:5,6,9,13 306:2,14,15,21 310:19 311:7,18 312:10 316:5,6 318:6,19 320:16 321:15,17
**2018** 1:13 6:13 280:9 316:5 361:13 363:4
**202** 4:10,11
**2020** 362:22
**20530** 4:9
**209** 6:6
**21st** 240:5,14
**212** 3:8 363:3
**21368** 1:22 363:5
**216** 363:2
**219** 6:8
**222** 32:14
**229** 159:17
**234** 221:9
**237** 221:8
**239** 361:11
**249** 6:10
**250** 6:12
**257** 5:5
**26** 6:13,15 280:9 312:10,17
**266** 221:11
**277** 221:9
**278** 6:14
**28** 6:18,20 271:20 318:6
**28th** 318:19 320:16

**3**

**3** 5:19 6:11 19:18 98:14 99:8,18 190:17 192:12 196:18 197:6 198:4 204:1 247:1 248:6,9 249:1,8 249:17 250:19 251:1,7,17 252:9 260:7 264:19 265:18
**3rd** 159:20 174:3 174:12 186:11 187:18 188:15 189:5,10,18
**3(b)(5)(b)(4)** 355:12
**3(c)** 355:13
**3:06** 190:10
**3:15** 190:11
**3:26** 198:10
**3:38** 198:11
**3:49** 207:16
**3:53** 207:17
**30** 53:18 221:5,10 322:6
**30(b)(6)** 69:8,13 76:12,15 83:20,22 84:7,21 86:12 87:9 89:4 90:5,22 91:17 94:2 102:15 118:3 165:9 168:10,21 170:16 171:22 172:12 173:12 179:2 224:15 242:6 243:5 245:13 247:14 248:12 250:8 253:2 255:10 277:16,16 282:11 283:12 285:16 286:20 307:10 308:19 315:5,15 317:4 321:18 331:11 333:6 342:20 345:19 349:11 352:21 358:15
**30(e)** 360:1
**30-day** 308:7
**301** 4:21
**3024(i)(1)** 15:8 40:18
**305-7919** 4:10
**311** 6:17
**314** 3:6
**316** 6:19
**317** 6:21
**327** 5:6
**330** 7:4,6
**341** 7:8
**351** 5:5
**353** 7:10
**36** 108:18,22 109:9 109:14 110:3,5 112:9 113:8 115:10 119:14,21 124:12 139:4
**3605** 15:19
**3605(a)** 15:9 40:18
**37** 109:1,10 110:6 112:9 113:8 115:10 119:21 124:12 198:17 199:18 200:15 201:3 203:17,18

**4**

**4** 96:17 99:15 104:21 196:4 264:20 265:18 343:15
**4a** 19:18
**4d** 19:18
**4:03** 216:19
**4:13** 216:20
**4:30** 232:9
**4:46** 232:10

**4:57** 241:17
**400-8845** 363:3
**41** 5:10 19:1,5,6,19
**415** 3:15
**42** 5:11 44:16,20,21 45:7,15 58:15 77:13,13,19 189:19,20 190:16 190:20 195:16 197:7 200:12 204:3
**43** 5:12,13 95:6,7 95:11,14,21 96:14 97:8,12 98:8,17 99:19 102:4 105:21 106:17 108:18,22 109:10 110:6 112:9 113:8 115:10 119:22 124:13 126:21 138:15 139:12 140:20 141:1 143:10 145:3 198:18 199:18 200:16 201:4 203:17 273:3
**44** 5:16 129:14,15 129:19 131:3,17 135:4 137:8 138:5 140:19,22 192:4 193:22 194:6 209:14
**443** 4:18 291:5,12
**45** 5:19 159:7,8,12 159:16,21,22 163:15 174:2 175:5,22 176:10 177:1,19 185:13 185:14 187:14,15 187:22 188:1
**45th** 363:2
**46** 6:4 210:1,2,8 211:9 212:19 214:8 217:3
**47** 6:7 220:1,5 221:6,7 224:20 226:8,15
**479-2613** 4:18
**48** 6:9 250:1,5 252:22
**49** 6:11 251:20 252:3,22 253:12 253:14

**5**

**5** 77:12 109:22 131:16 192:4 194:1,4,6 195:16 196:6 200:12 233:3,18,19 264:20 265:18
**5th** 3:13
**5:04** 241:18
**5:21** 258:2
**5:35** 258:3
**5:37** 260:12
**50** 6:13 15:8,9 40:18,18 279:11 279:15 280:13 281:14 282:19
**51** 6:15 312:1,4,14 313:18
**514-3358** 4:11
**52** 6:18 317:21 318:3
**53** 6:20 318:11,12 320:2,13
**535** 3:5
**54** 7:4 217:17 331:1 331:2,3,6,7,12,15 332:9 334:8
**55** 7:5 217:14 331:1 331:2,3 332:7 333:3,19 334:8
**56** 7:7 217:18 342:6 342:9 343:16 344:1
**57** 7:9 210:22 211:7 211:21 217:13 354:14,15

**6**

**6** 19:18 58:15 77:13 77:21,22 86:14 104:4 126:22 190:14 209:12,14
**6:23** 260:13
**6:26** 262:8
**6:28** 262:9
**6:34** 267:6
**6:37** 267:7
**6:40** 271:1
**6:43** 271:2
**6:45** 272:14
**6:57** 272:15
**688-6054** 4:21
**693-2116** 3:15

**7**

**7** 118:5 190:1,3,14 190:15 197:7 204:4
**7:01** 277:10
**7:08** 277:11
**7:16** 284:12
**7:23** 284:13
**7:26** 286:14
**7:28** 286:15
**7:30** 287:7
**7:32** 287:8
**7:42** 297:8
**7:43** 297:9
**7:45** 298:16
**7:59** 298:17
**702** 5:14,18 6:5,19 6:21 7:10 20:10 24:3,7 28:17 29:1 95:17 106:6 130:6 131:1,9 169:22 199:2 206:6 210:14 218:5 221:14 233:12 308:4 313:3 318:8 318:20 319:5 320:4,15 322:5 355:1
**79** 98:14 141:8

**8**

**8** 109:17 111:17 190:2,3,14,15 197:7 204:4
**8:04** 303:12
**8:18** 303:13
**8:25** 310:1
**8:36** 310:2
**8:42** 314:6
**8:43** 314:7
**8:57** 323:9
**854-1128** 3:8

**9**

**9** 6:8 7:7 109:16 117:3 119:15 343:13 355:6
**9th** 220:10
**9:12** 2:5
**9:22** 323:10
**9:29** 328:5
**9:39** 328:6
**9:49** 338:19,20
**9:53** 342:14
**9:59** 342:15
**94** 5:15
**94111-5800** 3:14

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | | |
|---|---|---|
| **WIKIMEDIA FOUNDATION,** | ) | |
| **Plaintiff,** | ) | |
| | ) | |
| **v.** | ) | **Case No. 1:15-cv-662** |
| | ) | |
| **NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE, *et al.*,** | ) | |
| | ) | |
| **Defendants.** | ) | |

## MEMORANDUM OPINION

At issue in this First and Fourth Amendment suit is plaintiff's motion to compel defendants to respond to discovery requests regarding defendant National Security Agency's ("NSA") Upstream surveillance program. Specifically, plaintiff served 84 discovery requests on defendants in an effort to establish that at least one of plaintiff's communications has been intercepted, copied, and reviewed by defendants. Defendants have objected to 53 of these requests on the basis of the common law state secrets privilege and other statutory privileges, arguing that the information plaintiff seeks, if disclosed, reasonably could be expected to result in exceptionally grave damage to U.S. national security. Plaintiff now moves for an order compelling defendants to produce any information responsive to plaintiff's requests, contending that the Foreign Intelligence Surveillance Act ("FISA")[1] displaces the common law state secrets privilege and establishes procedures for the *ex parte* and *in camera* review of sensitive national security information. These issues have been fully briefed and argued and are now ripe for disposition.

[1] 50 U.S.C. § 1801, *et seq.*

## I.

A brief summary of the statutory framework pertinent to defendants' electronic surveillance efforts provides context necessary for resolution of the question presented in this case. In 1978, Congress enacted FISA in response to growing concerns about the Executive Branch's use of electronic surveillance. Specifically, Congress sought through FISA to accommodate U.S. national security interests in obtaining intelligence about foreign powers while also providing meaningful checks on the Executive Branch's ability to conduct that surveillance. In this respect, FISA created a "secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights." S. Rep. No. 604, pt. 1, 95th Cong. 1st Sess. 15 (1977), reprinted in U.S.Code Cong. & Admin.News 1978, pp. 3904, 3916.

A central component of this framework is the U.S. Foreign Intelligence Surveillance Court ("FISC"). FISC, a tribunal composed of eleven federal district judges designated by the Chief Justice of the U.S. Supreme Court, is charged with the review of applications for electronic surveillance. *See* 50 U.S.C. § 1803(a). FISA provides that, with limited exceptions, the Executive Branch cannot conduct surveillance of a foreign power or its agents absent prior FISC authorization. To obtain FISC authorization for electronic surveillance, the Attorney General must personally approve an application for surveillance, which must (i) comport with FISA's procedural requirements and (ii) establish probable cause to believe that the target of electronic surveillance is a foreign power or an agent of a foreign power and that each of the facilities at which electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. *Id.* § 1805

FISA also establishes rules governing the use of information obtained through electronic surveillance. *See id.* § 1806. Specifically, if the Government, including any State or political subdivision, intends to "enter into evidence or otherwise use or disclose" at any proceeding information obtained through electronic surveillance against an "aggrieved person"—that is, any person who has been the subject of electronic surveillance—the Government must first "notify the aggrieved person and the court or other authority" of its intent to so disclose or use the information. *Id.* §§ 1806(c),(d). The person against whom the evidence is to be introduced may then move to suppress the evidence obtained through electronic surveillance on the grounds that (i) "the information was unlawfully acquired" or (ii) "the surveillance was not made in conformity with an order of authorization or approval." *Id.* § 1806(e). FISA establishes specific procedures that courts must follow in the event (i) that the government notices its intent to use electronic surveillance information, (ii) that an aggrieved person files a motion to suppress or (iii) that an aggrieved person files "any motion . . . pursuant to any other statute or rule of the United States . . . to discover, obtain, or suppress" information obtained from electronic surveillance. *Id.* § 1806(f). Specifically, the court

> shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure . . . would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary . . . ."

*Id.*

On the basis of its *ex parte* and *in camera* review of the materials at issue, the court must determine "whether the surveillance of the aggrieved person was lawfully authorized and conducted." *Id.* FISA permits courts making this determination to disclose to the aggrieved person portions of the application, order, or other materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.* If, in the end, the court

determines that the surveillance was not lawfully authorized or conducted, the court must suppress the unlawfully obtained evidence or otherwise grant the motion of the aggrieved person. *Id.* § 1806(g). If, on the other hand, the surveillance was lawfully authorized and conducted, the court "shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." *Id.*

In addition to mandating specific procedures governing the use of information obtained through electronic surveillance, FISA establishes additional checks on the Executive's use of electronic surveillance. Two such checks come by way of criminal sanctions and a civil cause of action. Specifically, FISA imposes criminal penalties on any person who intentionally "engages in electronic surveillance under color of law except as authorized by [FISA]" or "discloses 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 [FISA.]" *Id.* § 1809(a)(1)-(2). FISA also provides a civil cause of action to any "aggrieved person . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 . . . against any person who committed such violation . . . ." *Id.* § 1810.

In 2008, thirty years after FISA's enactment, Congress passed the FISA Amendments Act ("FAA"), which establishes additional procedures and requirements for the authorization of surveillance targeting persons located outside the United States. *See* 50 U.S.C. § 1881a-g. Specifically, § 702 of the FAA[2] provides that the Attorney General and the Director of National Intelligence may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence

[2] 50 U.S.C. § 1881a.

information" if the FISC approves "a written certification" submitted by the government attesting, *inter alia*, (i) that a significant purpose of the acquisition is to obtain foreign intelligence information and (ii) that the acquisition will be conducted "in a manner consistent with the [F]ourth [A]mendment" and the targeting and minimization procedures required by statute. 50 U.S.C. § 1881a(b),(g). To approve such a certification, the FISC must determine that the government's targeting procedures are reasonably designed:

> (i) to ensure that acquisition "is limited to targeting persons reasonably believed to be located outside the United States," *id.* § 1881 a(i)(2)(B)(i);
>
> (ii) to prevent the intentional acquisition of wholly domestic communications, *id.* § 1881a(i)(2)(B)(ii);
>
> (iii) 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," *id.* § 1801(h)(1); *see id.* § 1881a(i)(2)(C); and
>
> (iv) to ensure that the procedures "are consistent with . . . the [F]ourth [A]mendment," *id.* § 1881a(i)(3)(A).

Unlike FISA, these FAA procedures do not require the FISC to determine that probable cause exists to believe that the target of electronic surveillance is a foreign power and that each of the facilities at which electronic surveillance is directed is being used or is about to be used by a foreign power.

The recent release of public reports and declassification of FISC opinions have revealed additional details regarding the collection of communications under § 702. For example, the government has disclosed that it conducts § 702 surveillance through two programs—PRISM and Upstream surveillance. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 7 (2014) ("PCLOB Report"). The program at issue here, Upstream surveillance, involves

collection of communications of persons reasonably believed to be outside of the United States "with the compelled assistance . . . of the providers that control the telecommunications backbone over which [telephone and Internet] communications transit." *Id.* at 35. In this respect, "[t]he government 'tasks' certain 'selectors,' such as telephone numbers or email addresses, that are associated with targeted persons, and it sends these selectors to electronic communications service providers to begin acquisition." *Id.* at 7. The providers then assist the government in the collection of the communications associated with those selectors. *See id.*

**II.**

With this statutory framework in mind, it is appropriate to turn to the facts and procedural history in this case. Plaintiff Wikimedia Foundation, a non-profit organization based in San Francisco, California, operates several "wiki"-based projects and provides the contents of those projects to individuals around the world free of charge. Defendant National Security Agency/Central Security Service ("NSA") is the U.S. government agency responsible for conducting the surveillance at issue in this case. Defendant Office of the Director of National Intelligence ("ODNI") is the agency responsible for directing the activities of the U.S. intelligence community, including the NSA, and defendant Department of Justice ("DOJ") is one of the government agencies responsible for overseeing electronic surveillance. Several individual defendants are also named in their official capacities, including the Director of the NSA and the Chief of the Central Security Service, the Director of National Intelligence, and the Attorney General of the United States.

On June 22, 2015, plaintiff, along with eight other organizations,[3] filed the Amended Complaint in this suit, challenging the legality of defendants' Upstream surveillance program pursuant to § 702 of the FAA. The Amended Complaint alleges that this program violates (i) the Administrative Procedure Act ("APA"), (ii) the Fourth Amendment to the Constitution, (iii) the First Amendment to the Constitution, and (iv) Article III of the Constitution. The Amended Complaint seeks (i) a declaration that Upstream surveillance violates the APA and the Constitution and (ii) an injunction permanently enjoining defendants from continuing Upstream surveillance.

On August 6, 2015, defendants filed a Motion to Dismiss pursuant to Rule 12(b)(1), Fed. R. Civ. P., arguing that none of the plaintiff organizations plausibly alleged that they were injured by the interception, copying and review of online communications via the Upstream surveillance program and thus plaintiffs lacked Article III standing to contest the legality of the program. Subsequently, on October 23, 2015, an Order and a Memorandum Opinion issued, concluding that the allegations in the Amended Complaint were too speculative to establish Article III standing and granting defendants' motion to dismiss as to all plaintiffs. *See Wikimedia Found., et al., v. Nat'l Sec. Agency*, 143 F. Supp. 3d 344, 356-57 (D. Md. 2015), *aff'd in part, vacated in part, and remanded by* 857 F.3d 193 (4th Cir. 2017). Thereafter, plaintiffs appealed and the Fourth Circuit issued an opinion affirming in part, vacating in part, and remanding the case to the district court for further consideration. *See Wikimedia Found., et al., v. Nat'l Sec. Agency*, 857 F.3d 193 (4th Cir. 2017). Specifically, the Fourth Circuit concluded that although the eight other organizations had failed to allege injuries sufficient to satisfy the requirements of Article III standing, Wikimedia Foundation had alleged facts "sufficient to make plausible the conclusion that the NSA is

[3] These original plaintiffs included the National Association of Criminal Defense Lawyers, Human Rights Watch, Amnesty International USA, Pen American Center, Global Fund for Women, the Nation magazine, the Rutherford Institute, and the Washington Office on Latin America.

intercepting, copying, and reviewing at least some of Wikimedia's communications." *Wikimedia Found, et al..*, 857 F.3d at 210.

Shortly after the Fourth Circuit remanded the case to the district court for further proceedings, the parties submitted briefs on how to proceed in the case. Defendants indicated their intent to continue to challenge plaintiff's Article III standing and argued that any discovery should be bifurcated to allow for resolution of the standing question prior to resolution of the merits. Plaintiff opposed defendants' proposed discovery plan, contending that the jurisdictional facts at issue here are so intertwined with the merits as to require simultaneous discovery and summary judgment briefing on both questions. On October 3, 2017, an Order issued, directing the parties to conduct a limited five-month period of jurisdictional discovery prior to full discovery on the merits. *See Wikimedia Found. v. Nat'l Sec. Agency*, 1:15-cv-662 (D. Md. Oct. 3, 2017) (Order).

The parties then proceeded to engage in the limited discovery as directed. Plaintiff served 84 requests for admission, interrogatories, and requests for production on defendants, seeking what plaintiff describes as three broad categories of information: (i) direct evidence that Wikimedia has been surveilled, (ii) definition of key terms used in describing Upstream surveillance to the public, and (iii) evidence concerning the scope and breadth of Upstream surveillance.[4] Defendants responded to several of these discovery requests by producing 500 pages of unclassified documents, but objected to 53 of plaintiff's requests on the basis of privilege. In particular, defendants asserted that the information sought by plaintiff was protected by the common law state secrets privilege and other statutory privileges regarding the protection of national security information. In this respect, defendants submitted the unclassified declaration of Daniel Coats, the Director of National Intelligence, formally invoking the state secrets privilege on the basis of

[4] That these interrogatories covered both standing and merits matters is neither inappropriate nor unexpected, as these matters may well be inextricably entwined.

his personal consideration of the risks associated with disclosure of the information plaintiff seeks. Defendants also submitted a classified declaration of George C. Barnes, the Deputy Director of the NSA, providing additional detail concerning the harm to national security that would be caused by disclosure of the information contained in plaintiff's discovery requests.

Subsequently, on March 26, 2018, plaintiff filed the Motion to Compel at issue here pursuant to Rule 37(a)(3), Fed. R. Civ. P. Plaintiff contends that where, as here, a party moves to discover material relating to electronic surveillance, the court must follow FISA's § 1806(f) procedures and conduct an *ex parte* and *in camera* review of the materials relating to electronic surveillance. Plaintiff argues that these procedures apply despite defendants' assertion of state secrets privilege because in enacting FISA, Congress intended to displace the common law state secrets privilege. And even assuming the state secrets privilege was not displaced by FISA, plaintiff argues that the privilege does not bar disclosure of the information at issue here given the amount of information concerning Upstream surveillance already in the public record.

Defendants oppose plaintiff's motion, arguing (i) that § 1806(f) does not apply where, as here, plaintiff has not yet established that it is the target of electronic surveillance and (ii) that even assuming § 1806(f) does apply here, there is no clear statement indicating Congress's intent to displace the common law state secrets privilege through enactment of FISA. Finally, defendants contend that the government's assessment of the national security risks associated with disclosure of the information concerning plaintiff's discovery requests is entitled to deference and that plaintiff's arguments to the contrary are baseless.

## III.

A threshold question that must be addressed is whether the *ex parte* and *in camera* review procedures established in § 1806(f) apply where, as here, a plaintiff is seeking classified discovery

to establish that the plaintiff's communications were unlawfully seized and searched. Analysis of this question properly begins with the terms of that statute. Section 1806(f) provides, in pertinent part:

> Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to electronic surveillance . . . the United States district court . . . shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

50 U.S.C. § 1806(f). The statute further defines "aggrieved person" as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." *Id.* § 1801(k).

This statutory text points persuasively to the conclusion that § 1806(f) procedures do not apply where, as here, a plaintiff has not yet established that it has been the subject of electronic surveillance. Specifically, the text of § 1806(f) identifies only three circumstances in which its procedures apply: (i) when the government notifies the court that it plans to introduce evidence obtained through electronic surveillance, (ii) when an aggrieved person moves to suppress information obtained through electronic surveillance, and (iii) when an aggrieved person makes "any motion or request . . . pursuant to any other statute or rule of the United States . . . to discover or obtain . . . materials relating to electronic surveillance." *Id.* Here, (i) and (ii) are clearly not met. The government has not noticed its intent to use or disclose information obtained through electronic surveillance, and plaintiff has not filed a motion to suppress any such information.

Accordingly, the only possible § 1806(f) situation applicable here is (iii), the third circumstance that may trigger § 1806(f). But importantly, § 1806(f) provides that this third situation applies only when the motion or request at issue "is made by an *aggrieved person*[,]"[5] namely "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."[6] In this regard, the text of § 1806(f) makes clear that a party's status as an "aggrieved person," or the subject of surveillance, is a precondition to the application of § 1806(f)'s procedures; unless and until a party has adduced evidence that it has been the subject of electronic surveillance, a party's motion cannot trigger § 1806(f)'s *ex parte* and *in camera* review procedures.

This interpretation of the text is confirmed by the nature of § 1806(f)'s procedures once invoked. Specifically, § 1806(f)'s procedures require courts to engage in *ex parte* and *in camera* review of orders or other materials relating to surveillance to determine whether the surveillance at issue "was lawfully authorized and conducted." *Id.* § 1806(f). A determination that surveillance was lawfully authorized and conducted cannot occur unless a determination has previously been made that the surveillance at issue did, in fact, occur. Put differently, it is impossible to determine the lawfulness of surveillance if no surveillance has actually occurred. Thus, the text of § 1806(f) points persuasively to the conclusion that Congress intended § 1806(f) procedures to apply only after it became clear from the factual record that the movant was the subject of electronic surveillance.

Had Congress instead intended § 1806(f) to be a vehicle for parties to determine whether they were the target of electronic surveillance, one would expect to see language requiring courts

---

[5] *Id.*

[6] *Id.* § 1801(k).

to review materials relating to electronic surveillance to determine whether "electronic surveillance occurred," or requiring the government to affirm or deny the existence of any surveillance. Indeed, Congress has used precisely this language elsewhere in the U.S. Code. Specifically 18 U.S.C. § 3504, which was enacted eight years prior to FISA in 1970, provides that where a party claims evidence is admissible because the evidence is the product of an unlawful act, such as warrantless wiretapping, "the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act[.]" 18 U.S.C. § 3504. This provision demonstrates that Congress knew how to draft language requiring the government to affirm or deny the existence of some fact when Congress sought to do so. But importantly, § 1806(f) does not adopt this or similar language requiring an affirmation or denial of the fact of surveillance upon motion by an aggrieved person; rather, § 1806(f) provides that, upon a motion made by an aggrieved party, the court will determine whether the surveillance "was lawfully authorized and conducted." To assign meaning to this textual variation demands that § 1806(f) be interpreted to require *ex parte* and *in camera* review of the lawfulness of surveillance only after the individual has adduced evidence that he has been the target of electronic surveillance. *Cf. Lorillard v. Pons*, 434 U.S. 575, 584 (1978) (finding that Congress did not intend to apply the standards from one statute to a later-enacted statute where significant differences existed in the text of the two statutes).

Consideration of the other circumstances in which § 1806(f) procedures apply further bolsters the conclusion reached here. It is axiomatic that where, as here, "general words follow specific words in a statutory enumeration, the general words are usually construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." *Yates v. United States*, 135 S.Ct. 1074 (2015) (quoting *Washington State Dept. of Social & Health Servs. v. Guardianship Estate of Keffeler*, 537 U.S. 371, 384 (2003) (internal quotation marks omitted)).

In *Begay v. United States*, 553 U.S. 137, 142-43 (2008), the Supreme Court relied on this principle to determine whether specific crimes were covered by the statutory phrase "any crime . . . that . . . is burglary, arson, or extortion, involves use of explosives, or otherwise involves conduct that presents a serious potential risk of physical injury to another[.]" The Supreme Court reasoned that the enumeration of specific crimes—that is, burglary, arson, extortion, and use of explosives—indicated that the broadly worded "otherwise involves" provision covered "only similar crimes, rather than every crime that 'presents a serious potential risk of physical injury to another.'" *Id.* at 142.

The statutory provision at issue here—§ 1806(f)—is structured in precisely the same way as the provision at issue in *Begay*. Specifically, like the provision at issue in *Bergay*, § 1806(f) enumerates two specific situations covered by its procedures—namely, when the government provides notice pursuant to § 1806(c)-(d) and when a person against whom evidence is to be introduced moves to suppress that evidence pursuant to § 1806(e)—followed by a broadly-worded more general provision that also triggers § 1806(f)—namely, "whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to electronic surveillance . . . ." *Id.* As in *Bergay*, this broadly-worded, more general provision must be interpreted in light of the specifically enumerated provisions listed before it. And importantly, in each of these two specific situations, there is clear evidence that electronic surveillance has occurred; the only question is whether the evidence derived from the electronic surveillance may properly be disclosed.[7] Thus,

[7] This common thread uniting the situations in which § 1806(f) applies is further highlighted by the legislative history of this provision. Specifically, the Senate Report notes additional examples of instances in which § 1806(f)'s procedures apply, including "whenever an individual makes a motion pursuant to . . . 18 U.S.C. § 3504 . . . to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance . . . ." S. Rep. 95-701, 63, 1978 U.S.C.C.A.N. 3973, 4032. In this respect, the Senate Report explained that a defendant could "quer[y] the

to "avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words" and to avoid "giving unintended breadth to the Acts of Congress[,]" it is necessary to interpret the final provision of § 1806(f) as similarly requiring evidence of the fact of electronic surveillance. *Gustafson v. Alloyd Co.*, 513 U. S. 561, 575 (1995).

Support for the conclusion reached here is found not solely in the text of § 1806(f) itself, but also in the caption of § 1806 and the general structure of the provision. Although "headings are not commanding," the Supreme Court has recognized that headings can "supply cues" that Congress did not intend a particular meaning of the statute. *Yates v. United States*, 135 S. Ct. 1074, 1083 (2015). Section 1806's heading—use of information—suggests that Congress did not intend §1806(f) to apply in situations where, as here, it is yet unclear whether electronic surveillance even occurred. Rather, the heading suggests that Congress intended the provisions of § 1806 to apply where evidence already establishes the fact of surveillance, and the central dispute is instead how, and whether, information obtained via that electronic surveillance can be used or disclosed in a proceeding.

Finally, as the Supreme Court has recognized, "[i]t is axiomatic that statutes in derogation of the common law should be narrowly construed[.]" *Badaracco v. C.I.R.*, 464 U.S. 386, 403 n.3 (1984). In this case, as plaintiff notes, § 1806(f) seems on its face to conflict with traditional principles of common law, namely the common law state secrets privilege. Specifically, the mandatory *ex parte* and *in camera* review procedures established in § 1806(f), in situations in which these procedures apply, likely displace the common law process whereby courts review the government's assertion of the state secrets privilege to avoid disclosure of information potentially harmful to national security. Given this, traditional principles of statutory interpretation counsel

government under 18 U.S.C. § 3504," "discover[] that he has been intercepted by electronic surveillance" and then move to suppress or to discover or obtain information related to that surveillance.

that FISA must be narrowly construed so as to avoid excessive displacement inconsistent with Congress's intent. To interpret the text of § 1806(f) broadly, as plaintiff here suggests, to encompass not just motions raised by parties who have adduced evidence that they are "aggrieved persons," but also motions by parties who simply allege that they are "aggrieved persons," would do precisely this, namely displace the common law to an extent neither contemplated nor intended by Congress.

In an attempt to avoid this conclusion, plaintiff contends that the allegations contained in the complaint are sufficient to establish that plaintiff is an "aggrieved person" within the meaning of § 1806(f). Specifically, defendant cites to the Fourth Circuit's determination that plaintiff's complaint alleges sufficient facts "to make plausible the conclusion that the NSA is intercepting, copying, and reviewing at least some of [plaintiff's] communications" and contends that this plausibility determination is sufficient standing alone to require invocation of § 1806(f)'s procedures. *Wikimedia Found., et al.*, 857 F.3d at 211. But the Fourth Circuit concluded that plaintiff had sufficiently alleged injury-in-fact for the purposes of surviving a motion to dismiss; the Fourth Circuit never considered the requisite showing of "aggrieved person" status to trigger the earlier procedures outlined in § 1806(f). *Id.* at 207-11. As such, the Fourth Circuit's determination in *Wikimedia* does not answer the question raised here—namely what showing is required prior to invocation of § 1806(f) procedures.

Notably, the only circuit authority to consider this latter question—what a party must show to establish his or her "aggrieved person" status and invoke § 1806(f)—recognized that a party may not trigger § 1806(f) procedures unless and until the party has adduced evidence of its "aggrieved person" status. Specifically, in *ACLU Foundation of Southern California v. Barr*, 952 F.2d 457 (D.C. Cir. 1991), the D.C. Circuit reversed the district court's dismissal of the plaintiffs'

First Amendment claim based on the government's surveillance of plaintiffs' communications. In denying the motion to dismiss, the D.C. Circuit reasoned that "legitimate concerns about compromising ongoing foreign intelligence investigations" are more properly considered at the summary judgment stage, not upon the pleadings. *Id.* at 469. In this respect, the D.C. Circuit explained that plaintiffs challenging alleged unlawful electronic surveillance must survive summary judgment—that is, they must adduce evidence sufficient to prove the existence of a genuine dispute about the fact of ongoing surveillance before the court applies § 1806(f) procedures. *Id.* The D.C. Circuit recognized that "in the usual case some discovery is permitted before the court rules on a motion for summary judgment," but importantly, the D.C. Circuit noted that "normal rules regarding discovery must be harmonized with FISA and its procedures, notably 1806(f)." *Id.* In this regard, The D.C. Circuit further explained that:

> even plaintiffs who defeat summary judgment motions would not be entitled to obtain any of the materials relating to the authorization of the surveillance or the evidence derived from it unless the district court, in an *ex parte, in camera* proceeding, first determined that the surveillance was not "lawfully authorized and conducted."

*Id.* This analysis in *Barr* makes clear that the D.C. Circuit contemplated the conclusion reached here, namely that in order to trigger § 1806(f) procedures, a plaintiff must first adduce evidence sufficient at least to create a genuine dispute as to whether the plaintiff has been the target of electronic surveillance in the past or whether electronic surveillance is ongoing.

Plaintiff next argues that to require a plaintiff to adduce evidence of surveillance to demonstrate his or her "aggrieved person" status would necessarily mean that a plaintiff could not do so unless the government affirmatively acknowledges the fact of surveillance. And to require the government affirmatively to acknowledge the fact of surveillance prior to invocation of § 1806(f) procedures, plaintiffs contend, would be inconsistent with other provisions in the statute, namely the civil cause of action established in § 1810.

This argument fails to persuade because it mischaracterizes both (i) the requirements for establishing "aggrieved person" status and (ii) the nature of the civil remedy established in § 1810. To begin with, affirmative government acknowledgement of surveillance of a specific target is not the only means by which a plaintiff can establish evidence of his or her "aggrieved person" status. Indeed, courts have recognized that plaintiffs can "rely on many non-classified materials, including present and future public disclosures of the government or [telecommunications providers] on the alleged NSA programs" to establish that they have been the target of electronic surveillance. *Hepting v. AT&T Corp., et al.*, 439 F. Supp. 2d 974, 998 (N.D. Cal. 2006). Thus, to require a plaintiff to adduce evidence of surveillance to demonstrate his or her "aggrieved person" status does not necessarily require that the government affirmatively acknowledge the fact of surveillance.

And even assuming, *arguendo*, that affirmative government acknowledgment was the only means by which a plaintiff could prove his or her "aggrieved person" status, this requirement would not be inconsistent with the remedy established in § 1810. That section provides a civil remedy to "[a]n aggrieved person . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809." 50 U.S.C. § 1810. Plaintiff argues that to require government acknowledgement of surveillance prior to invocation of § 1806(f) procedures would render § 1810 a nullity because plaintiff's access to the remedy against the government would be dependent entirely on cooperation by the government. This argument is unpersuasive; courts have made clear that § 1810 is not actually a remedy against the government because § 1810 does not contain an explicit waiver of sovereign immunity. *See Al-Haramain Islamic Found., Inc. v. Obama*, 705 F.3d

845, 854 (9th Cir. 2012).[8] Instead, § 1810 provides a remedy against intelligence agents who engage in unlawful electronic surveillance or who disclose information obtained from unlawful surveillance in their personal, not official, capacities. In this respect, the civil cause of action in § 1810 is premised upon the individual agent's "violation of section 1809[,]" which establishes criminal penalties for unlawful surveillance. *Al-Haramain*, 705 F.3d at 854 (quoting 50 U.S.C. 1810).[9] There is no reason to believe that the government would be unwilling to cooperate in acknowledging that an individual agent conducted unlawful surveillance in his individual capacity. Indeed, to the extent that § 1810 is intended to track an individual agent's criminal liability, the government will necessarily acknowledge, and indeed prove, the fact of surveillance through a criminal prosecution of that individual agent.

Finally, plaintiff cites to one case in which a district court found that the plaintiffs "alleged enough to plead 'aggrieved person' status so as to proceed to the next step in proceedings under FISA sections 1806(f) and 1810." *In re NSA Telecommc'ns Records Litig.*, 595 F.Supp.2d 1077, 1085-86 (N.D. Cal. 2009). But in reaching this conclusion—namely that the allegations in plaintiff's complaint were sufficient to invoke § 1806(f) procedures—the court did not conduct an in-depth analysis of the text or indeed even of the legislative history of FISA. Instead, the *In re NSA Telecommunications Records Litigation* court imported a standard from the Ninth Circuit's analysis of claims pursuant 18 U.S.C. § 3504.[10] Section 3504 provides, in relevant part, that "upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an

---

[8] *See also Whitaker v. Barksdale Air Force Base*, 2015 WL 574697, *7 (W.D. La. Feb. 11, 2015) (agreeing with the "extensive analysis" in *Al-Haramain*).

[9] *See also* H.R. Conf. Rep. No. 95-1720 (noting that the cause of action in § 1810 is afforded "to any aggrieved person about whom information has been disclosed or used in violation of the criminal penalty provisions" and that "civil liability of intelligence agents under this act should coincide with the criminal liability.").

[10] 18 U.S.C. 3504

unlawful act . . . , the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act." 18 U.S.C. § 3504. In *United States v. Alter*, 482 F.2d 1016 (9th Cir. 1974), the Ninth Circuit concluded that § 3504's requirement to affirm or deny the occurrence of the alleged unlawful act is triggered where the party aggrieved makes a "prima facie showing that good cause exists to believe" the individual was subject to illegal surveillance. *Id.* at 1026.

Plaintiff's reliance on *In re NSA Telecommunications Records Litigation* and its application of the § 3504 standard in the FISA context is unpersuasive because § 3504 is different from § 1806(f) in significant ways. Notably, although both § 1806(f) and § 3504 use the term "aggrieved," § 1806(f), unlike § 3504, incorporates a statutory definition of an "aggrieved person," which specifies that an "aggrieved person" is "a person who is the target of an electronic surveillance" or "whose communications or activities were subject to surveillance[.]" 50 U.S.C. § 1801(k). As such, while a party can claim to be aggrieved for the purposes of § 3504 through a "mere assertion"[11] that unlawful surveillance has occurred, § 1806(f) requires that the person has actually been a target of electronic surveillance or has been subject to surveillance before that individual can trigger the *ex parte* and *in camera* review procedures outlined in § 1806(f).

Moreover, the reasoning in support of the low burden in the § 3504 context does not apply here. Specifically, in analyzing § 3504, courts have reasoned that the government's obligation to affirm or deny the occurrence of unlawful surveillance is triggered by the mere assertion of unlawful wiretapping because "requiring the government to affirm or deny the existence of illegal surveillance of witnesses imposes only a minimal additional burden upon the government." *Vielguth*, 502 F.2d at 1259 n.4 (citing *In re Evans*, 452 F.2d at 1247). But this reasoning is inapplicable here because § 1806(f) requires much more than a simple affirmation or denial by the

[11] *United States v. Vielghth*, 502 F.2d 1257, 1258 (9th Cir. 1974) (quoting *In re Evans*, 452 F.2d 1239, 1247 (1971)).

government. Section 1806(f) procedures, once triggered, require the court to review *ex parte* and *in camera* all of the relevant materials relating to electronic surveillance—in this case, potentially 10,000 pages of documents—to determine the lawfulness of the surveillance. The reasoning justifying the low burden in § 3504 is thus inapplicable here where a much higher burden is associated with the applicable procedures. Given that the *In re NSA Telecommunications Records Litigation* court, in interpreting the requirements of § 1806(f), relied on a standard imported from 18 U.S.C. § 3504, which, for the reasons described above, is inapplicable here, plaintiff's reliance on *In Re NSA Telecommunications Records Litigation* is unpersuasive and does not alter the conclusion reached here.[12]

In sum, when interpreted in light of traditional principles of statutory interpretation, the text of § 1806(f) makes clear that § 1806(f) procedures do not apply where, as here, the plaintiff has merely plausibly alleged that it has been the target of surveillance and has not yet adduced evidence establishing this fact of surveillance. Accordingly, it is not appropriate at this time to engage in *ex parte* and *in camera* review of the materials responsive to plaintiff's interrogatories or to those plaintiff describes in its motion to compel.

**IV.**

---

[12] It is also worth noting that despite the *In re NSA Telecommunications Records Litigation* court's determination that the plaintiffs there had sufficiently alleged their aggrieved person status, the court nonetheless declined to follow the mandatory § 1806(f) procedures. 595 F.Supp.2d at 1086-90. Specifically, the court ordered the government to produce responsive materials, but has yet to make a finding as to the lawfulness of any surveillance and has not provided the plaintiffs access to any discovery materials. *Id.*

Plaintiff also cites to *Jewel v. NSA*, a Northern District of California case in which the district court issued several orders, directing the government to produce materials for *ex parte* and *in camera* review. But the *Jewel* court appeared not to address the requisite showing of "aggrieved person" status, and as such, that case did not directly address the issues addressed here. Indeed, the *Jewel* court has not yet issued an order as to the lawfulness of any alleged surveillance in that case and has recently issued an order requesting additional briefing on how plaintiffs can "establish they may be aggrieved persons without access to [classified] information" and "the current legal standard for asserting standing in these circumstances." *Jewel v. NSA*, No. 08-cv-4373, at *1 (N.D. Cal. July 5, 2018). As such, it is clear that the *Jewel* court has not yet definitively resolved the issues addressed here.

Given that § 1806(f) procedures do not apply here, it is unnecessary to consider the question whether § 1806(f) displaces the state secrets privilege in situations in which § 1806(f) does apply. As such, the only remaining question is whether the government's invocation of the state secrets privilege defeats plaintiff's motion to compel.

**A.**

It is necessary first to review the well-settled Supreme Court and Fourth Circuit precedents governing the assertion of the state secrets privilege. Supreme Court and Fourth Circuit precedent make clear that "[u]nder the state secrets doctrine, the United States may prevent the disclosure of information in a judicial proceeding if 'there is a reasonable danger' that such disclosure 'will expose . . . matters which, in the interest of national security should not be divulged." *Abilt v. CIA*, 848 F.3d 305, 310-11 (4th Cir. 2017) (quoting *El-Masri v. United States*, 479 F.3d 296, 302 (4th Cir. 2007) (quoting *United States v. Reynolds*, 345 U.S. 1, 10 (1953)). In this regard, the Fourth Circuit has recognized that the state secrets privilege "performs a function of constitutional significance, because it allows the executive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities." *Id.* at 312 (quoting *El–Masri*, 479 F.3d at 303).

The Fourth Circuit has mandated a three-step analysis for resolution of a state secrets question:

> First, "the court must ascertain that the procedural requirements for invoking the state secrets privilege have been satisfied." Second, "the court must decide whether the information sought to be protected qualifies as privileged under the state secrets doctrine." Third, if the "information is determined to be privileged, the ultimate question to be resolved is how the matter should proceed in light of the successful privilege claim."

*Albit*, 848 F.3d at 311 (quoting *El-Masri*, 479 F.3d at 304).

With respect to the first step in this analysis, the Supreme Court has specified three procedural requirements for invocation of the state secrets privilege: (i) the state secrets privilege must be asserted by the United States government; it "can neither be claimed nor waived by a private party," (ii) "[t]here must be a formal claim of privilege, lodged by the head of the department which has control over the matter," and (iii) the department head's formal claim of the state secrets privilege must be made only "after actual personal consideration by that officer." *Reynolds*, 345 U.S. at 7-8 (footnotes omitted). If these procedural requirements are satisfied, the court may proceed to the second step of the analysis.

This second step of the analysis requires courts to "determine whether the information that the United States seeks to shield is a state secret, and thus privileged from disclosure." *El-Masri*, 479 F.3d at 304. In this respect, courts must "assure [themselves] that an appropriate balance is struck between protecting national security matters and preserving an open court system." *Albit*, 848 F.3d at 311-12 (quoting *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1203 (9th Cir. 2007)). That is, courts assessing a claim of state secrets privilege must simultaneously accord "utmost deference"[13] to the Executive Branch's assessment of the risk to national security posed by the disclosure of information while also "critically examin[ing] instances of [the privilege's] invocation" so as "not to accept at face value the government's claim or justification of privilege."[14]

The Supreme Court has balanced these competing concerns by requiring courts to determine "from all the circumstances of the case, [whether] there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security,

---

[13] *Albit*, 848 F.3d at 312 (quoting *United States v. Nixon*, 418 U.S. 683, 710 (1974), *superseded by statute on other grounds as recognized by Bourjaily v. United States*, 483 U.S. 171, 177-79 (1987)).

[14] *Id.* at 312 (quoting *Al-Haramain*, 507 F.3d at 1203; *Ellsberg v. Mitchell*, 709 F.2d 51, 58 (D.C. Cir. 1983)).

should not be divulged.'" *Reynolds*, 345 U.S. at 10. The government bears the burden of satisfying "the reviewing court that the *Reynolds* reasonable-danger standard is met." *Albit*, 848 F.3d at 312 (quoting *El-Masri*, 479 F.3d at 305). In this regard, the Fourth Circuit has recognized that the explanation proffered by the department head who formally invokes the privilege is "frequently . . . sufficient to carry the Executive's burden." *Id.* (quoting *El-Masri*, 469 F.3d at 305). In the end, if the government carries its burden and shows that there is a reasonable danger that disclosure of information will expose matters that should not be divulged, "court[s] [are] obliged to honor the Executive's assertion of the privilege[.]" *Id.* (quoting *El-Masri*, 479 F.3d at 305).

If the procedural requirements for invocation of the state secrets privilege are satisfied and the court determines that the information sought to be disclosed is properly privileged, the final step in the analysis is to assess how the matter should proceed. Here, again, Fourth Circuit and Supreme Court precedent is clear: if the state secrets privilege has been successfully invoked, "the claim of privilege will be accepted without requiring further disclosure." *Id.* (quoting *Reynolds*, 345 U.S. at 9).

**B.**

With these principles in mind, it is appropriate now to consider the assertion of the state secrets privilege in this case. To begin with, the procedural requirements for invocation of the state secrets privilege have been satisfied.[15] Defendants, the NSA, ODNI, and the DOJ, are U.S. government agencies and thus can properly claim the state secrets privilege. The claim of privilege was lodged by Daniel Coats ("Coats"), the Director of National Intelligence ("DNI"), who is the head of the U.S. Intelligence Community and in this regard, is tasked with the protection of

[15] Indeed, Wikimedia does not appear to dispute this point.

intelligence sources and methods from unauthorized disclosure. *See* Coats Decl. ¶ 1.[16] Finally, Coats invoked the privilege formally after personally considering the nature of plaintiff's discovery requests and determining that disclosure of the information requested reasonably could be expected to cause exceptionally grave damage, and at the very least, serious damage, to U.S. national security. *See* Coats Decl. ¶¶ 6, 16, 24, 28, 32, 35, 39, 43. Accordingly, it is clear that defendants have satisfied the procedural requirements for invocation of the state secrets privilege.

The government has similarly satisfied its burden with respect to the second step of the state secrets privilege analysis as careful review of the public Coats declaration and the classified Barnes declaration reveals that "there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged." *Reynolds*, 345 U.S. at 10. Specifically, through public and classified declarations defendants have identified seven categories of information covered by plaintiff's discovery requests, including: (i) entities subject to Upstream surveillance activities, (ii) operational details of the Upstream collection process, (iii) locations at which Upstream surveillance is conducted, (iv) categories of Internet-based communications subject to Upstream surveillance activities, (v) the scope and scale on which Upstream surveillance is or has been conducted, (vi) NSA's cryptanalytic capabilities, and (vii) additional categories in contained in FISC opinions and submissions. Moreover, defendants have provided detailed descriptions, in more than 60 pages of classified declarations, explaining that disclosure of these categories of information would undermine ongoing intelligence operations, deprive the NSA of existing intelligence methods, and significantly, provide foreign adversaries with the tools necessary both to evade U.S. intelligence operations and to conduct their

[16] *See also* 50 U.S.C. § 3024(i)(1) (providing that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.").

own operations against the United States and its allies. In sum, it is clear that there is a reasonable, and indeed likely, danger that disclosure of this information will expose matters which should not be divulged in the interest of national security, and as such, this information falls squarely within the ambit of the state secrets privilege. *See, e.g.*, *Albit*, 848 F.3d at 314 (concluding that "[t]here is little doubt that there is a reasonable danger that if information . . . regarding . . . the sources and methods used by the CIA [and] the targets of CIA intelligence collection and operations . . . were revealed, that disclosure would threaten the national security of the United States").[17]

In an attempt to avoid this conclusion, plaintiff contends that to acknowledge the fact that plaintiff has been subject to surveillance would not, in fact, threaten national security. This argument plainly fails because courts have concluded that where, as here, the information sought to be disclosed involves the identity of parties whose communications have been acquired, this information is properly privileged. *See* Al-*Haramain*, 507 F.3d at 1203-04 (finding that the fact of a plaintiff's surveillance by the NSA was covered by the state secrets privilege); *Halkin v. Helms*, 598 F.2d 1, 9 (D.C. Cir. 1978) (upholding assertion of state secrets privilege with respect to "the identity of particular individuals whose communications have been acquired").

Plaintiff contends that, contrary to surveillance of a particular individual with limited communications, plaintiff's communications are so ubiquitous that to reveal surveillance of its communications would not provide information regarding the structure of the Upstream surveillance program or its specific targets. Although this proposition may appear to have some force, courts have consistently recognized that "judicial intuition" about a proposition such as this

---

[17] *See also, e.g.*, *Sterling v. Tenet*, 416 F.3d 338, 342 (4th Cir. 2005) ("There is no question that information that would result in . . . disclosure of intelligence-gathering methods or capabilities . . . falls squarely within the definition of state secrets." (quoting *Molerio v. FBI*, 749 F.2d 815, 820-21 (D.C. Cir. 1984) (internal quotation marks omitted)); *Jewel v. NSA*, 2015 WL 545925, at *5 (N.D. Cal. Feb. 10, 2015) (finding "[d]isclosure of this classified information would risk informing adversaries of the specific nature and operational details of the Upstream collection process").

"is no substitute for documented risks and threats posed by the potential disclosure of national security information." *Al-Haramain*, 507 F.3d at 1203. And defendants have thoroughly documented those risks in the classified declaration here, explaining that to reveal the fact of surveillance of an organization such as plaintiff, even considering plaintiff's voluminous online communications, would provide insight into the structure and operations of the Upstream surveillance program and in so doing, undermine the effectiveness of this intelligence method.

Finally, plaintiff argues that there cannot be a reasonable danger of undermining national security because much of the information plaintiff seeks is already contained in publicly-accessible documents. But importantly, the information disclosed in these public documents is plainly different from the information that plaintiff seeks. For example, plaintiff's requests for admissions 13 through 15 ask defendants to admit that the NSA is conducting Upstream surveillance via "multiple INTERNET BACKBONE CIRCUITS," "multiple international Internet link[s]," and "multiple INTERNET BACKBONE 'chokepoints.'" Plaintiff contends that these facts have already been acknowledged by the NSA, as reflected in the PCLOB Report and certain unclassified portions of FISC opinions. Specifically, plaintiff contends that the PCLOB report's reference to "circuits" suggests the NSA is conducting surveillance on more than one circuit. To be sure, the PCLOB report does use the term "circuits," but it does not do so to refer to the number of sites the NSA is monitoring. Instead, the PCLOB report uses the term "circuits" in the context of defining the "Internet backbone." Specifically, the PCLOB report explains that the "Internet backbone" consists of "circuits that are used to facilitate Internet communications[.]" PCLOB Rep. at 36. Similarly, the redacted FISC Opinion cited by plaintiff does not, as plaintiff contends, confirm that the NSA is monitoring multiple international Internet links; instead, the redacted October 3, 2011 FISC Opinion states that "the government readily concedes that NSA will acquire a wholly

domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by the NSA . . . ." 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). Nothing in this statement confirms that the NSA is monitoring multiple internet links.[18] Ultimately, plaintiff's argument fails because although the government has declassified certain information about the Upstream surveillance program, the government has not yet released the precise information at issue here. Accordingly, this information is still properly subject to the state secrets privilege.

In sum, a careful review of defendants' public and classified declarations reveals (i) that defendants have satisfied the procedural requirements necessary to invoke the state secrets privilege and (ii) that the information sought to be protected qualifies as privileged under the state secrets doctrine. Given that defendants have satisfied the requirements of the state secrets privilege, "the claim of privilege will be accepted without requiring further disclosure." *Albit*, 848 F.3d at 31 (quoting *Reynolds*, 345 U.S. at 9). Accordingly, plaintiff's motion to compel must be denied.[19]

An appropriate Order will issue.

Alexandria, Virginia
August 20, 2018

/s/
T. S. Ellis, III
United States District Judge

[18] Plaintiff similarly argues that the fact that the NSA reviews the type of Internet communications in which plaintiff engages, namely HTTP and HTTPS Internet protocols, is available in the public record. But contrary to plaintiff's suggestion, the use of the general phrase "web activity" in an unclassified portion of the June 1, 2011 FISC Opinion does not confirm that the NSA is monitoring any specific Internet protocol, namely either HTTP or HTTPS.

[19] It is worth emphasizing the narrow scope of this decision, namely (i) that FISA § 1806 is not triggered in this case and that this provision and the associated FISA procedures do not operate here to displace the common law state secrets privilege and (ii) that the government has satisfied the well-settled procedural requirements necessary to invoke the privilege. Neither addressed nor resolved here is whether this long-ago judicially created privilege has, or should have, any continuing vitality today. That is not a question within the province of a district court.

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | | |
|---|---|---|
| **WIKIMEDIA FOUNDATION,** | ) | |
| **Plaintiff,** | ) | |
| | ) | |
| **v.** | ) | **Case No. 1:15-cv-662** |
| | ) | |
| **NATIONAL SECURITY AGENCY/ CENTRAL SECURITY SERVICE, *et al.*,** | ) | |
| | ) | |
| **Defendants.** | ) | |

**ORDER**

This matter came before the Court on plaintiff's Motion to Compel Discovery Responses and Deposition Testimony.

For the reasons stated in the accompanying Memorandum Opinion of even date,

It is hereby **ORDERED** that the motion is **DENIED**.

The Clerk is directed to provide a copy of this Order to all counsel of record.

Alexandria, Virginia
August 20, 2018

/s/
T. S. Ellis, III
United States District Judge

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE |

# Attachment C

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE<br><br>~~FILED UNDER SEAL~~ |

# EXHIBIT 1

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | | |
|---|---|---|
| WIKIMEDIA FOUNDATION, | ) | |
| Plaintiff, | ) | |
| v. | ) | No. 1:15-cv-0662 (TSE) |
| NATIONAL SECURITY AGENCY, *et al.*, | ) | |
| Defendants. | ) | |

**DECLARATION OF DR. HENNING SCHULZRINNE**

Dr. Henning Schulzrinne, for his declaration pursuant to 28 U.S.C. § 1746, deposes and says as follows:

**INTRODUCTION**

1. I am the Julian Clarence Levi Professor of Computer Science at Columbia University in New York, New York. I submit this declaration at the request of the United States Department of Justice to address technical issues surrounding, and to render opinions concerning, the assertion of plaintiff Wikimedia Foundation ("Wikimedia") that the National Security Agency ("NSA"), in the course of conducting electronic surveillance known as "Upstream" collection, must as a matter of technological necessity be intercepting, copying, and reviewing at least some of Wikimedia's electronic communications that traverse the Internet. For the reasons I detail herein, that assertion is incorrect. Based on what is publicly known about the NSA's Upstream collection technique, the NSA in theory could be conducting this activity, at least as Wikimedia conceives of it, in a number of ways that would not involve NSA interaction with Wikimedia's online communications.

2. A complete statement of my conclusions in this matter and the bases for them are set forth below, as are my background and qualifications in the fields of computer science, electrical engineering, and digital communications technology, and the sources of information I considered in arriving at the conclusions stated herein. I am being compensated for my services in this matter at the rate of $350 per hour. I have not previously testified as an expert whether by declaration, at trial, or by deposition.

## QUALIFICATIONS

3. I received my Ph.D. in Electrical Engineering in 1992 from the University of Massachusetts at Amherst, a Master's Degree in Electrical Engineering as a Fulbright scholar at the University of Cincinnati, Ohio, in 1987, and undergraduate degrees in Electrical Engineering and Economics from the Darmstadt University of Technology (Technische Hochschule) in Darmstadt, Germany, in 1984.

4. Prior to joining the faculty at Columbia University, I was an associate department head, from 1994 to 1996, at the Fraunhofer Institute for Open Communication Systems in Berlin, Germany (FOKUS), formerly an institute of the Society for Mathematics and Data Processing (GMD). From 1992 to 1994 I was a member of the technical staff at AT&T Bell Laboratories in Murray Hill, New Jersey.

5. I joined the faculty at Columbia University as a Professor of Computer Science and Electrical Engineering (a dual appointment) in 1996, and was named as Julian Clarence Levi Professor of Computer Science in 2009. I chaired the Department of Computer Science from 2004 to 2009. I teach courses in Computer Networks; Advanced Internet Services; and Internet Technology, Economics, and Policy and have in the past taught courses on network security and advanced programming. Concurrent with my position on the faculty at Columbia, from 2010 to 2012 I was an Engineering Fellow and Technical Advisor at the Federal Communications Commission (FCC), and Chief Technology Officer of the FCC from 2012 to 2017. In that role I guided the FCC's work on technology and engineering issues to ensure that FCC policies promoted technological innovation in the telecommunications industry.

6. In addition to my teaching responsibilities, I also head Columbia University's Internet Real-Time Laboratory, which under my supervision conducts research in the areas of real-time Internet multimedia services and Internet telephony; wireless and mobile networks; streaming; quality of service; resource reservation; dynamic pricing for the Internet; network measurement and reliability; service location; network security; media on demand; content distribution networks; multicast networks and ubiquitous and context-aware computing and communication; and designs, analyses and prototypes for next-generation "radio," "TV," and "telephone" networks. Additional research interests of mine include Internet signaling, packet scheduling, multicast, the use and development of security algorithms and protocols for prevention of denial-of-service attacks, secure multimedia services, and resource reservations.

7. Over the course of my career in the field of digital communications technology I have co-developed a number of Internet protocols (or supervised their development at the Internet Real-Time Lab). Broadly speaking, Internet protocols are generally accepted sets of rules governing how different types of Internet communications are to be structured so that they may be efficiently transported on, and intelligibly sent and received by devices connected to, the Internet. A number of the protocols that I have developed are now used by almost all Internet telephony and multimedia applications. Among the most prominent are:

- Real-time Transport Protocol (RTP): a network protocol for transmitting audio and video services over Internet Protocol networks, used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconferencing and television services.
- Real-Time Streaming Protocol (RTSP): a network control protocol designed for use in entertainment and communications systems to control (rather than transmit) streaming media services, allowing end users to issue VCR-style commands, such as *play*, *record* and *pause*, to facilitate real-time control of the media streaming
- Session Initiation Protocol (SIP): a signaling protocol used for initiating, maintaining, and terminating real-time multimedia communication sessions in applications of Internet telephony for voice and video calls, in private IP telephone systems, in instant messaging over Internet Protocol networks as well as mobile phone calling.

8. My current professional associations include the Institute of Electrical and Electronics Engineers (IEEE), of which I was named a Fellow in 2006 in recognition of my contributions to the design of protocols, applications, and algorithms for Internet multimedia. I have been a member of the Board of Governors of the IEEE Communications Society, past Chair of the IEEE Communications Society Technical Committee on Computer Communications, and past Co-Chair of the IEEE Communications Society Internet Technical Committee. I am also a member of the Association for Computing Machinery (ACM), and served as Vice Chair of ACM's Special Interest Group on Data Communications and the Internet (SIGCOMM).

9. I have also been a member of the Internet Architecture Board (IAB), a committee of the Internet Engineering Task Force (IETF) with responsibility for, among other matters, providing architectural oversight of Internet protocols and procedures, managing Internet standards documents (the "RFC" series) and protocol parameter value assignment. The IAB also acts as an advisory board to the Internet Society (ISOC), the internationally recognized body committed to the open development of Internet standards, protocols, and technical and administrative infrastructure. I also served on the Internet2 Applications, Middleware and Services Advisory Council and have led a working group in the National Science Foundation's GENI (Global Environment for Network Innovations) project, which provides a virtual laboratory for networking and distributed systems research and education.

10. I also serve on a number of conference and journal steering committees, including for the IEEE/ACM journal Transactions on Networking, a bi-monthly publication of high-quality papers that advance the state of the art in communication network research, including theoretical research presenting new techniques, concepts, or analyses, as well as applied contributions reporting on experiences and experiments with actual systems. In the past, I have chaired or co-chaired various IEEE and ACM annual global conferences in the field digital communications technology.

11. I have published more than 250 journal and conference papers, and more than 70 Internet RFCs. (RFCs are publications documenting Internet specifications, communications

protocols and procedures adopted as standards by the IETF, but from time to time are also informative in nature, describing research or innovations applicable to the working of the Internet and Internet-connected systems.) A list of my publications, including all publications I have authored in the previous 10 years, may be found in my curriculum vitae, a copy of which is attached to this declaration as Exhibit A. I have also been editor of several periodicals in the field of computer science, including "Computer Communications Journal," "ACM Transactions on Multimedia Computing," and "ComSoc Surveys & Tutorials," "IEEE Transactions on Image Processing," the "Journal of Communications and Networks," "IEEE/ACM Transactions on Networking," and "IEEE Internet Computing Magazine."

12. In 2013, I was inducted into ISOC's Internet Hall of Fame, in recognition of my contributions to the development of key Internet protocols, including the RTP, RTSP, and SIP protocols noted above. Among other awards, I received the New York City Mayor's Award for Excellence in Science and Technology, the VON Pioneer Award by the Voice-over-Net Conference, the IEEE Technical Committee on Computer Communications Outstanding Service Award, and the IEEE Region 1 William Terry Award for Lifetime Distinguished Service to the IEEE.

**FACTS AND INFORMATION CONSIDERED**

13. For purposes of preparing this declaration, I have relied on (and cite herein) various types of sources, including: (i) Internet standards documents adopted and published by the IETF, known as RFCs, *see* paragraph 11, above, available at https://www.rfc-editor.org/search/rfc_search.php; (ii) public registries and other websites where information concerning assigned protocol and port numbers, IP addresses, and the like, may be found; (iii) various publicly available statistics and technical information concerning Internet infrastructure; (iv) information obtained from manufacturer websites; (v) standard college textbooks, written by well-established leaders in the field, that have become the accepted teaching materials for engineering and computer science students entering the field of computer networks; and (vi) my own knowledge of and familiarity with the technology and operation of global communications networks.

14. As appropriate, I also refer to documents and information produced by Wikimedia in discovery proceedings in this case, and to official U.S. Government documents publicly describing, in unclassified terms, the operation of NSA Upstream surveillance. A list of the documents provided to me by Justice Department counsel, and which I have also reviewed, is attached as Exhibit B. In reaching the conclusions stated herein I have not considered nor have I been provided with any classified or other non-public information concerning the Upstream program.

## SUMMARY OF CONCLUSIONS

15. Principally, I have been asked to evaluate Wikimedia's assertion that the NSA, in the course of conducting Upstream surveillance, must as a matter of technological necessity be intercepting, copying, and reviewing at least some of Wikimedia's electronic communications that traverse any Internet backbone "link" monitored by the NSA. For the reasons I explain at length below, I conclude that Wikimedia's assertion is incorrect. Based on what is publicly known about the NSA's Upstream collection technique, the NSA could be conducting Upstream-type surveillance, at least as envisioned by Wikimedia, in a number of technically feasible, readily implemented ways that would not involve NSA interaction with Wikimedia's online communications.

## INTERNET INFRASTRUCTURE

16. Technically speaking, the Internet is a global collection of networks, large and small, "interconnected by a set of routers which allow them to function as a single, large virtual network." (RFC 1208, 1991) In other words, it is a network of networks, owned and operated by thousands of private and public entities across the world, including telecommunications service providers, governments, and non-profit organizations. There is no precise count of the number of networks that together make up the Internet, but currently there are approximately 62,000 autonomous systems (networks or collections of networks managed and supervised by large entities or organizations) with their own identifiers (Autonomous System Numbers) assigned by the global Internet Assigned Numbers Authority (IANA). These include networks operated by

Columbia University (AS 14), the Wikimedia Foundation (AS 14907), Google (AS 15169) and large carriers such as Verizon (AS 702 and others). Consisting of servers, communication links, and intermediate devices that route information from one network to another ("routers"), this infrastructure allows any device connected to this network of networks to send information to any other connected device (subject to restrictions imposed by the sender or recipient). These network devices, even though manufactured by many different companies, can communicate with one another since they use a common set of agreed-upon technical standards.

17. To communicate over the Internet an individual user must obtain a connection from an Internet Service Provider ("ISP"), either directly or indirectly through an organization such as an employer, or an Internet café (for example, a Starbucks). Typically, an ISP is a private company that provides subscribers access to the Internet for a periodic fee. Subscribers to an ISP's services can be individuals, businesses, educational institutions, government agencies, or other organizations. An ISP maintains one or more local facilities, referred to as points of presence (POPs), at which subscribers can connect with the ISP's network and thereby gain access to the rest of the Internet. Access can be provided via the twisted-pair copper cables originally installed for telephone service, coaxial cable also used to provide cable television service, fiber-optic cable, or wireless satellite signal.

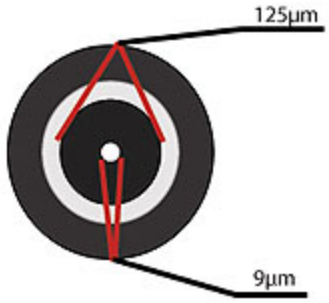
18. In a residential setting the connection is ordinarily made through a device located at the subscriber's home (and often supplied by the ISP) called a router or modem. (Increasingly, however, some individual Internet users have "cut the cord" and only use services provided by cellular telephone networks.) In a business, government agency, or other large organization, the device used by an individual will be part of a local area network (LAN) operated by the organization. The local area network is then connected to the network of a local or regional ISP with which the organization has contracted. The networks of local and regional ISPs in turn connect, at locations known as regional points of presence, to the networks of still larger ISPs, the largest of which are so-called "Tier 1" telecommunication service providers such as AT&T, CenturyLink, Cogent, Verizon or their international equivalents such as NTT or Deutsche Telekom.

19. Tier 1 and other large carriers maintain high-capacity terrestrial fiber-optic networks, generally known as Internet "backbone" networks, which use long-haul terrestrial cables to link large metropolitan areas across entire nations or regions. (Shown below are the North American parts of Cogent's fiber-optic network.) Data travel across these fiber-optic cables in the form of optical signals, or pulses of light. Each fiber-optic cable contains between 4 and 432 glass fibers, with strand counts of around 144 common.

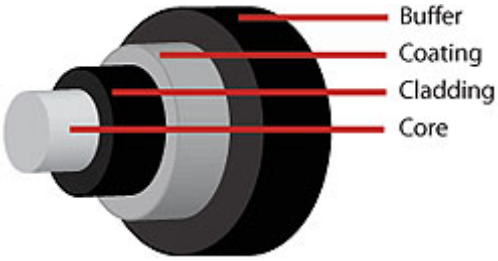



*Cogent US domestic fiber network*

Each fiber has at its core a thin, flexible strand of glass, about 9 micrometers thin, surrounded by another glass strand of 125 micrometers. (A micrometer is one-millionth ($10^{-6}$) of a meter. A human hair has a diameter of between 17 and 181 micrometers.) Data is transmitted by lasers, carried long distances through the insertion of optical amplifiers, and received by photo detectors.




*Fiber-optic strand*

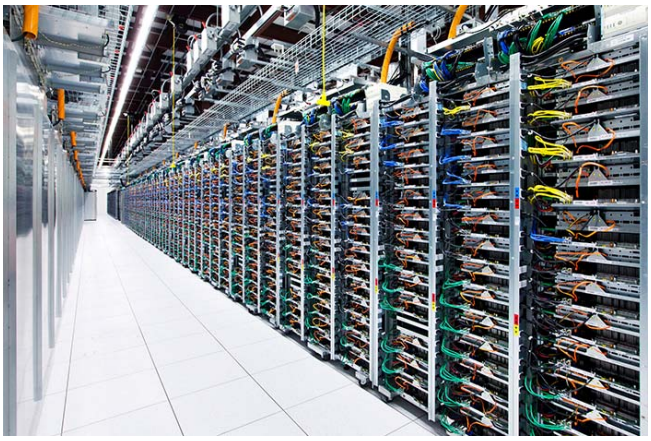



*Fiber-optic cable*

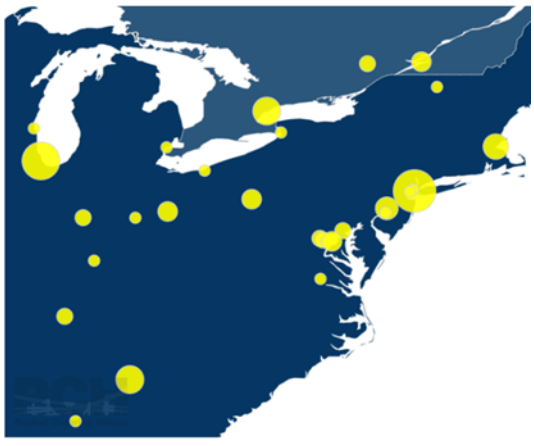


*Buried fiber cable*

20. To make possible communications between users linked to one provider's network with users linked to another's, Tier 1 providers typically interconnect (link) their networks either directly, at facilities known as private peering points, or through public Internet exchange points (IXPs). In an Internet exchange, many different telecommunication carriers can link with each other, exchanging traffic. For example, the Amsterdam Internet Exchange (AMS-IX) (shown below) connects 824 different networks, using 1,423 ports (connections), and carries about 5 terabits (5 billion bits) per second of traffic during the peak hour of the day.[1] A public directory[2] lists 905 such IXPs, differing greatly in the number of carriers that interconnect at each and the total volume of traffic carried.



AMS-IX Internet exchange (Amsterdam)[3]



*Map of IXPs in eastern United States (source: PCH)*

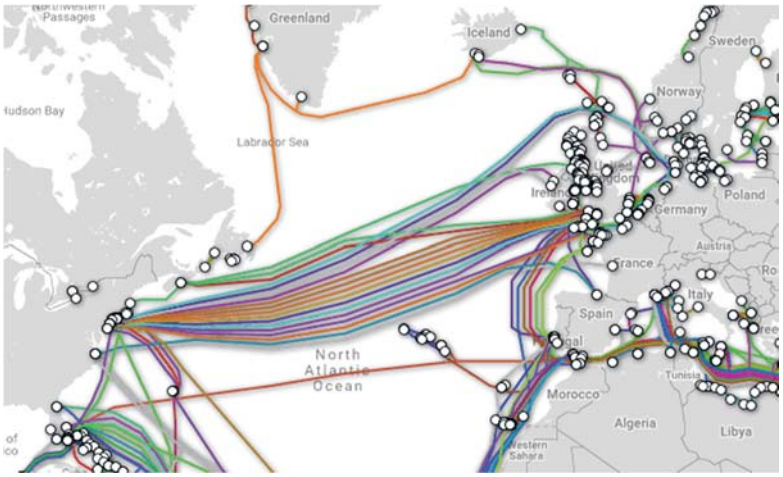
[1] https://ams-ix.net/technical/statistics

[2] https://www.pch.net/ixp/dir

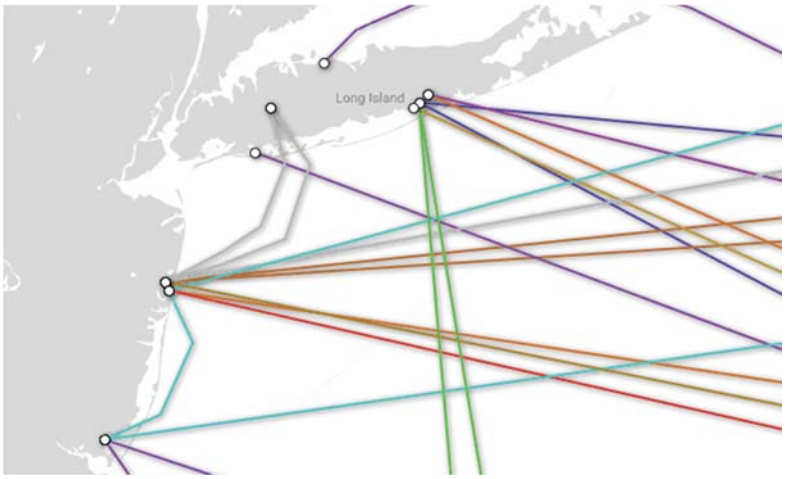
[3] https://pcmweb.nl/artikelen/internet/zo-werkt-ams-ix-alles-over-het-grootste-internetknooppunt-ter-wereld/

21. In addition to long-haul terrestrial cables, the Internet backbone also includes transoceanic cables linking North and South America with each other and with Europe, Asia, the Middle East, and Africa. These undersea cables are laid directly on the ocean floor, and make landfall at points known as cable landing stations. Technologically speaking, there is no fundamental difference between long-haul terrestrial and transoceanic links. Both types use buried fiber cable with optical amplifiers placed at regular intervals, although the hostile environment of the oceans and the difficulty of providing power to amplifiers far from shore influence design details. As an example, the recently-completed MAREA cable has landing points in Virginia Beach, Virginia and Bilbao, Spain, and is composed of eight fibers delivering a total of 160 terabits per second (160,000 billion bits per second). The fiber bundle, encased in heavy-duty metal shielding, has a diameter similar to a garden hose and is placed directly on the ocean floor, except for the shallow stretches near the landing stations, where it is buried to protect it against ship anchors and other disturbances.

22. The map below, provided by TeleGeography, illustrates some of the Internet-carrying fiber-optic cables linking the east coast of the United States to Europe.




The map enlargement below, from the same source, shows that most east coast transatlantic fibers originate from a few landing sites in New Jersey and on Long Island.




23. At each shore location, cable landing stations connect the transoceanic cable to terrestrial cable networks. An example of a cable landing station (Cape Broyle, Canada) is shown below, drawn from the manufacturer's web site.[4] It contains fiber amplifiers, management systems, and possibly Internet routers. The adjacent picture shows the inside of the same facility, showing fiber racks and ceiling cable trays. A terrestrial cable then connects the landing station to the nearest Internet exchange point (IXP), where multiple service providers then link to the terrestrial cable.



[4] http://americanmanufacturedsystemsandservices.com/products-services/products/cable-landing-stations/new-cable-landing-project.html

24. Using this infrastructure, every device connected to the Internet can communicate with every other device, no matter where located or to which providers it is connected. While the process is usually not apparent to the individual user, a communication (such as an email) being sent from one device to another across the country, or across the globe, can travel through numerous other networks en route to its destination. If the communication is traveling to a destination outside of the network of the user's ISP, it will flow onto the networks of Tier 1 or other larger providers, typically reached via an Internet exchange point, before reaching its destination via regional and local networks on the receiving end. If an international communication, it may also be carried on one or more transoceanic undersea cables, traversing cable landing stations as it exits one continent and makes landfall on the next. Such communications may traverse the networks of anywhere from one to maybe a dozen different carriers. Usually, the path is roughly similar to the shortest geographic route, but business relationships and the availability of interconnection points and transoceanic links may lead to detours, similar to how airlines may use hub airports to connect smaller or more far-flung cities.

**TRANSMISSION OF COMMUNICATIONS ON THE INTERNET**

25. Generally speaking, to send a communication on the Internet, the transmitting device (e.g., a personal computer, a cell phone, or the computer—a.k.a. "server"—on which a website is physically stored) first converts the communication into one or more "packets." Packets are relatively small chunks of digital information that can be transported more efficiently than transporting communications (such as entire webpages, or large documents) whole. Packets are typically between a few tens of bytes and 1,500 bytes long, where each byte, roughly speaking, can carry one text character of information. A brief discussion of network protocols and "layers" is helpful to understanding how the packets comprising a communication travel across the Internet.

26. In all communications networks, including the Internet, communicating entities need to agree on a set of technical conventions concerning how to exchange information. These conventions are generally called protocols. "A protocol defines the format and order of messages

exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event."[5] Most telecommunications protocols are defined in engineering specifications, drawn up by international bodies and revised periodically. For the Internet, protocols are primarily defined by the Internet Engineering Task Force (IETF), discussed above, in documents known for historical reasons as RFCs. Each protocol operates and serves its function within a "layer" of the communications network architecture. The concept of layering is a way of functionally sub-dividing a communications system into subsystems, or "layers," of similar functions that provide services to the layer "above" and receive services from the layer "below."

27. In the most widely used network model, the Internet protocol suite, the layers from the "bottom" to "top" of the "stack" are the physical, data link, network, transport, and application layers. For purposes here, the primary layers of interest are the physical, network, transport, and application layers. The physical layer transports electrons or photons between routers and switches, e.g., via fiber-optic or copper cable. The network layer allows two devices on the Internet to communicate with each other by making it possible for packets to travel and be exchanged across many links and networks of different providers using differing technologies. The Internet Protocol, now in two different versions, is the only widely used network-layer protocol at the moment. The transport layer ensures that the receiver can detect whether the information has arrived without error, with the Transmission Control Protocol (TCP) as the dominant protocol. TCP also retransmits any packets that may have been lost by the network and makes a sequence of packets appear as a stream of data and thus hides the packet nature of the Internet from applications using the protocol. UDP, the other transport protocol, does not provide reliability and in-order delivery. Finally, the application layer makes possible the transmission of various communications applications, such as email, or web pages, using protocols specific to each application, such as the Simple Mail Transfer Protocol (SMTP) and the

[5] J. Kurose and K. Ross, "Computer Networking: A Top-Down Approach," p. 5 (Pearson, 2017).

Internet Messaged Access Protocol (IMAP) (both for email), and the Hyper Text Transfer Protocol HTTP (for web pages). As a rough analogy to road networks, the asphalt is the physical layer, the trucks and cars offer network services, a shipping company offers a transport service, and an e-commerce company provides the application service.

28. When a communication is broken into separate packets, each packet includes (i) a "header," that is, the routing, addressing, and other technical information required by the transport protocol to facilitate the travel of the packets from their source to their intended destination, and (ii) a "payload," that is, a portion of the contents of the communication being transmitted. A rough analogy can be drawn between the transmission of packets and delivery of mail by the postal service. A business letter has a "header" containing the sender address, a date ("time stamp") and the recipient address, in addition to various processing indications, such as confidentiality markings or signatures. The letter is then placed in an envelope for delivery that displays this "header" information, but contents of the letter remain invisible to the postal service. The manner and timing of the letter's delivery is unaffected by such factors as the contents, language, or format of the letter.

29. Each layer of the communication stack uses a different header, corresponding to that layer's purpose. For our purposes here, I mainly focus on the network and transport layers. The packet headers for the network and transport layers contain three relevant pieces of address and routing information: (i) the packet's source and destination Internet Protocol (IP) addresses and (ii) protocol numbers, in the network layer header; and (iii) the source and destination ports, in the transport protocol header.

30. IP Addresses: IP addresses are unique numeric identifiers assigned to particular computers, devices, or systems connected to the Internet, and which, as the name suggests, are used by the Internet Protocol at the network layer to send data from one computer or other online device to one or more other devices, and back. IP addresses may be analogized, as in the example above, to the destination and return addresses on an envelope sent through the mail, or to telephone numbers identifying the source and destination of a call. On the telephone

network, telephone switches rely on telephone numbers, area codes, and country codes to route calls locally, within the same local exchange, and long distance. On the Internet, IP addresses fulfill a similar function.

31. Currently there are two versions of IP addresses in use. Since the 1980s the Internet has used so-called IP version 4 addresses (RFC 791, 1981), abbreviated as IPv4. There are approximately four billion such addresses. For example, the web server hosting Wikipedia (Wikimedia's largest website) has an IPv4 address written as 208.80.154.224 in the US. (It may use other addresses elsewhere.[6]) The growth of the Internet, primarily through mobile devices, has outstripped the supply of IPv4 addresses, so a new version, IP version 6 (IPv6) has been adopted that uses a greater number of characters, thus allowing for as many as 340 undecillion ($10^{36}$) addresses. That is sufficient to assign as many addresses as the current IPv4 provides to every star in the universe. In the United States, the Wikipedia server currently uses the IPv6 address 2620:0:861:ed1a::1. Many computers "speak" both protocols; web servers, including the Wikipedia servers, may deliver content using either Internet protocol, depending on the computer connecting to the server.

32. Each ISP or other large enterprise with a fixed presence on the Internet acquires blocks of IP addresses from the appropriate regional Internet registry affiliated with the IANA. For example, the American Registry for Internet Numbers (ARIN) allocates blocks of IP addresses to large enterprises in the United States and Canada. Columbia University has been assigned the 65,536 IP addresses from 128.59.0.0 to 128.59.255.255. Comcast uses, among many other IPv4 address blocks, the roughly eight million addresses starting at 50.128.0.0. There are public databases that record, with very high accuracy, which address blocks are used by what entities, at least at the granularity of ISPs or other large organizations that have assigned autonomous system (AS) numbers, like the Wikimedia Foundation (ASN 14907).

[6] Sites such as https://www.whatsmydns.net/ can be used to determine the IP addresses of a domain (e.g., a website) as they would appear from various geographic locations.

33. IP addresses can be assigned on a permanent or temporary basis, referred to respectively as "static" and "dynamic" addresses. Static IP addresses can be assigned directly to a "self-hosting" organization by the regional Internet registry (as in Wikimedia's case), or indirectly to businesses or other organizations that obtain Internet access via ISPs. (ISPs, after obtaining their allocations of IP address blocks from the registry, in turn assign smaller blocks of fixed addresses to their business customers.) Static IP addresses almost never change. Fixed IP addresses are necessary to run servers, as a server's IP address needs to be disseminated to client (user) computers and mobile devices that want to connect to it. For example, the IP addresses of the servers that host Amazon.com, or Wikipedia.org, must remain unchanging if online shoppers, or Wikipedia's readers and contributors, are to reach them over the Internet. As a rough analogy, static IP addresses are like business phone numbers, which typically do not change for years since they are advertised on business cards and painted on delivery vans. So that Internet users are not required to ascertain, or memorize, the IP addresses of every website they visit, a database service called the domain name service (DNS) translates the names that users type into their browsers, e.g., Wikipedia.org, into Internet addresses, e.g., 208.80.154.224.

34. While the business customers of ISPs may be allotted a fixed block of IP addresses, assigned permanently, ordinarily residential customers get exactly one "dynamic" IPv4 address at a time, assigned on a temporary basis. Dynamic IP addresses may be assigned for a day, an hour, or some other period of time, depending on the needs, resources, and business practices of a particular ISP, after which they are assigned to other customers. An ISP may even assign a particular IP address to a home customer only for the specific length of time (session) that the customer is connected to the Internet, after which the IP address may be released and assigned for temporary use by another customer. (Consumers may be assigned a block of IPv6 addresses, but again without any claim to keep that particular block.)

35. Ports: IP addresses alone are not sufficient to operate networks having multiple functions. For example, the same server may host a web service, an email service and a voice-over-IP (Internet telephony, a.k.a. VoIP) service. The operating system on the server, such as

Windows or Linux, uses *port numbers*, carried in the transport layer protocol (typically TCP or UDP), and included in the header of each communication packet, to distinguish packets destined for the web service from those meant for the email or VoIP services. Likewise, on the user's end, a client computer (a home or office computer, or mobile phone) may run multiple applications for various online activities, such as web-browsing, sending and receiving email, or voice communications using VoIP technology. The user's device also uses port numbers contained in packet headers to ensure, for example, that pages downloaded from a website are routed to the user's browser, not his or her email application, and vice versa.

36. While IP addresses used to route a communication to a particular destination device can be analogized to the street address on a letter, or to a telephone number, port numbers are roughly analogous to the apartment numbers at a multi-unit dwelling, or individual extensions to a business telephone number. Port numbers for common applications like web-browsing and email, each with its own application-layer protocol, are maintained in a common industry registry maintained by the IANA. Some common port number assignments are in the table below; they are generally numbers between 1 and 49,151.

| Port number | Protocol | Application |
|---|---|---|
| **20** | ftp | File transfer |
| **22** | ssh | Remote login |
| **25** | SMTP | Mail delivery between servers |
| **53** | DNS | Domain name system (host name lookup) |
| **80** | HTTP | Web pages, unencrypted |
| **123** | NTP | Network time (clock) synchronization |
| **143** | IMAP | Remote email message access |
| **443** | HTTPS | Encrypted web pages, using SSL/TLS |

| | | |
|---|---|---|
| **587** | SMTP | Email submission protocol, from client to server |
| **993** | IMAP | Email access, encrypted using TLS |
| **5060** | SIP | VoIP session setup |

37. It is possible to run network applications on non-standard ports, but then users on both ends of the communication have to be aware that this is being done. For example, http://portquiz.net:8080/ is a website that uses port 8080, but needs to indicate that fact by including the port number in the web address (URL). Some applications, such as the media (voice or video) components of voice-over-IP, do not have fixed port numbers; rather, devices on each end of the conversation agree on suitable port numbers on a call-by-call basis.

38. Protocol Numbers: Protocols associated with various layers of the network architecture are also assigned numbers maintained in a registry by the IANA. Protocol numbers are also included in packet headers and used by receiving devices to determine the appropriate protocols to apply for interpreting and acting on each packet upon arrival.

39. Once a communication has been broken into constituent packets by the transmitting device, the job of ensuring that the packets travel an appropriate path across the Internet from their source to their destination IP address is performed by devices known as routers and switches. Routers and switches are specialized computers, located at strategic network points, that take on a similar role for the Internet as switches on the telephone network. That is, their basic function is to determine where on the Internet to send packets next. Packets constituting a single communication can travel through several to as many as dozens of routers and switches to reach their destination. Typically, so-called carrier- or enterprise-grade routers are located at ISP points of presence (POPs), peering stations, or Internet exchanges, routing packets from one network to another. A large router commonly found in such Internet exchanges is shown below. Carrier- or enterprise-grade switches are typically located at points of presence where different legs of the same carrier backbone network interconnect, and forward packets from one leg of the network to another.



*Juniper router ((c) Juniper Networks)*

40. To perform its function, each router or switch along a packet's path "decodes" the incoming light pulses from the connected fiber-optic cable and reconstitutes the individual packets for processing. The router or switch then scans each packet's header information, including its destination IP address, and matches the address against an internal routing table. The routing table contains rules (updated by a routing protocol) determining the direction in which packets with addresses falling in particular IP ranges should be forwarded. This exercise may leave the router or switch with a choice of anywhere between three and hundreds of possible next-leg destinations for the packet. The routing protocol can also be used to convey performance-based rules for determining which of the available paths to choose. This allows the router or switch to find a connection with good performance, avoid congested connections, detour packets around failed network links, and use newly available connections, somewhat similar to the manner in which Google Maps updates the fastest route to take between a user's starting point and his/her destination. The largest routers and switches, those used to handle exchanges of communications data at major intersections on the Internet, handle millions of data packets every second.

41. While, in theory, each packet in a single communication could take a different path across the Internet, in practice packets traveling between two points on the Internet generally follow the same path for long distances, just like most motorists traveling between New York City and Washington, D.C., take Interstate 95, following different possible paths (like different county

roads, or neighborhood streets) only when nearing their destinations, or to avoid traffic jams. In particular, since transoceanic connections are only added and removed infrequently, and since most carriers only have a few links that they use, any traffic between international destinations is likely to keep using the same fiber links for months, if not years, except for routing around any outages. Generally, traffic takes the shortest route, subject to business arrangements between carriers. For example, packets comprising an email sent from New York to Amsterdam will traverse the Atlantic Ocean via undersea cable to a landing site in northern Europe, rather than take a circuitous route via the Pacific Ocean, or even a southern route across the Atlantic via Africa.

42. To protect the privacy and integrity of information, users sending data across the Internet may choose to encrypt their traffic, i.e., convert the data into code by a mathematical transformation, so that it can only be read by parties who have the encryption key. Generally, modern encryption techniques are considered to be unbreakable by any third party that does not have access to the key, even if the encryption mechanism is known. The most common encryption mechanism is the Transport Layer Security (TLS) protocol, which operates at the transport layer, one below the web HTTP protocol. The combined use of TLS and HTTP is commonly referred to as HTTPS, even though it is not a single protocol and TLS can also be used for other applications. Use of the encrypted HTTPS protocol is designed to ensure that information sent to or from a web site can only be read by the user's web browser and the host web server, but not third parties, including entities capable of copying packets en route between the browser and the web server. HTTPS offers the exact same functionality of retrieving web pages, but ensures that the web browser connects to the correct web server, and that no third party can read the content of the communications. Despite its relation to HTTP, HTTP-over-TLS (HTTPS) has been assigned a different port, port 443 (the unencrypted HTTP protocol is assigned port 80), allowing web browsers and web servers to distinguish encrypted from unencrypted information by the port number.

43. Increasingly, most popular websites, including those of the Wikimedia Foundation, use HTTPS or at least offer their content via both HTTP or HTTPS. In fact, given the commonality of encryption today, most entities with an Internet presence offer an encrypted version of their content, and the temporary use of unencrypted content to, for example, support legacy applications that have not yet made the transition, is increasingly rare.

44. Once the packets making up a communication arrive at the receiving computer or smartphone, the operating system of the receiver reassembles the packets into the original communication, such as a web page or email, even if the network between the sender and receiver discards, corrupts or reorders some of the packets. As noted earlier, TCP, a transport layer protocol, performs this service, by retransmitting missing or corrupted packets.

**PUBLICLY AVAILABLE INFORMATION ABOUT NSA "UPSTREAM" COLLECTION**

45. NSA "Upstream" collection of communications is described, in general terms, in a number of official public reports issued by the Government, albeit not all of them authored or released by the NSA. Because such reports are relied on by Wikimedia in its Amended Complaint to inform its view of how Upstream collection might work, I rely on them as well.

46. According to these reports, once the necessary approvals are obtained from the Foreign Intelligence Surveillance Court, NSA analysts identify non-U.S. persons located outside the United States who are reasonably believed to possess or receive, or are likely to communicate, designated foreign-intelligence information. NSA Civil Liberties and Privacy Office Report, NSA's Implementation of FISA Section 702 at 4 (Apr. 16, 2014) ("NSA Civil Liberties Report), available at https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/nsa_report_on_section_702_program.pdf. Once the NSA has designated such persons as targets, it then tries to identify specific means by which the targets communicate, such as email addresses or telephone numbers, which are referred to as "selectors." See NSA Civil Liberties Report at 4; Privacy & Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA at 32-33, 36 ("PCLOB Section 702 Report") available at https://www.pclob.gov/library/702-Report.pdf. A telecommunications service

provider may then be compelled to provide the Government all information or assistance necessary to acquire communications associated with the selector, a process referred to as "tasking." NSA Civil Liberties Report at 4-5; PCLOB Section 702 Report at 32-33.

47. Upstream collection is one of the methods through which the NSA receives information concerning tasked selectors. Upstream collection occurs as communications transit the Internet backbone within the United States. PCLOB Section 702 Report at 36-37. Under Upstream collection, tasked selectors are sent to a U.S. electronic-communications-service provider to acquire communications that are transiting the Internet backbone. PCLOB Section 702 Report 36-37. Internet communications are first filtered to eliminate potential domestic communications, and are then scanned to capture only communications containing the tasked selector. PCLOB Section 702 Report at 37. Unless communications pass both these screens, they are not ingested into NSA databases. PCLOB Section 702 Report at 37.

**WIKIMEDIA'S CONTENTIONS**

48. Wikimedia alleges in its First Amended Complaint that "[t]he NSA conducts Upstream surveillance by connecting surveillance devices to multiple major internet cables, switches, and routers on the internet backbone inside the United States," for the purpose of "enabl[ing] the comprehensive monitoring of international internet traffic." (Amended Complaint ¶¶ 47, 48). Wikimedia envisions Upstream surveillance as encompassing four processes, some implemented by telecommunications service providers at the NSA's direction:

- **Copying:** the use of surveillance devices, installed at key access points along the internet backbone, to make a copy of substantially all international text-based communications, and many domestic ones, flowing across certain high-capacity cables, switches, and routers.
- **Filtering:** the attempted exclusion of wholly domestic communications from the copied stream of internet data, perhaps using IP filters, while preserving the international communications.
- **Content review:** review of the full content of copied communications for the NSA's search terms, called selectors, including email addresses, phone numbers, IP addresses, and other identifiers believed by the NSA to be associated with foreign intelligence targets.

- **Retention and Use:** the retention of communications containing selectors associated with NSA targets for querying and review by NSA analysts, and sharing of the results with the Federal Bureau of Investigation.

(Amended Complaint ¶ 49)

49. I reiterate that I have not been given access to classified or other non-public information about Upstream surveillance, and so have no knowledge or information concerning the accuracy of Wikimedia's description of the Upstream collection process.

50. Wikimedia maintains that it is "virtually certain" that the NSA "has intercepted, copied, and reviewed" at least some of its communications in the course of conducting Upstream surveillance (Amended Complaint ¶ 60), based on several assumptions. First, Wikimedia asserts that given "the geographic distribution of [its] contacts and communications across the globe," with "individuals in virtually every country on earth," its communications "almost certainly traverse every international backbone link connecting the United States with the rest of the world." (Amended Complaint ¶¶ 60, 61) Second, and critically for purposes of this declaration, Wikimedia posits that "as a technical matter" the NSA "must be" copying and reviewing all international text-based communications transiting any link it is monitoring, in order to "reliably" obtain communications to or from its targets. (Amended Complaint ¶ 62) This is so, according to Wikimedia, because (i) the NSA cannot know beforehand which communications will contain selectors associated with its targets, and so must copy and review them all in order to identify those of interest, and (ii) in order to review the contents of a communication for the presence of a targeted selector, the NSA must first copy and reassemble all the packets making up that communication, requiring that it copy all packets traversing a given backbone link in order to reassemble and review communications in the manner Wikimedia describes. (Amended Complaint ¶¶ 62, 63)

51. On these premises, Wikimedia concludes that "even if the NSA conducts Upstream surveillance on only a single internet backbone link, it must be intercepting, copying, and reviewing at least those communications of [Wikimedia] traversing that link." (Amended Complaint ¶¶ 64) For the reasons I discuss in the following two sections, Wikimedia's conclusion

is incorrect. Even assuming, hypothetically, that the NSA conducts Upstream collection in the manner Wikimedia posits, by connecting collection equipment to routers and switches at links on the Internet backbone, there are a number of methods by which the NSA could be conducting Upstream surveillance without intercepting (much less copying or reviewing) all communications transiting any Internet backbone link it (hypothetically) monitors. Using these methods, the NSA could conduct Upstream surveillance without intercepting, copying, reviewing, or otherwise interacting with communications of Wikimedia. This would be true regardless of where on the Internet, or at how many locations, the NSA conducts Upstream collection.

**WHETHER THE NSA "MUST BE" INTERCEPTING, COPYING, AND REVIEWING ALL COMMUNICATIONS THAT TRAVERSE A GIVEN INTERNET BACKBONE LINK**

52. Wikimedia bases its belief that the NSA, in the course of Upstream collection, "must be" intercepting, copying, reviewing, or otherwise interacting with Wikimedia's online communications on the premises (i) that the NSA must be conducting Upstream surveillance at one or more Internet backbone links, such as peering points, Internet exchanges, points of presence, or cable landing stations, and (ii) that the NSA, at any given link where Upstream collection is conducted, must, as a matter of technical necessity, be intercepting, copying, and reviewing all communications crossing that link (including, therefore, Wikimedia's). I have no information concerning the actual number or location(s) of the site(s) at which the NSA conducts Upstream surveillance, so for purposes of my analysis I accept the first of these premises as given, that Upstream surveillance must be conducted at one or more links constituting the Internet backbone.

53. The second premise, however, is incorrect. As I explain below, there are a number of technically feasible, readily implemented means of conducting Upstream-type surveillance that would not require interception, copying, reviewing, or otherwise interacting with all communications that traverse any Internet backbone link the NSA allegedly monitors. I do not mean to suggest that the NSA is, in fact, conducting its surveillance by any of these means, or that these are the only possible methods by which the NSA could be conducting Upstream

surveillance. As I have stated elsewhere in this declaration, I have no knowledge or information concerning how Upstream surveillance is actually conducted. What I am saying is that, regardless of the number or types of locations on the Internet backbone at which the NSA might be conducting Upstream surveillance, there are at least several practical means for conducting that surveillance, in a manner akin to that posited by Wikimedia, that would not involve intercepting, copying, reviewing, or otherwise interacting with, all communications transiting the links the NSA allegedly monitors, thus disproving Wikimedia's hypothesis that such interception, copying, review, or other interaction with all communications "must be" occurring.

54. There are at least two well-known approaches to obtaining copies of Internet communications at locations other than the sources or destinations of the communications (or an ISP's server), which is to say, while the communications are still in transit. Locations where either of these approaches could be implemented include, but are not necessarily limited to, peering points, Internet exchanges, cable landing stations, and Internet points of presence.

55. Under the first approach, an entity desiring to obtain copies of communications for purposes of surveillance (or otherwise) could intercept the pulses of light carried on an optical fiber through the use of a device called a fiber-optic splitter (also referred to as an optical splitter). As its name suggests, a splitter, when attached to an optical fiber, "splits" the light signals on the fiber, making an identical copy of the communications stream. Through the use of one or more splitters, an exact duplicate of the communications stream flowing over each fiber-optic cable at an Internet exchange point, cable landing station, or other location could be made. The original communications could continue to travel uninterrupted to their intended destinations on the Internet, while copies of all the communications in each stream could be diverted elsewhere for processing to identify communications of interest.

56. Fiber-optic splitters are passive devices that are incapable of copying selectively, that is, they are incapable of copying only certain communications, but not others, according to specified criteria. Hence, the use of fiber-optic splitters to obtain copies of online

communications for surveillance purposes would entail, as alleged by Wikimedia, the copying of all communications flowing across a given fiber-optic link. (Amended Complaint ¶¶ 49, 62)

57. In contrast, the second approach to obtaining copies of Internet communications while in transit would allow for selectively copying only those communications that are deemed more likely to include communications of interest, without copying or otherwise handling those that are not. This approach would be desirable from the perspective of reducing the volume of communications that must be processed (electronically scanned) to identify the communications of interest, which would in turn reduce the associated time and expense. This selective copying of communications can be accomplished through the use of intelligent devices such as routers and switches (specialized computers, as discussed above), operated by carriers, to "mirror" selected communications carried in a given communications stream.

58. "Mirroring" is the technical term for a process which may be described as follows. As discussed in paragraph 40, above, when the light pulses on a fiber-optic cable enter a router, or a switch, the device "decodes" the stream into individual packets, and examines the address and routing information contained in the header of each packet, to determine where on the Internet each packet should be forwarded next. In the course of this process, the router, or the switch, can also "mirror" some or all of the traffic by making copies of selected packets, and diverting the designated copies off-network for separate processing. Almost all carrier-grade routers and switches, of the kind found at Internet exchanges and regional points of presence, are capable of traffic mirroring, as this functionality is required in order to conduct routine operational monitoring of a carrier's network. For example, traffic mirroring is used as a means of detecting denial-of-service attacks (intentionally flooding a device or network with traffic to force a shutdown and render it inaccessible to its intended users), or of ensuring that a carrier's traffic-routing policies are being properly implemented. Traffic mirroring does not interfere with the delivery of packets and is invisible to both the source and destination of the traffic.

59. Cisco Systems, the largest vendor of carrier-grade routers (based on market-share data from Dell'Oro and IDC[7]), describes the traffic-mirroring process as follows:

> "Traffic mirroring, which is sometimes called port mirroring, or Switched Port Analyzer (SPAN) … enables you to monitor Layer 3 network traffic passing in, or out of, a set of Ethernet interfaces. You can then pass this traffic to a network analyzer for analysis. Traffic mirroring copies traffic from one or more Layer 3 interfaces or sub-interfaces and sends the copied traffic to one or more destinations for analysis by a network analyzer or other monitoring device. Traffic mirroring does not affect the switching of traffic on the source interfaces or sub-interfaces, and allows the mirrored traffic to be sent to a destination next-hop address."[8]

60. Traffic mirroring can be employed to provide a collecting entity with access to select copies of communications transiting a particular Internet link, using fine-grained controls known as access control lists (ACLs). Routers are programmed using ACLs to determine whether packets are forwarded or blocked at a given router interface, that is, a given link between the router and another device.[9] Each of a router's interfaces has an associated ACL with criteria defining which types of packets may pass through the interface, and which not. The criteria used include a packet's source or destination IP address, the port number, protocol numbers, or other information contained in a packet header. The router examines the header information of each packet it processes, and compares it to the criteria established by the ACLs corresponding to each interface, to determine which interfaces the packet may or may not pass through. The router then allows separate copies of the packet to pass, in other words, to be mirrored, through each of the interfaces whose criteria it satisfies, as specified in the associated ACL.

61. Carrier-grade switches, too, can be programmed with access control lists, and, in the same fashion as a router, a switch uses the criteria in the ACLs associated with each of its

[7] https://www.telecomlead.com/telecom-statistics/cisco-leads-service-provider-router-and-carrier-ethernet-switch-market-84577

[8] Cisco, "Configuring Traffic Mirroring on the Cisco IOS XR Software," Manual; available at https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r5-1/interfaces/configuration/guide/hc51xcrsbook/hc51span.pdf.

[9] RFC 4949 (2007) defines ACL: "A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity."

interfaces to determine which packets processed by the switch can pass (be mirrored) through each interface.

62. Carriers routinely use access control lists for a variety of reasons, one of the most important being network security. ACLs prevent packets coming from other carriers' or providers' networks, or from less secure areas of a carrier's own network, from entering more sensitive areas of the carrier's network. The use of access control lists to control the flow of network traffic is sometimes referred to as filtering. Publicly available documentation from Cisco explains the filtering capabilities of its carrier-grade routers using access control lists.[10] The skills required to configure ACLs and load them into a router are part of the repertoire of any trained network technician.

63. Cisco produces two commonly used models of router, the Cisco CRS and ASR, that support traffic mirroring.[11] The figure below, drawn from related Cisco documentation[12] shows a simplified schematic representation of a network topology wherein the network analyzer (i.e., the collecting entity's equipment) receives some or all of the packets sent between transmitting device A and receiving device B. The access control lists (ACLs) supported by Cisco devices can restrict or allow packets' passage based on either source or destination characteristics, including the interface (*e.g.*, a particular fiber), Internet (IP) address, the Internet protocol version (IPv4 or IPv6), the next-layer protocol (*e.g.*, IPsec or TCP), or the port number.[13] The number of ACL entries varies depending on the hardware. For example, the Cisco ASR 9000 router supports up to 4,095 unique access control lists. The practical limits of the number of white list or black list

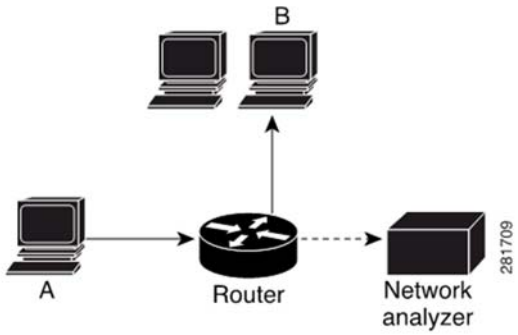
[10] https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-0/addr_serv/command/reference/ir40asrbook_chapter1.html is one example of this capability.

[11] https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r5-1/interfaces/configuration/guide/hc51xcrsbook/hc51span.pdf and https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-1/interfaces/configuration/guide/hc51xasr9kbook/hc51span.html#96505

[12] https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-1/interfaces/configuration/guide/hc41asr9kbook/hc41span.pdf

[13] https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-0/addr_serv/command/reference/ir40asrbook_chapter1.html#wp49507452

entries depends on the router model and may vary. Other router vendors support similar functionality.




64. Traffic mirroring through the use of access control lists could likewise be used in a surveillance context to make only certain packets available for inspection by the collecting entity at any given link on the Internet where surveillance may be conducted. There are several ways in which this could be accomplished. Initially, it would be necessary to establish a link between the router, or switch, directing traffic at that location, and the separate set of equipment used by the collecting entity (wherever situated) to electronically scan the packets to which it is given access for communications of interest.

65. Once the link is established, traffic passing through the carrier's router, or switch, to the collector's equipment could be filtered by various "whitelisting" or "blacklisting" techniques, defined below, that involve configuration of an access control list that allows only packets meeting the ACL's criteria to be copied and passed through the interface to the collector's equipment. For example, if the collecting entity possesses information that communications of interest to it are associated with a particular IP address, or set of IP addresses, then it could request that the carrier provide it only with packets whose source or destination IP addresses match the IP addresses of interest. (I assume for purposes of this discussion that the "tasking" described earlier can go beyond simply enumerating targeted email addresses or phone numbers to the carrier, i.e., include limitations on the protocols, sources and destinations of Internet traffic to be made available for NSA examination.) The carrier, in turn, could configure the ACL of the appropriate interface with a "whitelist" of the specified IP addresses. As a result,

when the router (or switch, as the case may be) examines the header information of each packet it processes, it would, as usual, forward a copy of the packet (as determined by its routing tables) toward the packet's intended destination, possibly create and forward additional copies of the packet through other interfaces, depending on the routine policies and practices of the carrier, and if, but only if, the packet header contains a source or destination IP address on the designated whitelist, create an additional copy of the packet and forward it through the interface with the collector's equipment to the collector's possession and control.

66. Packets not meeting the whitelist criteria would not be copied for, or made available to, the collector's equipment for reassembly, review, retention, or any other purpose, and would not be handled or processed in any way other than would ordinarily occur under the carrier's routine practices.

67. Blacklisting, as the name suggests, is the converse of whitelisting. Tipton and Krause define them as follows in a more general information security context: "Blacklisting consists of banning a list of resources from access. … Whitelisting is listing entities that are granted a set of privileges (access, services, validity, etc.) within an environment. A whitelist is solely used to define what is allowed to be executed, whereas anything that is not included in the whitelist cannot be executed."[14] Blacklisting involves the configuration of an access control list that allows all packets to pass through the interface with the collector's equipment except those meeting the ACL's criteria. For example, the collecting entity might conclude that communications traffic to and from certain IP addresses, perhaps by virtue of the geographic locations or the organizations they are associated with, are of little interest for the collector's purposes, and that these communications burden the processing capacity of its equipment without yielding information of significant value. In that situation, the collector may advise the carrier that it does not wish to receive traffic to and from these "low-yield" IP addresses. In that case, the carrier could configure the ACL corresponding to the interface with the collector's

[14] Harold Tipton and Micki Krause, "Information Security Management Handbook," CRC, 2007.

equipment with a "blacklist" of the specified IP addresses. Once so programmed, the router, or switch, would as usual examine the header of each packet it processes, forward each packet toward its destination on the Internet, create and forward copies of each packet through various interfaces as dictated by the carrier's business practices, and create an additional copy of each packet, and forward it through the interface with the collector's equipment to the collector's possession and control, *except* for those packets with source or destination IP addresses on the designated blacklist.

68. If on examination a packet is found to contain a source or destination IP address on the blacklist, an additional copy of that packet is not created or forwarded through the interface to the control of the collecting entity, and would not be handled or processed in any way other than would ordinarily occur under the carrier's routine practices.

69. Whitelisting and blacklisting techniques can also be used to limit mirroring to particular sources of traffic. For example, if a router at an exchange, landing station, or point of presence is linked to multiple fiber-optic cables used respectively by different carriers, or linked to particular countries, mirroring can be restricted to traffic only from certain carriers' networks, or certain global regions.

70. In addition, whitelisting and blacklisting can be used to mirror only particular kinds of communications based on their protocols. As discussed above, communications of different types, having different protocols, are assigned different port numbers to ensure that user communications, or requests for information, are directed to the appropriate service hosted on the recipient server, and that the response to the user is directed to the appropriate application on the user's computer, cellphone, or other device. The access control list associated with the interface between a router or switch and a collecting entity's equipment can also be configured to whitelist or blacklist distinct types of communications based on their assigned port numbers. Suppose, for example, that the collecting entity is interested only in examining email. Email communications use the SMTP and IMAP protocols, the default ports for which are port 25 and port 143, respectively. If advised by the collecting entity that it only wishes to examine email

communications, the carrier could configure the ACL corresponding to the router interface with the collector's equipment to create additional copies of packets, and forward them to the collector's control, only if the port number contained in the packets' headers is port 25 or 143.

71. On the other hand, the collecting entity may determine that certain types of communications yield little information of value, and simply burden the capacities of its processing equipment. In that event, the collecting entity may inform the carrier that it does not wish to receive communications of that type. The carrier could then configure the appropriate ACL so that packets containing port numbers corresponding to those undesired types of communications are not copied and passed through the interface to the collecting entity's control. For example, as discussed above, the encrypted HTTPS protocol, used to communicate with sites on the World Wide Web, provides a high degree of assurance that communications sent to or from a website can only be read by the user's web browser and the host web server, but not third parties who intercept them in transit. A collecting entity, if it lacks the capability of decrypting HTTPS communications, and therefore can glean no useful information from them, might advise an assisting carrier that it does not wish access to such communications. Because HTTPS communications are assigned port number 443, the carrier could simply configure the access control list for the interface with the collecting entity's equipment so that no packets containing port number 443 are copied and passed to the collecting entity's possession and control.

72. Wikimedia, in fact, posits a highly similar type of scenario in its Amended Complaint. Wikimedia states:

> By some estimates . . . two-thirds of internet traffic consists of video traffic. The NSA could readily configure its surveillance equipment to ignore that traffic, or at least the significant portions of it (e.g., Netflix traffic) that are almost certainly of no interest. Because of the substantial efficiency gains to be had, it is extremely likely that the government engages in this kind of filtering . . . .

Amended Complaint ¶ 59. To achieve the result hypothesized by Wikimedia, the carrier at any Internet link where the NSA might theoretically be conducting Upstream surveillance could "readily," as Wikimedia says, configure the access control list associated with the interface

between the carrier's router or switch and the NSA's surveillance equipment to block transmission of any packets whose source IP addresses correspond to the streaming video services whose traffic the NSA did not wish to have access to.

73. As mentioned above, Wikimedia gives two specific reasons why it believes the NSA nevertheless "must be" copying all the international text-based communications that travel across any given Internet link where it conducts Upstream surveillance. I address both here. First, Wikimedia maintains that because the NSA cannot know beforehand which international, text-based communications traversing a link will contain selectors associated with its targets, it must copy and review them all in order to "reliably" identify those of interest. (Amended Complaint ¶ 62) The foregoing discussion of traffic mirroring demonstrates that this is not necessarily the case. If a collecting entity, by whatever means, were to ascertain to an acceptable degree of confidence that the communications of interest to it are associated with particular IP addresses, then by whitelisting packets containing those IP addresses in their headers, it can reliably obtain the packets of all communications to and from those IP addresses crossing that link, without obtaining access to any other communications crossing that link. Conversely, if the collecting entity ascertained to an acceptable degree of confidence that communications to and from certain IP addresses do not include communications of interest to it, then by blacklisting communications to and from those "low-interest" IP addresses, it could reliably obtain all communications of interest that are crossing that link without obtaining access to any of the blacklisted communications. And in either scenario, the packets not accessed would undergo no handling or processing other than would ordinarily occur under the carrier's routine practices.

74. The question remains, of course, how confident would a collecting entity have to be that it could "reliably" acquire its targets' communications using these more selective approaches, based on IP addresses (or port or protocol numbers), before it would deem them acceptable. Speaking as someone who has studied the economics as well as the technology underlying large-scale network engineering, I would say that the answer to that question

depends on the collector's objectives, capabilities, resources, and competing organizational priorities. So far as this case is concerned, these are all matters known only to the NSA.

75. Second, Wikimedia maintains that the NSA cannot "reliably" obtain its targets' communications without copying and reviewing all international text-based communications traveling across a link because, according to Wikimedia, to review a communication for the presence of a targeted selector, the NSA must first copy and reassemble all the packets making up that communication. (Amended Complaint ¶ 63) This reasoning is flawed.

76. It is not the case that all the packets on a communication link must be collected before the communication of interest can be reassembled. Each set of communication relationships and protocols is independent. For example, an email communication between two parties does not depend on a web transfer, either between those two parties or any other party, and reassembling the web communication is neither necessary nor helpful to obtain or analyze the email communications. Thus, it is sufficient to reassemble only the email-related packets, identifiable by protocol number and port, if email is of interest. All of the packets in a communication to or from an individual target will have a common destination or source IP address, respectively. If the target can be identified by IP address or range of addresses, and if the collecting entity obtains access to all packets crossing the link that contain that address (or an address falling in that range), it will have all the packets making up that communication, and can reconstruct it. Through traffic mirroring, this objective can readily be achieved either by whitelisting packets containing IP addresses associated with communications of interest, or blacklisting communications to and from IP addresses that are likely of no interest. In either case, it would not be necessary, as a technical matter, to copy all packets crossing the link in order to "reliably" reassemble and identify communications of interest, so long as the collecting entity itself were sufficiently confident in its ability to identify the IP addresses of high-interest communications, or communications (and their IP addresses) that are of low interest.

**WHETHER THE NSA "MUST BE" INTERCEPTING, COPYING, AND REVIEWING WIKIMEDIA'S ONLINE COMMUNICATIONS**

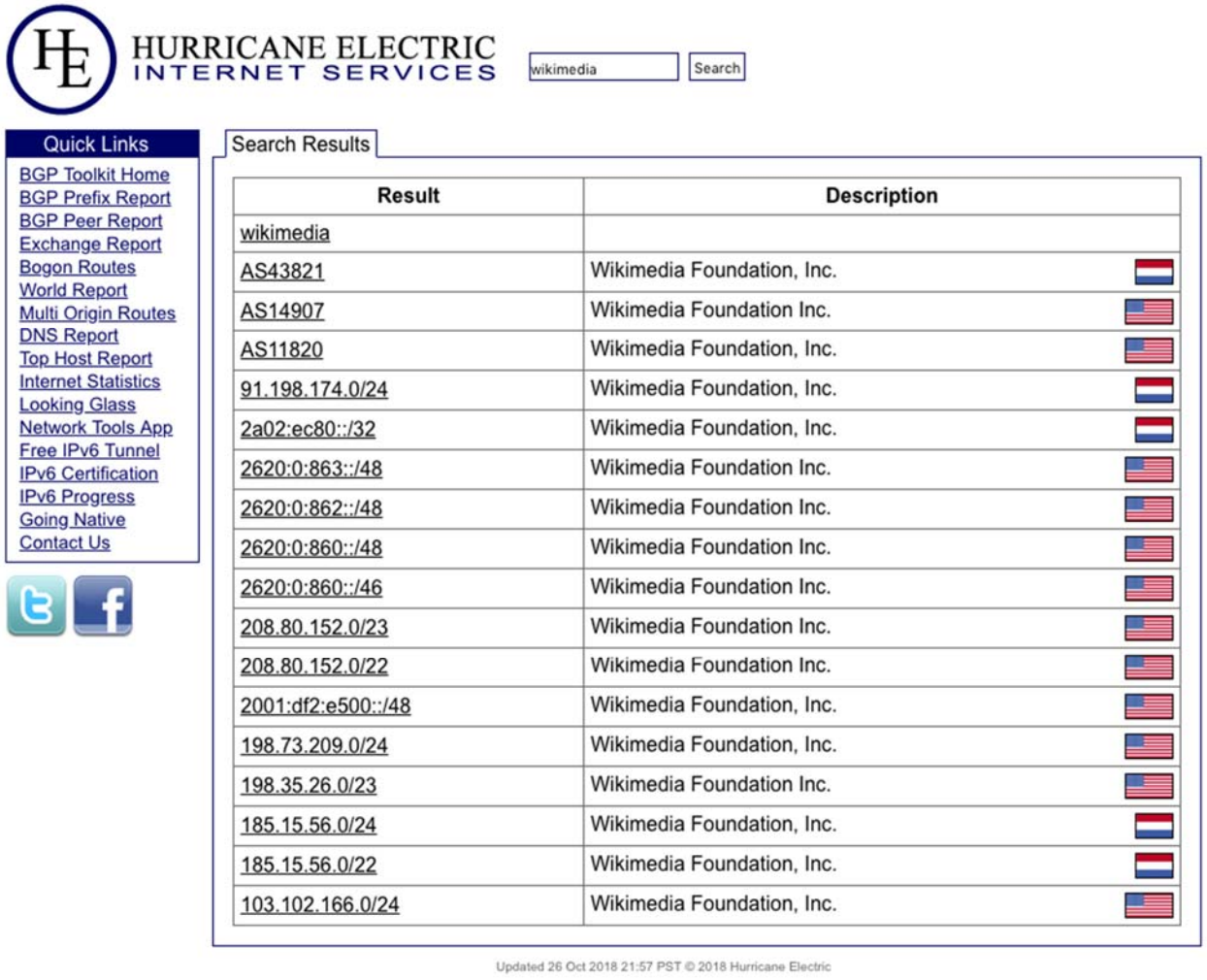
77. In this section I explain how the NSA, through the use of traffic-mirroring techniques such as those discussed in the preceding section, could conduct Upstream-type surveillance in a manner similar to that posited by Wikimedia without intercepting, copying, reviewing, or otherwise interacting with communications of Wikimedia. I emphasize, again, that I do not mean to suggest that the NSA in fact employs any of these techniques in conducting Upstream collection, only that they are technically feasible, readily implemented means by which it could do so without intercepting, copying, reviewing, or otherwise interacting with Wikimedia's communications. I am advised by Justice Department counsel that Wikimedia has identified three categories of its communications that it believes are subjected to Upstream collection processes: (1) communications with and among its "community members," that is to say, individuals who read or contribute to its websites; (2) its server log communications; and (3) communications to and from its staff. I discuss each category below in turn.

78. Category 1 (communications with and among "community members"): In a chart entitled "Technical Statistics for 2017 to 2018 Responsive to ODNI Interrogatory No. 19," Wikimedia describes the first category of its allegedly intercepted communications as "Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other." It specifies three types of communications as falling within this first category, HTTP and HTTPS requests from foreign users to Wikimedia servers in the United States (presumably requests to view or download content from Wikimedia websites); HTTP and HTTPS requests from users in the United States to foreign Wikimedia servers (presumably the same), and SMTP communications from foreign users to Wikimedia servers in the United States (presumably email). In brief, then, Category 1 communications consist of traffic using the HTTPS protocol (i.e., encrypted web traffic), the HTTP protocol (unencrypted web traffic) and the SMTP protocol (email traffic), all destined to a limited number of IP addresses used by Wikimedia, that are also listed in the chart.

79. To my knowledge, the Government has publicly acknowledged that the NSA uses email addresses and telephone numbers as "selectors" to identify communications involving its Upstream targets, but has not publicly confirmed whether or not it uses any other kind of identifier for that purpose. It is therefore unknown (at least publicly) what types of communications other than email or telephone calls, if any, that the NSA acquires via Upstream collection. If, hypothetically, the NSA does not collect web communications, whether due to their volume, because they may be of insufficient interest, or both, then it would stand to reason that the NSA, at any link where Upstream surveillance may be conducted, might not seek access to traffic using either of the current web protocols, HTTP and HTTPS. (If the NSA does not possess the capability to decipher encrypted HTTPS communications—whether it does or does not I do not know—then that is an additional reason it might regard such unreadable communications to be of low interest.) Using a blacklisting approach such as I describe above, the assisting carrier could block any HTTP and HTTPS traffic transiting that link (*i.e.*, packets with port numbers 80 and 443, respectively) from being forwarded to the NSA's collection equipment. Under such a scenario, none of Wikimedia's HTTP or HTTPS communications crossing that link would be intercepted or copied (other than for the carrier's own purposes, if any) and would not be made available to the NSA. If the NSA, for whatever reason, were not interested in collecting web communications, including Wikimedia's, there is no technical reason why it would nevertheless be compelled to intercept, copy, or review them, as Wikimedia suggests.

80. Even if HTTP and HTTPS communications are not excluded, as a general matter, from those the NSA obtains access to for Upstream purposes, Wikimedia's web communications could still be subject to exclusion from the communications provided to the NSA at any given link, through whitelisting or blacklisting. As reflected in Wikimedia's technical statistics chart, Wikimedia has been allocated a number of static (permanent) IP addresses, as is essential for users around the world to access and contribute to its public websites. For the same reason, these addresses are publicly disseminated, and are available from online directories that track organizations' IP addresses according to their assigned AS (autonomous system) numbers.

(Shown below is an example from Hurricane Electric, a well-known Internet backbone carrier.) Additionally, for global routing of international traffic, each router or switch located at a link on a major carrier's network contains an accessible registry, also organized by AS number, of the IP addresses that can be reached via that link. Anyone knowledgeable in the realm of network traffic management would have the skill needed to access these registries and compile a list of all IP addresses associated with any organization, such as Wikimedia, that has been assigned its own AS number. That list could be used, in turn, to exclude communications associated with such an organization, including Wikimedia.




81. Therefore if, at a given link, the NSA was being given access only to communications to or from specified IP addresses (whitelisting), and Wikimedia's addresses were

not among them, then the NSA would not obtain access to any Wikimedia HTTP or HTTPS communications (or communications of any kind), unless users communicating with its websites had been assigned a targeted (whitelisted) IP address. Conversely, if at a given link the NSA were, at its request, not being given access to traffic to or from the IP addresses of certain high-volume but perhaps low-interest sites (blacklisting), such as, hypothetically, Amazon.com, and Wikimedia's sites, then under this scenario, as well, the NSA would receive no access to Wikimedia HTTP or HTTPS communications (or, for that matter, Wikimedia communications of any kind).

82. Regarding the email (SMTP) communications in Category 1, the chart of technical statistics provided by Wikimedia states that the volume of these email communications and the countries from which they are received are unknown. There is no basis, then, on which to assert that these communications with Wikimedia "almost certainly traverse every international backbone link connecting the United States with the rest of the world," the first of the assumptions on which Wikimedia bases its belief that its communications are intercepted by the NSA. (Paragraph 50, above; Amended Complaint ¶ 60) Because the SMTP communications do not satisfy this condition for interception under Wikimedia's own theory, further discussion of these communications is unnecessary for present purposes. Nevertheless, I observe that because all of these communications are received at a sub-set of the same IP addresses as the HTTP and HTTPS communications in Category 1 (as shown in Wikimedia's technical statistics chart), then whitelisting or blacklisting by IP address, as discussed in paragraphs 80-81, above, would also block NSA access to these Wikimedia SMTP email communications as well.

83. Category 2 (server log communications): Wikimedia's technical statistics chart describes the second category of its allegedly intercepted communications, "Wikimedia's internal log communications," as "Apache Kafka log communications" transmitted from Wikimedia servers in the Netherlands to Wikimedia servers in the United States. (Apache Kafka is a commercial data-streaming software application.) These are communications containing server logs, files automatically created and maintained by servers of the activities they perform. A

common example are logs maintained by web servers of user requests to view or download information from a website. These logs typically contain such information as the user's IP address, the time and date of the request, the webpage requested, and the amount of data transmitted. Server logs may be analyzed in aggregate to study traffic patterns, ensure adequate site resources, maintain efficient site administration, and for other purposes. When, as is common, server logs are transmitted elsewhere (to another server) for the performance of such analyses, they are typically encrypted, for security. According to the Amended Complaint, the log communications at issue here are of server logs created by Wikimedia web servers when they receive requests from users seeking to access Wikimedia websites. (Amended Complaint ¶ 93) Wikimedia's technical statistics chart indicates that it encrypts its log communications using an encryption protocol known as IPSec.

84. If the NSA did not wish in the course of Upstream collection to have access to Wikimedia's server log communications, or those of the many other entities that generate such logs, due to their aggregate volume and the relatively limited amount of information they offer (especially if indecipherably encrypted), then it would be a simple matter to block NSA access to those communications, in either of two ways. First, packets encrypted using the IPSec protocol are easily recognized by the corresponding protocol number, protocol 50, contained in their header information. It would be a simple matter at any given link for an assisting carrier to configure the access control list to the interface between its router or switch and a (hypothetical) set of NSA collection equipment to blacklist, that is, to block transmission of, all packets containing protocol 50 in their headers. Second, as shown in Wikimedia's technical statistics chart, its log communications are received at one of the same public IP address ranges as its HTTP, HTTPS, and SMTP communications in Category 1. Like those communications, NSA access to Wikimedia's log communications could be blocked by whitelisting or blacklisting by IP address, as discussed in paragraphs 80-81, above.

85. Category 3 (staff communications): The third and final category of Wikimedia's allegedly intercepted communications, "Communications by Wikimedia staff," are described in

the technical statistics chart as "[l]ogged international" TCP, UDP, and ICMP "connections" using Wikimedia's Office Network or its Virtual Private Network (VPN). "TCP" refers to the Transmission Control Protocol, discussed in paragraph 27, which operates at the transport layer, just beneath the application layer, and allows two devices on the Internet (such as a web server and a user's computer) to establish a connection with one another and exchange streams of data. "UDP" stands for the User Datagram Protocol, another transport layer protocol typically used with applications for which speed is more critical than reliability, such as Internet telephony and video streaming. "ICMP" is the Internet Control Message Protocol, a network layer protocol used by network devices such as routers and servers to send error messages (such as "host unreachable") to other devices when problems are encountered delivering packets.

86. Wikimedia's technical statistics chart does not identify the applications (email, web browsing, VoIP, etc.) used in connection with the TCP and UDP communications identified in Category 3, and so it is unclear whether they are identifiable by port or protocol number. Although the chart specifies that communications conducted over Wikimedia's Virtual Private Network are encrypted using the SSL/TLS protocol described in paragraph 42, it indicates further that not all of its staff communications are sent or received over the encrypted VPN.

87. Nevertheless, the technical statistics chart indicates that Wikimedia's encrypted and unencrypted staff communications are sent from and received at IP addresses that are readily ascertainable from publicly available sources. The IP address range stated for Wikimedia's unencrypted Office Network, 198.73.209.0/24, is discoverable from such sources as the Hurricane Electric directory (see paragraph 80, above, and referenced search results for Wikimedia). (The notation 198.73.209.0/24 in the Hurricane Electric table encompasses the addresses from 198.73.209.0 through 198.73.209.255, and thus includes the address 198.73.209.25 listed as the VPN address in Exhibit 1.) In other words, Wikimedia's staff communications, like its HTTP, HTTPS, and SMTP communications in Category 1, and its log communications in Category 2, could be blocked by whitelisting or blacklisting by IP address, as discussed in paragraphs 80-81, above.

88. In short, at any given Internet backbone link where the NSA might hypothetically be conducting Upstream-type surveillance in a manner posited by Wikimedia, it would be technically feasible for the assisting carrier, through one or more of the traffic-mirroring techniques I have discussed, to configure its routing or switching equipment so that Wikimedia's communications transiting that link are not intercepted, copied, or forwarded to surveillance equipment under the NSA's control.

**RELEVANCE OF THE NUMBER OF SITES AT WHICH UPSTREAM SURVEILLANCE OCCURS**

89. Finally, I briefly address the import of Wikimedia's assertion that the NSA "must conduct Upstream surveillance at many different backbone chokepoints" if it is to "comprehensively and reliably obtain" communications involving its targets. (Amended Complaint ¶ 66) Wikimedia says this must be true because communications to and from individual targets "may take multiple paths when entering or leaving the United States," even "in the course of a single exchange." (*Id.*) Wikimedia's allegation overstates the extent to which communications between the same two endpoints are likely to take different paths across the Internet, and in particular on Internet backbone networks. As I explained above (paragraph 41), barring network outages or other atypical events, in practice packets transiting between two points on the Internet will follow the same path for the great majority of the distance traveled. The path followed from one communication to the next will differ, if at all, only when the constituent packets first make their way toward the Internet backbone, or as they near their destination.

90. The point is a moot one, though. As I have set out above, at any given backbone link where the NSA might hypothetically be conducting Upstream surveillance in a manner envisioned by Wikimedia, there are various traffic-mirroring techniques available that would allow the NSA, as a technical matter, to obtain access to communications of its targets without intercepting, copying, reviewing, or otherwise interacting with communications of Wikimedia. This would remain the case, therefore, regardless of the number of such locations, whether one, or dozens, at which Upstream surveillance might in theory be conducted.

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

Executed in New York, New York, on November 12, 2018.

Henning G. Schulzrinne

HENNING G. SCHULZRINNE

**DECLARATION OF DR. HENNING G. SCHULZRINNE**
***WIKIMEDIA FOUND. V. NSA*, NO. 1:15-CV-00662-TSE (D. MD)**

# EXHIBIT A

# Henning Schulzrinne

Julian Clarence Levi Professor
Dept. of Computer Science
Columbia University
New York, NY 10027
USA

work phone: +1 212 939 7042
fax: +1 212 666 0140
email: hgs@cs.columbia.edu
WWW: http://www.cs.columbia.edu/~hgs
SIP: sip:hgs@cs.columbia.edu

## INTERESTS

*Internet multimedia, policy, services, architecture, computer networks and performance evaluation.* Telecommunication policy; Internet telephony, collaboration and media-on-demand; Internet of things; emergency services; signaling and session control; mobile applications; ubiquitous and pervasive computing; network measurements; quality of service; Internet protocols and services; congestion control and adaptive multimedia services; implementations of multi-media and real-time networks; operating system support for high-bandwidth services with real-time constraints; performance analysis of computer networks and systems.

## WORK EXPERIENCE

**Chief Technology Officer,** Federal Communications Commission (FCC), January 2017–August 2017.

**Senior Advisor for Technology,** Federal Communications Commission (FCC), September 2016–December 2016.

**Technology Advisor,** Federal Communications Commission (FCC), September 2014–August 2016.

**Chief Technology Officer,** Federal Communications Commission (FCC), January 2012–August 2014.

**Engineering Fellow,** Federal Communications Commission (FCC), Sept. 2010–May 2011.

**Professor (tenured),** Dept. of Computer Science and Dept. of Electrical Engineering (joint appointment), Columbia University. August 1996–. Department vice chair, 2002–2003; Department chair, 2004–2009.

**Researcher,** GMD Fokus[1], Berlin, Germany. March 1994 - July 1996. Multimedia systems, ATM performance issues. Deputy department head; project leader TOMQAT, Multicube, MMTng. Lecturer at Technical University Berlin.

**Consultant,** 1994-1996: design and implementation of an Internet packet audio tool for a WWW-based "Virtual Places" shared environment (Ubique, Israel). Consultant on real-time packet audio (Vocaltec, Israel).

**Postdoc,** Distributed Systems Research Department, AT&T Bell Laboratories, Murray Hill, New Jersey. September 1992 – February 1994: designed and implemented BENE network emulator, research in real-time multimedia and electronic publishing.

**Teaching Assistant,** Dept. of Computer Science, University of Massachusetts, January 1992 – June 1992: co-taught senior-level computer networking course.

**Research Assistant,** Dept. of Computer Science, University of Massachusetts, July 1988 – September 1992: research in congestion control and performance evaluation related

[1] GMD - Forschungszentrum Informationstechnik (German National Research Center for Information Technology), Research Institute for Open Communication Systems

to high-speed computer networks. Also assisted in teaching performance evaluation course.

**Research Assistant,** Dept. of Electrical and Computer Engineering, University of Massachusetts at Amherst, January 1988 – July 1988: collaboration with Dr. Wei-Bo Gong in the area of perturbation analysis.

**Teaching Assistant,** Dept. of Electrical and Computer Engineering, University of Massachusetts at Amherst, September 1987 – July 1988: taught discussion section of introductory programming class for engineers (Pascal and Fortran).

**Research Assistant,** Dept. of Electrical and Computer Engineering, University of Cincinnati, March 1985 – August 1987: planning and implementation of speech processing laboratory and networking, tool development, vector quantization research, system administration.

## EDUCATION

**PhD Electrical Engineering,** Department of Electrical and Computer Engineering at the University of Massachusetts, Amherst, September 1992.

**PhD Thesis:** *Congestion Control and Packet Loss for Real-Time Traffic in High-Speed Networks*. Principal advisors: Jim Kurose, Don Towsley and Christos Cassandras.

**Master of Science,** Department of Electrical and Computer Engineering at the University of Cincinnati, Cincinnati, Ohio; with emphasis on digital signal processing (voice coding, software models). August 1987.

**Master's thesis:** *Multi-Stage Vector Quantization for Speech and Image Coding; The DSP Workbench: Distributed Multiprocess System Simulation*. Experimental and theoretical results for a new method of vector quantization and development of a distributed high-level simulator for signal processing applications. Principal advisor: P. A. Ramamoorthy.

**B.S. Electrical Engineering,** (combined with B.S. Industrial Engineering), Technical University of Darmstadt, Federal Republic of Germany, June 1984.

## HONORS AND AWARDS

- IEEE Infocom 2018 *Test of Time Paper Award* for "An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol" (with Salman Baset).
- IEEE Internet award, 2016.
- ACM Fellow, 2015.
- WCNC 2015, "Intelligent Content Delivery over Wireless via SDN", best paper award.
- IEEE Communications Society Internet Technical Committee Distinguished Service Award, 2014.
- Internet Hall of Fame, 2013
- GREE 2013 best paper award ("Wimax in the classroom: Designing a cellular networking hands-on lab")
- 2011 Internet2 IDEA Award winner for "Do You See What I See" tool (Kyung Hwa Kim, PhD Student)
- Region 1 William Terry Award for Lifetime Distinguished Service to IEEE Region 1 (2010)

- IPTComm 2010 best paper award ("Reliability and Relay Selection in Peer-to-Peer Communication Systems")
- IMSAA-08 3rd best paper award for *A New SIP Event Package For Group Membership Management in Advanced Communications* (co-authored with Vishal Singh and Piotr Boni)
- VDE ITG Preis 2008 for *Ubiquitous Device Personalization and Use: The Next Generation of IP Multimedia Communications* (co-authored with Ron Shacham, Srisakul Thakolsri and Wolfgang Kellerer)
- IPTCOMM 2008 Best Student Paper Award for *SIP Server Overload Control: Design and Evaluation* (co-authored with Charles Shen)
- CATT lifetime innovation award (Brooklyn Polytech University) (2007)
- Sputnik Innovator Award (2005)
- IEEE Fellow (2006)
- IEEE ComSoc Technical Committee on Computer Communications (TCCC) Outstanding Service Award 2005
- IEEE Senior Member (2004)
- Internet Telephony 2004 Product of the Year
- Mayor's Award for Excellence in Science and Technology (2004)
- VON Pioneer Award, 2000
- *IEEE Communication Society* Lecturer, 1997
- nominated for ACM Best Dissertation award
- University of Massachusetts Graduate School Fellowship, 1990-1991
- University Summer Research Fellowship 1987
- University Summer Research Fellowship 1985
- German Fulbright Scholarship 1984
- President Electrical Engineering Graduate Student Association 1985/86
  Graduate Outstanding Service award 1986
- German National Scholarship Foundation ("Studienstiftung des deutschen Volkes")
- Regional finalist German Young Scientists Competition (Jugend forscht)

PROFESSIONAL ACTIVITIES

Editorial positions:

- Associate Editor, *Computer Communications*, 2009–
- Editor, *Foundations and Trends in Networking*, 2005–.
- Editor, *ACM Transactions on Multimedia Computing, Communications and Applications*, 2005–
- Associate Editor, *ACM/IEEE Transactions on Networking*, 2000–2008
- Associate Editor, *IEEE Transactions on Image Processing*, 1999–2000
- Guest editor for *IEEE Network Magazine* and *IEEE Internet Computing* on Internet Telephony, May/June 1999
- *Journal of Communications and Networks*, editor (1998–2001), division editor (2001–2004)

- *IEEE Communication Surveys*, member editorial board, 1996–2000, 2002–
- *Internet Computing*, Communications Society liaison editor, 1996–1999, editor, 2008–
- *IEEE Communications Magazine*, Internet Technology feature series editor (1996–1998)
- Guest editor for *IEEE Journal on Selected Areas in Communications* on the Global Internet

Technical program committees:

- *P2P* 2008
- *ANCS (Architectures for Networking and Communication Systems)* 2005
- *ACM Multimedia* 2005
- *SIP 2000–2008*
- *Feature Interaction Workshop (FIW)* 2003, 2005
- *International Conference on Distributed Computing Systems (ICDCS)* 2005
- *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks* (WoWMoM) 2005, 2006
- ACM *Mobihoc* 2002, 2005
- IEEE *INFOCOM* 1994–1996, 1998, 2000–2004, 2006–2019
- *Network and Operating System Support for Digital Audio and Video* (NOSSDAV), 1997–2010, 2012–2014
- *IEEE Global Internet* 1996–2000, 2005, 2007
- *Packet Video Workshop*, 1999, 2000
- *ACM/SPIE Multimedia Computing and Networking*, 1998
- *Open Architectures and Network Programming (OPENARCH)* 1998, 1999
- NSF review panel, 1999, 2002, 2003, 2004, 2006, 2007, 2008, 2010, 2011, 2015
- *IEEE Global Internet*, November 1996 (conference technical program vice chair)
- W3C *Real-Time Multimedia Workshop* (RTMW), October 1996
- *International Conference on Network Protocols (ICNP)*, 1996, 2008
- *Workshop on Integration of IP and ATM*, 1996

Advisory boards and committees:

- North American Numbering Council (NANC), a federal advisory committee (FCC, 2017–2018)
- Computing Community Consortium, Intelligent Infrastructure Task Force (2017–2018)
- Applied Technology Council (ATC) - ATC-126 (*Community Resilience of Lifeline Systems*) project technical committee (2016)
- Steering Committee (member, current chair), *IEEE/ACM Transactions on Networking* (2007–2017)
- ACM publication board technology committee (2015)
- ACM SIGCOMM vice chair (2007–2013)
- Member of the Board, Armstrong Memorial Research Foundation (2009–)

- Internet2 Applications, Middleware and Services Advisory Council (AMSAC) (2008–2012)
- GENI OptIn working group co-chair (2008–2009)
- board of directors, *SIP Forum* (1998–2002)
- Member of Internet Architecture Board (IAB), the technical advisory group of the Internet Society and the architectural oversight body of the IETF (1999–2001)
- Co-chair, *Internet Technical Committee* of the IEEE Communications Society (1994-2000)
- Chair, *IEEE Communications Society Technical Committee on Computer Communications* (1999–2001)
- SIP Bake-Offs, Columbia University (April 1999, August 1999, December 1999)
- IEEE *Infocom* Executive Committee (1995–2000)
- Internet2 Applications, Middleware and Services Advisory Council (AMSAC) 2008–2010
- GENI OptIn working group co-chair, 2008–2009
- IEEE Travel Reduction Task Force, 2009
- member-at-large, Board of Governors, IEEE *Communications Society*, 2002
- board of directors, *SIP Forum*, 1998–2002
- past co-Chair, *Internet Technical Committee* of the IEEE Communications Society
- Chair, *IEEE Communications Society Technical Committee on Computer Communications* (1999–2001)
- member IEEE Electronic Processes Steering Group, 2000

Conference leadership:

- *Mobiquitous 2018* general co-chair
- *e-Energy 2011* technical program co-chair
- *IEEE COMSNETS 2010* general co-chair
- *IEEE P2P 2009* general co-chair
- *IEEE ICNP 2009* general co-chair
- *IFIP Networking 2009* technical program co-chair
- *IEEE IM 2009* technical program co-chair
- *ACM IPTCOMM 2008* technical program co-chair
- *ACM IPTCOMM 2007* general co-chair
- *CoNext 2007* general co-chair
- *ACM Multimedia* 2004 general co-chair
- technical program co-chair Internet Telephony Workshop 2001
- IEEE *Infocom* 2000 technical program co-chair
- *NOSSDAV* technical program co-chair 2001
- IEEE *Infocom* 1998 vice general chair
- Organizer, SIP Bake-Offs, Columbia University (April 1999, August 1999, December 1999)

- IEEE *Infocom* Executive Committee 1995–2000
- *NOSSDAV*, *MobiArch* and *IPTComm* steering committees (current)

Referee for *IEEE Transactions on Networking*, *Springer/ACM Multimedia Systems Journal*, *IEEE Transactions on Communications*, *Computer Networks and ISDN Systems*, *Internetworking*, IEEE Infocom, ACM Sigcomm, IC$^3$N, National Science Foundation, and others.

Maintainer and editor of the web-based Network Bibliography.

PATENTS

US patent 5,509,074: *Method of protecting electronically published materials using cryptographic protocols* (issued April 1996)

US patent 6,141,788: *Method And Apparatus For Forward Error Correction In Connection In Packet Networks* (October 2000)

US patent 6,446,108: *Method For Network Address Translation* (September 2002)

US patent 6,538,416: *Border Gateway Reservation Protocol for Tree-Based Aggregation of Inter-Domain Reservations* (March 2003)

US patent 6,771,644: *Program insertion in real time IP multicast* (August 2004)

US patent 6,937,597: *Signaling Method For Internet Telephony* (August 2005)

US patent 6,970,909: *Multi-protocol data communication systems supporting wireless telephony and content delivery* (November 2005)

US patent 7,257,201: *System and method for unified messaging in inter/intranet telephony* (August 2007)

US patent 7,266,091: *System and method for conferencing in inter/intranet telephony* (September 2007)

US patent 7,296,091: *System and method for receiving over a network a broadcast from a broadcast source* (November 2007)

US patent 7,319,689: *Method for handling the simultaneous mobility of mobile hosts in infrastructure-based networks* (January 2008)

US patent 7,610,384: *Network telephony appliance and system for inter/intranet telephony* (October 2009)

US patent 7,610,384: *Network telephony appliance and system for inter/intranet telephony* (October 2009)

US patent 7,636,336 *Methods and systems for reducing MAC layer handoff latency in wireless networks* (December 2009)

US patent 8,027,251 *Systems and methods for implementing protocol-aware network firewall* (September 2011)

US patent 8,166,102 *Signaling method for internet telephony* (April 2012)

US patent 8,302,186 *System and method for testing network firewall for denial-of-service (DOS) detection and prevention in signaling channel* (October 2012)

US patent 8,522,344 *Theft of service architectural integrity validation tools for session initiation protocol (SIP)-based systems* (August 2013)

US patent 8,565,384 *Systems, methods, and media for connecting emergency communications* (October 2013)

US patent 8,689,328 *Malicious user agent detection and denial of service (DOS) detection and prevention using fingerprinting* (March 2014)

US patent 8,719,926 *Denial of service detection and prevention using dialog level filtering* (April 2014)

US patent 8,737,220 *Systems for providing feedback to sending entities* (May 2014)

US patent 8,737,351 *Methods and systems for reducing MAC layer handoff latency in wireless networks* (May 2014)

US patent 8,750,242 *Methods, media, and devices for moving a connection from one point of access to another point of access* (June 2014)

US patent 8,804,513 *Methods and systems for controlling SIP overload* (August 2014)

US patent 8,966,619 *Prevention of denial of service (DoS) attacks on session initiation protocol (SIP)-based systems using return routability check filtering* (February 2015)

US patent 8,995,742 *Methods and systems for controlling traffic on a communication network* (March 2015)

US patent 9,036,605 *Methods, media, and devices for moving a connection from one point of access to another point of access* (May 2015)

US patent 9,118,814 *Set-top box peer-assisted video-on-demand* (August 2015)

US patent 9,374,342 *System and method for testing network firewall using fine granularity measurements* (June 2016)

US patent 8,750,242 *Methods, media, and devices for moving a connection from one point of access to another point of access* (July 2016)

US patent 9,473,529 *Prevention of denial of service (DoS) attacks on Session Initiation Protocol (SIP)-based systems using method vulnerability filtering* (October 2016)

US patent 10,039,033 *Systems, methods, and media for implementing call handoff between networks* (July 2018)

TUTORIALS

Partial listing:

- *IDMS/PROMS*, Coimbra, November 2002;
- *Mobicom* tutorial, Atlanta, September 2002;
- *Sigcomm* tutorial, Stockholm, August 2000;
- *International Conference on Multimedia (ICME)*, July 2000;
- *Networking 2000* tutorial, Paris, May 2000;
- *IEEE Real Time Applications Symposium*, May 2000;
- *VON Developers Conference*, semi-annually since 1999;
- BellSouth (Atlanta), February and March 1998, November 1999;
- *IEEE International Conference on Network Protocols* (ICNP), October 1999;
- ASSET conference (Dallas, Texas), March 1999;
- CEFRIEL (Milan), May 1999;
- MCI Corp. (Colorado Springs), August 1998;
- EPFL summer school (Lausanne, Switzerland), June 1998;

- 16th Brazilian Symposium on Computer Networks, May 1998;
- IEEE Infocom, March 1998;

SOFTWARE

**MICE:** Web-based information management for departmental personnel, student, space and financial data;

**CINEMA:** Columbia InterNet Extensible Multimedia Architecture (with Jonathan Lennox, Kundan Singh, and others);

**EDAS:** editor's assistant; conference paper management software used for IEEE ICC, IEEE Globecom, Mobicom, IEEE Infocom, ICNP, NOSSDAV, Packet Video (about 8,000 total), with roughly 770,000 users;

**e*phone:** Ethernet packet audio device; the first SIP-speaking embedded Internet phone (with Jianqi Yin).

**graph++:** graphing tool with matrix manipulation facilities.

**NeVoT:** network voice terminal, first RTP-capable Internet voice application.

**rtptools:** set of tools for analyzing, recording and playing back RTP packets; used in a number of media-on-demand projects.

**RTP library:** library implementing RTP (with Jonathan Lennox, Jonathan Rosenberg and Dan Rubenstein);

**rtspd:** RTSP multimedia server (with Jonathan Lennox and Kundan Singh).

**sipc:** SIP user agent (Internet telephony agent) (with Xiaotao Wu).

**sipconf:** SIP-based software conferencing server (with Kundan Singh);

**sipd:** First publically available SIP proxy and redirect server (with Jonathan Lennox);

**sipum:** SIP-based unified messaging system (with Kundan Singh);

**simul:** discrete-event simulator emulating SIMAN.

JOURNAL PUBLICATIONS

[1] H. Schulzrinne, "Network neutrality is about money, not packets (invited paper)," *IEEE Internet Computing*, Vol. 22, November/December 2018.

[2] H. Schulzrinne, "Networking research – a reflection in the middle years (invited paper)," *Computer Communications*, 2018.

[3] S. G. Hong, S. Seo, H. Schulzrinne, and P. Chitrapu, "ICOW: Internet access in public transit systems," *IEEE Communications Magazine*, Vol. 53, pp. 134–141, June 2015.

[4] M. Berman, P. Demeester, J. W. Lee, K. Nagaraja, M. Zink, D. Colle, D. K. Krishnappa, D. Raychaudhuri, H. Schulzrinne, I. Seskar, and S. Sharma, "Future internets escape the simulator," *Communications ACM*, Vol. 58, pp. 78–89, May 2015.

[5] E. Piri and H. Schulzrinne, "Scaling network information services to support hetnets and dynamic spectrum access," *Journal of Communications and Networks*, Vol. 16, Apr. 2014.

[6] S. G. Hong and H. Schulzrinne, "PBS: Signaling architecture for network traffic authorization," *IEEE Communications Magazine*, Vol. 51, pp. 89–96, July 2013.

[7] O. Boyaci, V. Beltran, and H. Schulzrinne, "Bridging communications and the physical world," *IEEE Internet Computing*, Vol. 16, no. 2, pp. 35–43, 2012.

[8] D. Touceda, J. Sierra, A. Izquierdo, and H. Schulzrinne, "Survey of attacks and defenses on P2PSIP communications," *IEEE Communications Surveys Tutorials*, Vol. 14, no. 3, pp. 750–783, 2012.

[9] C. Shen, E. Nahum, H. Schulzrinne, and C. P. Wright, "The impact of TLS on SIP server performance: Measurement and modeling," *IEEE/ACM Transactions on Networking*, Vol. 20, pp. 1217–1230, Aug. 2012.

[10] J. Kayfetz, H. Schulzrinne, T. Sherwood, and M. Tiwari, "Your desktop or mine: Extending the reach of writing instruction," *Ubiquitous Learning*, Vol. 3, no. 3, 2011.

[11] E. Brosh, S. A. Baset, V. Misra, D. Rubenstein, and H. Schulzrinne, "The Delay-Friendliness of TCP for Real-Time traffic," *IEEE/ACM Transactions on Networking*, Oct. 2010.

[12] H. Tschofenig and H. Schulzrinne, "Emergency services for internet multimedia," *The Internet Protocol Journal*, Dec. 2010.

[13] S. Subramanya, X. Wu, H. Schulzrinne, and S. Buriak, "VoIP-based air traffic controller training," *IEEE Communications Magazine*, Nov. 2009.

[14] S. Alexander, Y.-H. Cheng, B. Coan, A. Ghetie, V. Kaul, B. Siegell, S. Bellovin, N. Maxemchuk, and H. Schulzrinne, "The dynamic community of interest and its realization in ZODIAC," *IEEE Communications Magazine*, Oct. 2009.

[15] H. Schulzrinne, "Double submissions: publishing misconduct or just effective dissemination?," *CCR*, July 2009.

[16] H. Schulzrinne, "Double-blind reviewing: more placebo than miracle cure?," *CCR*, Apr. 2009.

[17] S. Shin and H. Schulzrinne, "Measurement and analysis of the VoIP capacity in IEEE 802.11 WLAN," *IEEE Transactions on Mobile Computing*, Sept. 2009.

[18] R. Dantu, S. Fahmy, H. Schulzrinne, and J. Cangussu, "Issues and challenges in securing VoIP," *Computers & Security*, May 2009.

[19] X. Fu, H. Schulzrinne, H. Tschofenig, C. Dickmann, and D. Hogrefe, "Overhead and performance study of the general internet signaling transport (GIST) protocol," *IEEE/ACM Transactions on Networking*, Feb. 2009.

[20] D. Chopra, H. Schulzrinne, E. Marocco, and E. Ivov, "Peer-to-peer overlays for real-time communication: security issues and solutions," *IEEE Communications Surveys & Tutorials*, Jan. 2009.

[21] H. Schulzrinne, "Conferences as organizations: advising, steering and establishing expectations," *ACM SIGCOMM Computer Communication Review*, Jan. 2009.

[22] G. Camarillo, H. Schulzrinne, S. Loreto, and J. Hautakorpi, "Effect of head of the line blocking on session initiation protocol session establishment delays," *Journal of Communications and Networks*, Feb. 2009.

[23] S. G. Hong, V. Hilt, and H. Schulzrinne, "Evaluation of control message overhead of DHT-based P2P system," *Bell Labs Technical Journal*, Nov. 2008.

[24] A. Dutta, D. Famolari, S. Das, Y. Ohba, V. Fajardo, K. Taniuchi, R. Lopez, and H. Schulzrinne, "Media-independent pre-authentication supporting secure interdomain handover optimization," *IEEE Wireless Communications*, Apr. 2008.

[25] X. Wang and H. Schulzrinne, "Measurement and analysis of LDAP performance," *IEEE/ACM Transactions on Networking*, Feb. 2008.

[26] K. Arabshian and H. Schulzrinne, "An ontology-based hierarchical Peer-to-Peer global service discovery system," *Journal of Ubiquitous Computing and Intelligence (JUCI)*, Vol. 1, pp. 133–144, Dec. 2007.

[27] W. Yuen and H. Schulzrinne, "Improving search efficiency using bloom filters in partially connected ad hoc networks: A node-centric analysis," *Computer Communications*, Nov. 2007.

[28] A. Dutta, S. Das, D. Famolari, Y. Ohba, K. Taniuchi, V. Fajardo, R. M. Lopez, T. Kodama, and H. Schulzrinne, "Seamless proactive handover across heterogeneous access networks," *Wireless Personal Communications*, Nov. 2007.

[29] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "Ubiquitous device personalization and use: The next generation of IP multimedia communications," *ACM Transactions on Multimedia Computing, Communications, and Applications*, Aug. 2007.

[30] R. Dantu, D. Ghosal, and H. Schulzrinne, "Securing voice over IP," *IEEE Network*, Vol. 20, pp. 4–5, Sept. 2006.

[31] X. Wang and H. Schulzrinne, "Pricing network resources for adaptive applications," *IEEE/ACM Transactions on Networking*, Vol. 14, pp. 506–519, June 2006.

[32] K. Wong, A. Dutta, H. Schulzrinne, and K. Young, "Simultaneous mobility: analytical framework, theorems, and solutions," *Wireless Communication and Mobile Computing*, June 2006.

[33] K. Singh and H. Schulzrinne, "Failover, load sharing and server architecture in SIP telephony," *Computer Communications*, Mar. 2007.

[34] W. Zhao and H. Schulzrinne, "Enhancing service location protocol for efficiency, scalability and advanced discovery," *The Journal of Systems & Software*, Vol. 75, pp. 193–204, Feb. 2005.

[35] X. Wang and H. Schulzrinne, "Incentive-Compatible adaptation of internet Real-Time multimedia," *IEEE Journal on Selected Areas in Communications*, Vol. 23, pp. 417–436, Feb. 2005.

[36] W. Kellerer, M. Wagner, W.-T. Balke, and H. Schulzrinne, "Preference-based session management for IP-based mobile multimedia signaling," *European Transactions on Telecommunications*, Vol. 15, pp. 415–427, Aug. 2004.

[37] L. Amini, A. Shaikh, and H. Schulzrinne, "Issues with inferring internet topological attributes," *Computer Communications*, Vol. 27, pp. 557–567, Apr. 2004.

[38] P. Mendes, H. Schulzrinne, and E. Monteiro, "How to increase the efficiency of receiver-driven adaptive mechanisms in a new generation of IP networks," *Computer Communications*, Vol. 27, pp. 345–354, Feb. 2004.

[39] A. Dutta and H. Schulzrinne, "MarconiNet: overlay mobile content distribution network," *IEEE Communications Magazine*, Feb. 2004.

[40] H. Schulzrinne, X. Wu, S. Sidiroglou, and S. Berger, "Ubiquitous computing in home networks," *IEEE Communications Magazine*, pp. 128–135, Nov. 2003.

[41] D. Wong, A. Dutta, J. Burns, K. Young, and H. Schulzrinne, "A multilayered mobility management scheme for auto-configured wireless IP networks," *IEEE Wireless Magazine*, Oct. 2003.

[42] A. Dutta, J. Chennikara-Varghese, W. Chen, O. Altintas, and H. Schulzrinne, "Multicasting streaming media to mobile users," *IEEE Communications Magazine*, Oct. 2003.

[43] P. Mendes, H. Schulzrinne, and E. Monteiro, "How to increase the efficiency of receiver-driven adaptive mechanisms in a new generation of IP networks," *Computer Communications*, Vol. 26, 2003.

[44] G. Camarillo, H. Schulzrinne, and R. Kantola, "Evaluation of transport protocols for the session initiation protocol," *IEEE Network*, 2003.

[45] P. Mendes, H. Schulzrinne, and E. Monteiro, "Session-aware popularity resource allocation for assured differentiated services," *IEEE Communications Magazine*, Sept. 2002.

[46] J. Brassil and H. Schulzrinne, "Enhancing Internet streaming media with cueing protocols," *IEEE/ACM Transactions on Networking*, Vol. 10, Aug. 2002.

[47] H. Schulzrinne and K. Arabshian, "Providing emergency services in Internet telephony," *IEEE Internet Computing*, Vol. 6, pp. 39–47, May 2002.

[48] W. Jiang, J. Lennox, S. Narayanan, H. Schulzrinne, K. Singh, and X. Wu, "Integrating Internet telephony services," *IEEE Internet Computing*, Vol. 6, pp. 64–72, May 2002.

[49] H. Schulzrinne, "Internet telefonie – mehr als nur ein telefon mit paketvermittlung," *PIK – Praxis der Informationsverarbeitung und Kommunikation*, Vol. 24, Jan. 2001.

[50] X. Wang and H. Schulzrinne, "An integrated resource negotiation, pricing, and QoS adaptation framework for multimedia applications," *IEEE Journal on Selected Areas in Communications*, Vol. 18, pp. 2514–2529, Dec. 2000.

[51] H. Schulzrinne and J. Rosenberg, "The session initiation protocol: Internet-centric signaling," *IEEE Communications Magazine*, Vol. 38, Oct. 2000.

[52] H. Schulzrinne and E. Wedlund, "Application-layer mobility using SIP," *Mobile Computing and Communications Review (MC2R)*, Vol. 4, pp. 47–57, July 2000.

[53] P. Pan, E. Hahne, and H. Schulzrinne, "The border gateway reservation protocol (BGRP) for tree-based aggregation of inter-domain reservations," *Journal of Communications and Networks*, June 2000.

[54] X. Wang and H. Schulzrinne, "Comparison of adaptive Internet multimedia applications," *IEICE Transactions on Communications*, June 1999.

[55] C. A. Polyzois, K. H. Purdy, P. Q. Yang, D. C. Shrader, H. Sinnreich, F. Ménard, and H. Schulzrinne, "From POTS to PANS – a commentary on the evolution to Internet telephony," *IEEE Network*, Vol. 13, pp. 58–64, May/June 1999.

[56] J. Rosenberg and H. Schulzrinne, "The IETF Internet telephony architecture and protocols," *IEEE Network*, Vol. 13, pp. 18–23, May/June 1999.

[57] J. Rosenberg, J. Lennox, and H. Schulzrinne, "Programming Internet telephony services," *IEEE Network*, Vol. 13, pp. 42–49, May/June 1999.

[58] P. Pan and H. Schulzrinne, "YESSIR: a simple reservation mechanism for the Internet," *ACM Computer Communication Review*, Vol. 29, pp. 89–101, Apr. 1999.

[59] J. Brassil, S. Garg, and H. Schulzrinne, "Program insertion in real-time IP multicasts," *ACM Computer Communication Review*, Vol. 29, pp. 49–68, Apr. 1999.

[60] H. Schulzrinne and J. Rosenberg, "Internet telephony: Architecture and protocols – an IETF perspective," *Computer Networks and ISDN Systems*, Vol. 31, pp. 237–255, Feb. 1999.

[61] H. Schulzrinne and J. Rosenberg, "The session initiation protocol: Providing advanced telephony services across the Internet," *Bell Labs Technical Journal*, Vol. 3, pp. 144–160, October-December 1998.

[62] H. Schulzrinne, "Transatlantische netze," *DFN Mitteilungen*, Vol. 46, pp. 23–24, Mar. 1998.

[63] D. Sisalem and H. Schulzrinne, "The multimedia Internet terminal (mint)," *Telecommunications Systems*, Vol. 9, pp. 423–444, Sep 1998.

[64] H. Schulzrinne, "Operating system issues for continuous media," *Multimedia Systems*, Vol. 4, pp. 269–280, Oct. 1996.

[65] H. Schulzrinne, "World-wide web: Whence, whither, what next?," *IEEE Network*, Vol. 10, pp. 10–17, March/April 1996.

[66] I. Busse, B. Deffner, and H. Schulzrinne, "Dynamic QoS control of multimedia applications based on RTP," *Computer Communications*, Vol. 19, pp. 49–58, Jan. 1996.

[67] J. Crowcroft, D. Estrin, H. Schulzrinne, and M. Schwartz, "Guest editorial: The global Internet," *IEEE Journal on Selected Areas in Communications*, Vol. 13, pp. 1366–1369, Oct. 1995.

[68] H. Schulzrinne, "Conferencing and collaborative computing: Where are we?," *it+ti (Informationstechnik und Technische Informatik)*, Vol. 37, pp. 58–63, Aug. 1995.

[69] J. P. Sterbenz, H. Schulzrinne, and J. D. Touch, "Report and discussion on the IEEE comsoc TCGN gigabit networking workshop 1995," *IEEE Network*, Vol. 9, pp. 9–21, July/August 1995.

[70] H. Schulzrinne, "IPv6 – the new Internet protocol," *PIK – Praxis der Informationsverarbeitung und Kommunikation*, Vol. 18, pp. 165–167, July-September 1995.

[71] A. K. Choudhury, N. F. Maxemchuk, S. Paul, and H. Schulzrinne, "Copyright protection for electronic publishing over computer," *IEEE Network*, Vol. 9, pp. 12–20, May/June 1995.

[72] Çaglan M. Aras, J. F. Kurose, D. Reeves, and H. Schulzrinne, "Real-time communications in packet-switched networks," *Proceedings of the IEEE*, Vol. 82, pp. 122–139, Jan. 1994.

[73] W.-B. Gong and H. Schulzrinne, "Application of smoothed perturbation analysis to probabilistic routing," *Mathematics and Computers in Simulation*, Vol. 32, pp. 467–485, 1992.

BOOKS AND CHAPTERS

[1] A. Dutta and H. Schulzrinne, *Mobility Protocols and Handover Optimization: Design, Evaluation and Application*. Chichester: John Wiley, 2014.

[2] H. Tschofenig and H. Schulzrinne, *Internet Protocol-based Emergency Services*. Chichester: Wiley, 2013.

[3] M. Papadopouli and H. Schulzrinne, *Peer-to-Peer Computing for Mobile Networks*. Springer, Jan. 2009.

[4] D. Sisalem, J. Floroiu, J. Kuthan, U. Abend, and H. Schulzrinne, *SIP Security*. Wiley, May 2009.

[5] T. Chiba, H. Yokota, A. Idoue, A. Dutta, K. Manousakis, S. Das, and H. Schulzrinne, "Trombone routing mitigation techniques for IMS/MMD networks," in *IEEE Wireless Communications and Networking Conference 2007 - Networking*, (Hong Kong, Hong Kong), Mar. 2007.

[6] A. Dutta, H. Schulzrinne, and K. Wong, *Supporting Continuous Services to Roaming Clients*, ch. 17. USA: CRC, 2006.

[7] H. Schulzrinne, "Internet telephony," in *Practical Handbook of Internet Computing*, CRC, 2004.

[8] K. Wong, H.-Y. Wei, A. Dutta, K. Young, and H. Schulzrinne, "IP micro-mobility management using host-based routing," in *Wireless IP and building the Mobile Internet* (S. Dixit and R. Prasad, eds.), Artech House, 2002.

[9] H. Schulzrinne, "IP networks," in *Compressed Video Over Networks* (A. Reibman and M.-T. Sun, eds.), Marcel Dekker, 2001.

[10] R. Guérin and H. Schulzrinne, "Network quality of service," in *Grid: Blueprint for a New Computing Infrastructure* (I. Foster and C. Kesselman, eds.), San Francisco, California: Morgan Kaufmann Publishers, 1998.

[11] H. Schulzrinne, "Operating system issues for continuous multimedia," in *Handbook of Multimedia Computing* (B. Furht, ed.), pp. 627–648, Boca Raton: CRC Press, 1998.

CONFERENCE PUBLICATIONS

[1] V. Gadiraju, A. Panat, R. Poddar, Z. Sherriff, S. Kececi, and H. Schulzrinne, "Who gets broadband when? A panel data analysis of demographic, economic and technological factors explaining U.S. broadband deployment," in *TPRC46: Research Conference on Communications, Information and Internet Policy*, (Washington, DC), Sept. 2018.

[2] W. Falcon and H. Schulzrinne, "Predicting floor-level for 911 calls with neural networks and smartphone sensor data," in *Sixth International Conference on Learning Representations*, (Vancouver, Canada), Apr. 2018.

[3] J. Janak and H. Schulzrinne, "Framework for rapid prototyping of distributed IoT applications powered by WebRTC," in *Proc. of IPTComm 2016*, (Chicago, Illinois), Oct. 2016.

[4] H. Nam, K. H. Kim, and H. Schulzrinne, "QoE matters more than QoS: why people stop watching cat videos," in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications (INFOCOM 2016)*, (San Francisco, USA), pp. 847–855, Apr. 2016.

[5] K. H. Kim, J. W. Lee, M. Ben-Ami, H. Nam, J. Janak, and H. Schulzrinne, "Flexible network address mapping for container-based clouds," in *First IEEE Conference on Network Softwarization 2015 (NetSoft 2015)*, (London, United Kingdom), Apr. 2015.

[6] H. Nam, D. Calin, and H. Schulzrinne, "Intelligent content delivery over wireless via SDN," in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*, (New Orleans, USA), pp. 2203–2208, Mar. 2015.

[7] M. Varela, P. Zwickl, P. Reichl, M. Xie, and H. Schulzrinne, "Experience level agreements (ELA): the challenges of selling QoE to the user," in *IEEE ICC 2015 - Workshop on Quality of Experience-based Management for Future Internet Applications and Services (QoE-FI) (ICC'15 - Workshops 04)*, (London, United Kingdom), June 2015.

[8] H. Nam, K. H. Kim, J. Y. Kim, and H. Schulzrinne, "Towards QoE-aware video streaming using SDN," in *Globecom 2014 - Communications Software, Services and Multimedia Symposium (GC14 CSSM)*, (Austin, USA), pp. 1334–1339, Dec. 2014.

[9] H. Nam, K.-H. Kim, D. Calin, and H. Schulzrinne, "YouSlow: A performance analysis tool for adaptive bitrate video streaming," in *Proc. of SIGCOMM 2014 Posters and Demos*, (Chicago, Illinois), Aug. 2014.

[10] K. H. Kim, H. Nam, V. Singh, D. Song, and H. Schulzrinne, "DYSWIS: Crowdsourcing a home network diagnosis," in *Proc. of 23rd International Conference on Computer Communications and Networks (ICCCN 2104)*, (Shanghai, China), Aug. 2014.

[11] H. Nam, K. H. Kim, D. Calin, and H. Schulzrinne, "Towards dynamic network condition-aware video server selection algorithms over wireless networks," in *19th IEEE Symposium on Computers and Communications (IEEE ISCC 2014)*, (Madeira, Portugal), June 2014.

[12] W. Song, J. W. Lee, B. S. Lee, and H. Schulzrinne, "Finding 9-1-1 callers in tall buildings," in *15th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 2014)*, (Sydney, Australia), June 2014.

[13] H. Nam, K. H. Kim, B. H. Kim, D. Calin, and H. Schulzrinne, "Towards dynamic QoS-aware Over-The-Top video streaming," in *15th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (IEEE WoWMoM 2014)*, (Sydney, Australia), June 2014.

[14] K. H. Kim, H. Nam, J. H. Park, and H. Schulzrinne, "MoT: a collaborative network troubleshooting platform for the Internet of things," in *IEEE WCNC'14 Track 4 (Services, Applications, and Business) (IEEE WCNC'14 Track 4: SAB)*, (Istanbul, Turkey), pp. 3461–3466, Apr. 2014.

[15] K. H. Kim, H. Nam, and H. Schulzrinne, "WiSlow: a WiFi network performance troubleshooting tool for end users," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications (INFOCOM'2014)*, (Toronto, Canada), pp. 862–870, Apr. 2014.

[16] H. Schulzrinne, "Transitioning the public switched telephone network into the 21st century," in *Proc. of ConTEL (12th International Conference on Telecommunications)*, (Zagreb, Croatia), pp. 3–4, June 2013.

[17] J. Y. Kim and H. Schulzrinne, "Cloud support for latency-sensitive telephony applications," in *Proceedings of the 2013 IEEE International Conference on Cloud Computing Technology and Science*, CLOUDCOM '13, (Bristol, UK), pp. 421–426, IEEE Computer Society, Dec. 2013.

[18] A. Singh, H. Schulzrinne, G. Ormazabal, S. Addepalli, P. Thermos, and Y. Zou, "Unified heterogeneous networking design," in *Principles, Systems and Applications of IP Telecommunications 2013 (IPTComm 2013)*, (Chicago, Illinois, USA), Oct. 2013.

[19] H. Nam, B. H. Kim, D. Calin, and H. Schulzrinne, "A mobile video traffic analysis: Badly designed video clients can waste network bandwidth," in *Globecom*

*2013 Workshop - Control Techniques for Efficient Multimedia Delivery (GC13 WS - CTEMD)*, (Atlanta, USA), pp. 512–517, Dec. 2013.

[20] M. Femminella, G. Reali, D. Valocchi, R. Francescangeli, and H. Schulzrinne, "Advanced caching for distributing sensor data through programmable nodes," in *Proc. of IEEE LANMAN*, (Brussels, Belgium), Apr. 2013.

[21] K.-H. Kim, H. Nam, and H. Schulzrinne, "WiSlow: A performance troubleshooting tool for Wi-Fi networks," in *Proc. of NSDI (poster/demo)*, (Lombard, Illinois), Apr. 2013.

[22] J. Marasevic, J. Janak, H. Schulzrinne, and G. Zussman, "WiMAX in the classroom: Designing a cellular networking hands-on lab," in *Proc. of 2nd GENI Research and Educational Experiment Workshop (GREE2013)*, (Salt Lake City, Utah), Mar. 2013.

[23] W. Song, G. Hampel, A. Rana, T. E. Klein, and H. Schulzrinne, "MOSAIC: stateless mobility for HTTP-based applications," in *IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, (Barcelona, Spain), pp. 69–76, Oct. 2012.

[24] S. Srinivasan, A. Singh, D. Batni, J. W. Lee, H. Schulzrinne, V. Hilt, and G. Kunzmann, "CCNxServ: dynamic service scalability in Information-Centric networks," in *IEEE ICC 2012 - Next-Generation Networking Symposium (ICC'12 NGN)*, (Ottawa, Ontario, Canada), pp. 2632–2637, June 2012.

[25] E. Maccherani, M. Femminella, J. W. Lee, R. Francescangeli, J. Janak, G. Reali, and H. Schulzrinne, "Extending the netserv autonomic management capabilities using openflow," in *Network Operations and Management Symposium (NOMS), 2012 IEEE*, (Maui, Hawaii), pp. 582–585, Apr. 2012.

[26] M. Femminella, R. Francescangeli, G. Reali, and H. Schulzrinne, "Gossip-based signaling dissemination extension for next steps in signaling," in *Network Operations and Management Symposium (NOMS)*, (Maui, Hawaii), pp. 1022–1028, Apr. 2012.

[27] A. Moghadam, T. Jebara, and H. Schulzrinne, "A markov routing algorithm for mobile DTNs based on Spatio-Temporal modeling of human movement data," in *14th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM 2011)*, (Miami Beach, USA), Oct. 2011.

[28] M. Femminella, R. Francescangeli, G. Reali, J. W. Lee, W. Song, and H. Schulzrinne, "Future internet autonomic management using NetServ," in *Demonstrations of the IEEE Conference on Local Computer Networks (LCN) (LCN-Demos 2011)*, (Bonn, Germany), pp. 1081–1083, Oct. 2011.

[29] F. M. Roberto, J. Celestino JÃºnior, and H. Schulzrinne, "Using a symmetric game based in volunteer's dilemma to improve vanets multihop broadcast communication," in *22nd IEEE Personal Indoor Mobile Radio Communications (PIMRC'11 - ITN)*, (Toronto, Canada), pp. 777–782, Sept. 2011.

[30] J. Y. Kim, G. Bond, E. Cheung, T. M. Smith, and H. Schulzrinne, "An evaluation framework for highly available and scalable SIP server clusters," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'11)*, (Chicago, Illinois, USA), Aug. 2011.

[31] K. Ono and H. Schulzrinne, "Using Cross-Media relations to identify important communication requests: Testing the concept and implementation," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'11)*, (Chicago, Illinois, USA), Aug. 2011.

[32] J. Y. Kim and H. Schulzrinne, "SipCloud: dynamically scalable SIP proxies in the cloud," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'11)*, (Chicago, Illinois, USA), Aug. 2011.

[33] O. Boyaci, V. Beltran, and H. Schulzrinne, "Bridging communications and the physical world: Sense everything, control everything," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'11)*, (Chicago, Illinois, USA), Aug. 2011.

[34] E. Shim, V. Krishnaswamy, and H. Schulzrinne, "Automatic phone number mapping verification for phone number based SIP peering," in *The 8th Annual IEEE Consumer Communications and Networking Conference - Content Distribution and Peer-to-Peer Networks (CCNC'2011 Content Distribution and Peer-to-Peer Networks)*, (Las Vegas, NV, USA), pp. 995–999, Jan. 2011.

[35] S. Srinivasan, I. Rimac, M. Steiner, V. Hilt, and H. Schulzrinne, "Unveiling the content-centric features of TCP," in *ICC 2011 Next Generation Networking and Internet Symposium (ICC'11 NGNI)*, (Kyoto, Japan), June 2011.

[36] W. Song, J. W. Lee, and H. Schulzrinne, "Polygon simplification for Location-Based services using population density," in *ICC 2011 - Communication Software, Services and Multimedia Applications Symposium (ICC'11 CSMA)*, (Kyoto, Japan), June 2011.

[37] J. W. Lee, H. Schulzrinne, W. Kellerer, and Z. Despotovic, "0 to 10k in 20 seconds: Bootstrapping large-scale DHT networks," in *ICC 2011 - Communication Software, Services and Multimedia Applications Symposium (ICC'11 CSMA)*, (Kyoto, Japan), June 2011.

[38] J. W. Lee, R. Francescangeli, J. Janak, S. Srinivasan, S. A. Baset, H. Schulzrinne, Z. Despotovic, and W. Kellerer, "NetServ: active networking 2.0," in *ICC 2011 Workshop TF1 (T2), Future Network (ICC'11 Workshop TF1 (T2) FutureNet IV)*, (Kyoto, Japan), June 2011.

[39] S. Komorita, H. Yokota, A. Dutta, C. Makaya, S. Das, D. A. Chee, F. J. Lin, and H. Schulzrinne, "User-transparent reconfiguration method for self-organizing IP multimedia subsystem," in *16th IEEE Symposium on Computers and Communications (IEEE ISCC 2011)*, (Kerkyra (Corfu), Greece), June 2011.

[40] A. Dutta, B. Lyles, and H. Schulzrinne, "A formal approach to mobility modeling," in *The Third International Conference on COMmunication Systems and NETworkS (COMSNETS 2011) (COMSNETS 2011)*, (Bangalore, India), Jan. 2011.

[41] J. Kayfetz, H. Schulzrinne, T. Sherwood, and M. Tiwari, "Your desktop or mine: Extending the reach of writing instruction," in *Ubiquitous Learning International Conference ()*, (Vancouver, Canada), Dec. 2010.

[42] C. Makaya, A. Dutta, B. Falchuk, D. A. Chee, S. Das, F. J. Lin, M. Ito, S. Komorita, T. Chiba, H. Yokota, and H. Schulzrinne, "Enhanced Next-Generation service overlay networks architecture," in *IEEE International Conference on Internet Multimedia Systems Architecture and Application (IMSAA-10)*, (Bangalore, India), Dec. 2010.

[43] O. Boyaci, V. Beltran, and H. Schulzrinne, "Bridging communications and the physical world: Sense everything, control everything," in *IEEE Globecom 2010 Workshop on Ubiquitous Computing and Networks (UbiCoNet 2010)*, (Miami, Florida, USA), pp. 1735–1740, Dec. 2010.

[44] S. G. Hong, H. Schulzrinne, and S. Weiland, "Signaling architecture for network traffic authorization," in *IEEE Globecom 2010 - Communication & Information System Security (GC10 - CIS)*, (Miami, Florida, USA), Dec. 2010.

[45] C. Shen and H. Schulzrinne, "On TCP-based SIP server overload control," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'10)*, (Munich, Germany), Aug. 2010.

[46] M. Barnes, L. Miniero, R. Presta, S. P. Romano, and H. Schulzrinne, "CCMP: a novel standard protocol for conference management in the XCON framework," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'10)*, (Munich, Germany), Aug. 2010.

[47] S. A. Baset and H. Schulzrinne, "Reliability and relay selection in Peer-to-Peer communication systems," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'10)*, (Munich, Germany), Aug. 2010.

[48] C. Shen, E. Nahum, H. Schulzrinne, and C. P. Wright, "The impact of TLS on SIP server performance," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'10)*, (Munich, Germany), Aug. 2010.

[49] A. Amirante, S. P. Romano, H. Schulzrinne, and K. H. Kim, "Online Non-Intrusive diagnosis of One-Way RTP faults in VoIP networks using cooperation," in *Principles, Systems and Applications of IP Telecommunications (IPTComm'10)*, (Munich, Germany), Aug. 2010.

[50] K. Sung, S. Srinivasan, and H. Schulzrinne, "BBS-ONE: bulletin board and forum system for mobile opportunistic networks," in *IEEE WCNIS2010-Wireless Networks (IEEE WCNIS2010-WN)*, (Beijing, China, P.R. China), June 2010.

[51] K. Andersson, A. G. Forte, and H. Schulzrinne, "Enhanced mobility support for roaming users: Extending the IEEE 802.21 information service," in *8th International Conference on Wired / Wireless Internet Communications (WWIC 2010)*, (Lulea, Sweden), May 2010.

[52] A. Cooper, H. Schulzrinne, E. Wilde, and D. Mulligan, "Challenges for the Location-Aware web," in *WebSci10: Extending the Frontiers of Society On-Line ()*, (Raleigh, North Carolina), Apr. 2010.

[53] A. Misra and H. Schulzrinne, "Policy-Driven distributed and collaborative demand response in Multi-Domain commercial buildings," in *1st Int'l Conf. on Energy-Efficient Computing and Networking ()*, (Passau, Germany), Apr. 2010.

[54] K. Arabshian, C. Dickmann, and H. Schulzrinne, "Ontology-Based service discovery Front-End interface for GloServ," in *6th European Semantic Web Conference on The Semantic Web: Research and Applications*, (Heraklion, Crete, Greece), May 2009.

[55] W. Song, J. Y. Kim, H. Schulzrinne, P. Boni, and M. Armstrong, "Using IM and SMS for emergency text communications," in *Principles, Systems and Applications of IP Telecommunications*, (Atlanta, Georgia, USA), July 2009.

[56] K. Ono and H. Schulzrinne, "Have i met you before? using Cross-Media relations to reduce SPIT," in *Principles, Systems and Applications of IP Telecommunications*, (Atlanta, Georgia, USA), July 2009.

[57] H. Cui, S. Srinivasan, and H. Schulzrinne, "ONEChat: enabling group chat and messaging in opportunistic networks," in *HotMobile (Poster) ()*, (Annapolis, Maryland), Feb. 2010.

[58] M. Ge, S. Srinivasan, and H. Schulzrinne, "FileXChange: Drag-and-Drop file sharing in opportunistic networks," in *HotMobile (Poster) ()*, (Annapolis, Maryland), Feb. 2010.

[59] O. Boyaci, A. Forte, and H. Schulzrinne, "Performance of Video-Chat applications under congestion," in *Eleventh IEEE International Symposium on Multimedia*, (San Diego, California, USA), Dec. 2009.

[60] O. Boyaci, A. Forte, S. Baset, and H. Schulzrinne, "vdelay a tool to measure Capture-to-Display latency and frame-rate," in *Eleventh IEEE International Symposium on Multimedia*, (San Diego, California, USA), Dec. 2009.

[61] O. Boyaci, A. Forte, S. Baset, and H. Schulzrinne, "vdelay: A tool to measure Capture-to-Display latency and frame-rate," in *Eleventh IEEE International Symposium on Multimedia*, (San Diego, California, USA), Dec. 2009.

[62] A. Dutta, C. Makaya, S. Das, D. Chee, F. Lin, S. Komorita, T. Chiba, H. Yokota, and H. Schulzrinne, "Self organizing IP multimedia subsystem," in *IEEE International Conference on Internet Multimedia Systems Architecture and Application*, (Bangalore, India), Dec. 2009.

[63] S. Srinivasan, J. Lee, E. Liu, M. Kester, H. Schulzrinne, V. Hilt, S. Seetharaman, and A. Khan, "NetServ: dynamically deploying in-network services," in *2nd ACM Workshop on Re-Architecting the Internet*, (Rome, Italy), Dec. 2009.

[64] S. G. Hong, S. Srinivasan, and H. Schulzrinne, "Measurements of multicast service discovery in a campus wireless network," in *IEEE Globecom 2009 Communications Quality of Service, Reliability and Performance Modeling Symposium*, (Honolulu, Hawaii, USA), Nov. 2009.

[65] K. Yasukawa, A. Forte, and H. Schulzrinne, "Distributed delay estimation and call admission control in IEEE 802.11 wireless LANs," in *ICC 2009 Wireless Networking*, (Dresden, Germany, Germany), June 2009.

[66] A. Moghadam and H. Schulzrinne, "Interest-aware content distribution protocol for mobile disruption-tolerant networks," in *10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, (Kos Island, Greece), June 2009.

[67] M. Tauil, A. Dutta, Y.-H. Cheng, S. Das, D. Baker, M. Yajnik, D. Famolari, Y. Ohba, and V. Fajardo, "Realization of IEEE 802.21 services and preauthentication framework," in *Testbeds and Research Infrastructures for the Development of Networks & Communities and Workshops*, Apr. 2009.

[68] S. Srinivasan, A. Moghadam, and H. Schulzrinne, "BonAHA: service discovery framework for mobile Ad-Hoc applications," in *2009 IEEE Consumer Communications and Networking Conference - Personal Ad Hoc and Sensor Networks*, (Las Vegas, USA), Jan. 2009.

[69] A. Dutta, B. Lyles, H. Schulzrinne, and J. Wang, "Systems modeling for IP-Based handoff using timed petri nets," in *42nd Hawaii International Conference on System Sciences*, (Big Island, Hawaii), Jan. 2009.

[70] J. Lee, H. Schulzrinne, W. Kellerer, and Z. Despotovic, "mDHT: multicast-augmented DHT architecture for high availability and immunity to churn," in *2009 IEEE Consumer Communications and Networking Conference - P2P and Content Delivery*, (Las Vegas, USA), Jan. 2009.

[71] V. Singh, H. Schulzrinne, and P. Boni, "A new SIP event package for group membership management in advanced communications," in *International Conference on Internet Multimedia Services Architecture and Applications*, (Bangalore, India), Dec. 2008.

[72] A. Dutta, F. Lin, S. Das, B. Lyles, T. Chiba, H. Yokota, H. Schulzrinne, and D. Chee, "A-IMS architecture analysis and experimental IPv6 testbed," in *The 1st International Conference on IP Multimedia Subsystems Architecture and Applications*, (Bangalore, India), Dec. 2008.

[73] O. Boyaci and H. Schulzrinne, "BASS application sharing system," in *Tenth IEEE International Symposium on Multimedia*, (Berkeley, California, USA), Dec. 2008.

[74] T. Okabe and H. Schulzrinne, "Peer-to-Peer SIP features to eliminate a SIP sign-up process," in *IEEE Globecom 2008 Communications Software and Services Symposium*, (New Orleans, LA, USA), Nov. 2008.

[75] K. Ono and H. Schulzrinne, "The impact of SCTP on server scalability and performance," in *IEEE Globecom 2008 Communications Quality of Sevice, Reliability, and Performance Modeling Symposium*, (New Orleans, LA, USA), Nov. 2008.

[76] A. Forte and H. Schulzrinne, "Deployment guidelines for highly congested IEEE 802.11b/g networks," in *LANMAN 2009*, (Chij-Napoca, Transylvania), Sept. 2008.

[77] A. Moghadam, S. Srinivasan, and H. Schulzrinne, "7DS - a modular platform to develop mobile disruption-tolerant applications," in *International Conference and Exhibition on Next Generation Mobile Applications, Services, and Technologies*, (Cardiff, Wales, United Kingdom), Sept. 2008.

[78] T. Chiba, H. Yokota, A. Dutta, D. Chee, and H. Schulzrinne, "Performance analysis of next generation mobility protocols for IMS/MMD networks," in *IWCMC 2008 Next Generation Mobile Networks Symposium*, (Chania Crete Island, Greece, Greece), Aug. 2008.

[79] C. Shen, H. Schulzrinne, and E. Nahum, "SIP server overload control: Design and evaluation," in *Principles, Systems and Applications of IP Telecommunications*, (Heidelberg, Germany), July 2008.

[80] A. Forte and H. Schulzrinne, "Template-based signaling compression for Push-To-Talk over cellular (PoC)," in *Principles, Systems and Applications of IP Telecommunications*, (Heidelberg, Germany), July 2008.

[81] G. Ormazabal, H. Schulzrinne, E. Yardeni, and S. Nagpal, "Secure SIP: a scalable prevention mechanism for DoS attacks on SIP based VoIP systems," in *Principles, Systems and Applications of IP Telecommunications*, (Heidelberg, Germany), July 2008.

[82] K. Ono and H. Schulzrinne, "One server per city: Using TCP for very large SIP servers," in *Principles, Systems and Applications of IP Telecommunications*, (Heidelberg, Germany), July 2008.

[83] S. Baset, E. Brosh, D. Rubenstein, and H. Schulzrinne, "The delay friendliness of TCP," in *SIGMETRICS 2008–International Conference on Measurement and Modeling of Computer Systems*, (Annapolis, Maryland, USA), June 2008.

[84] S. Greco Polito and H. Schulzrinne, "SIP and 802.21 for service mobility and proactive authentication," in *Sixth Annual Conference on Communication Networks and Services Research*, (Halifax, Nova Scotia, Canada), May 2008.

[85] V. Singh, H. Schulzrinne, and K. Miao, "DYSWIS: an architecture for automated diagnosis of networks," in *Network Operations and Management Symposium (NOMS)*, (Salvador, Bahia), Apr. 2008.

[86] W. Kho, S. Baset, and H. Schulzrinne, "Skype relay calls: Measurements and experiments," in *11th IEEE Global Internet Symposium 2008*, (Phoenix, AZ, USA), Apr. 2008.

[87] R. Dantu, H. Schulzrinne, and P. Sroufe, "Experiences in building a multi-university testbed for research in multimedia communications," in *IEEE International Conference on Parallel and Distributed (IPDPS)*, (Miami, Florida), Apr. 2008.

[88] K. Arabshian and H. Schulzrinne, "An ontology-based hierarchical Peer-to-Peer global service discovery system," *Journal of Ubiquitous Computing and Intelligence (JUCI)*, Vol. 1, pp. 133–144, Dec. 2007.

[89] S. G. Hong, S. Srinivasan, and H. Schulzrinne, "Accelerating service discovery in ad-hoc zero configuration networking," in *IEEE Globecom 2007 Ad-hoc and Sensor Networking Symposium*, (Washington, DC, USA), Nov. 2007.

[90] A. Dutta, S. Chakravarty, K. Taniuchi, V. Vfajardo, Y. Ohba, D. Famolari, and H. Schulzrinne, "An experimental study of location assisted proactive handover," in *IEEE Globecom 2007 Internet Protocol Symposium*, (Washington, DC, USA), Nov. 2007.

[91] K. Yasukawa, A. Forte, and H. Schulzrinne, "Distributed delay estimation and call admission control in IEEE 802.11 WLANs," in *15th IEEE International Conference on Network Protocols*, (Beijing, P.R. China), pp. 334–335, Oct. 2007.

[92] A. Dutta, B. Lyles, H. Schulzrinne, T. Chiba, H. Yokota, and A. Idoue, "Generalized modeling framework for handoff analysis," in *18th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*, Sept. 2007.

[93] S. Gandhi, V. Singh, and H. Schulzrinne, "Analyzing user behavior in instant messaging," in *The First Annual Conference of ITA*, (Maryland, USA), Sept. 2007.

[94] R. Lopez, A. Dutta, Y. Ohba, H. Schulzrinne, and A. Skarmeta, "Network-Layer assisted mechanism to optimize authentication delay during handoff in 802.11 networks," in *MobiQuitous*, Aug. 2007.

[95] S. Greco Polito, H. Schulzrinne, and A. Forte, "Inter-provider AAA and billing of VoIP users with token-based method," in *Global Information Infrastructure Symposium*, July 2007.

[96] R. Shacham, H. Schulzrinne, W. Kellerer, and S. Thakolsri, "Composition for enhanced SIP presence," in *12th IEEE Symposium on Computers and Communications*, (Aveiro, Portugal), July 2007.

[97] C. Shen and H. Schulzrinne, "Measurement and evaluation of ENUM server performance," in *ICC 2007 Network Services and Operation Symposium*, (Glasgow, Scotland, United Kingdom), June 2007.

[98] S. Srinivasan, A. Moghadam, S. G. Hong, and H. Schulzrinne, "7DS - node cooperation and information exchange in mostly disconnected networks," in *ICC 2007 Wireless Adhoc and Sensor Networks Symposium*, (Glasgow, Scotland, United Kingdom), June 2007.

[99] S. Shin and H. Schulzrinne, "Experimental measurement of the capacity for VoIP traffic in IEEE 802.11 WLANs," in *IEEE INFOCOM 2007*, (Anchorage, Alaska, USA), May 2007.

[100] T. Chiba, H. Yokota, A. Idoue, A. Dutta, S. Das, F. Lin, and H. Schulzrinne, "Mobility management schemes for heterogeneity support in next generation wireless networks," in *3rd Euro-NGI Conference on Next Generation Internet Networks - Design and Engineering for Heterogeneity*, (Trondheim, Norway), May 2007.

[101] S. Greco Polito and H. Schulzrinne, "Authentication and authorization method in multi-domain, multi-provider networks," in *3rd Euro-NGI Conference on Next Generation Internet Networks - Design and Engineering for Heterogeneity*, (Trondheim, Norway), May 2007.

[102] T. Chiba, H. Yokota, A. Idoue, A. Dutta, K. Manousakis, S. Das, and H. Schulzrinne, "Trombone routing mitigation techniques for IMS/MMD networks," in *IEEE Wireless Communications and Networking Conference 2007 - Networking*, (Hong Kong, Hong Kong), Mar. 2007.

[103] V. Singh, H. Schulzrinne, P. Boni, B. Elman, and D. Kenneson, "Presence aware Location-Based service for managing mobile communications," in *2007 IEEE Consumer Communications and Networking Conference - Enabling Technologies Track*, (Las Vegas, NV, USA), Jan. 2007.

[104] W. Yuen and H. Schulzrinne, "Improving search efficiency using bloom filters in partially connected ad hoc networks: A Location-Centric analysis," in *IEEE Globecom 2006 - Wireless Ad Hoc and Sensor Networks - towards Anytime Anywhere Internetworking*, Nov. 2006.

[105] S. Shin, A. Forte, and H. Schulzrinne, "Passive duplicate address detection for the dynamic host configuration protocol (DHCP)," in *IEEE Globecom 2006 - Internet Services and Enabling Technologies*, Nov. 2006.

[106] S. Patnaik, E. Yardeni, H. Schulzrinne, G. Ormazabal, and D. Helms, "Securing SIP: scalable mechanisms for protecting SIP-Based VoIP systems," in *NANOG (North American Network Operators Group)*, (St. Louis, Missouri), NANOG, Oct. 2006.

[107] A. Forte, S. Shin, and H. Schulzrinne, "Improving layer 3 handoff delay in IEEE 802.11 wireless networks," in *Wireless Internet Conference (WICON)*, Aug. 2006.

[108] W. Yuen and H. Schulzrinne, "Performance evaluation of time-based and hop-based TTL schemes in partially connected ad hoc networks," in *ICC 2006 Wireless Ad Hoc and Sensor Networks*, June 2006.

[109] W. Zhao and H. Schulzrinne, "DotSlash: an automated web hotspot rescue system with on-demand query result caching," in *IEEE International Conference on Autonomic Computing (ICAC) (poster session)*, (Dublin, Ireland), June 2006.

[110] J. Y. Kim, W. Song, and H. Schulzrinne, "An enhanced VoIP emergency services prototype," in *Information Systems for Crisis Response and Management (ISCRAM)*, (Newark, New Jersey), ISCRAM, May 2006.

[111] A. Dutta, E. van den Berg, D. Famolari, V. Fajardo, Y. Ohba, K. Taniuchi, and H. Schulzrinne, "Dynamic buffering scheme for mobile handoff," in *PIMRC*, (Helsinki), IEEE, IEEE, 2006.

[112] A. Dutta, S. Das, D. Famolari, Y. Ohba, K. Taniuchi, V. Fajardo, T. Kodama, and H. Schulzrinne, "Secured seamless convergence across heterogeneous access networks," in *World Telecommunication Congress*, (Budapest), IEEE, IEEE, May 2006.

[113] X. Fu, H. Schulzrinne, H. Tschofenig, C. Dickmann, and D. Hogrefe, "Overhead and performance study of the general internet signaling transport (GIST) protocol," in *IEEE INFOCOM 2006*, (Barcelona, SPAIN), Apr. 2006.

[114] S. Baset and H. Schulzrinne, "An analysis of the skype Peer-to-Peer internet telephony protocol," in *IEEE INFOCOM 2006*, (Barcelona, SPAIN), Apr. 2006.

[115] A. Dutta, S. Madhani, W. Chen, O. Altintas, and H. Schulzrinne, "GPS assisted fast-handoff mechanism for real-time communication," in *2006 IEEE Sarnoff Symposium*, (Princeton NJ, USA), Mar. 2006.

[116] K. Singh and H. Schulzrinne, "Failover and load sharing in SIP telephony," in *International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS)*, (Philadelphia, PA), July 2005.

[117] A. Dutta, B. Kim, T. Zhang, S. Baba, K. Taniuchi, Y. Ohba, and H. Schulzrinne, "Experimental analysis of multi interface mobility management with SIP and MIP," in *IEEE Wirelesscom*, IEEE, IEEE, June 2005.

[118] K. Singh and H. Schulzrinne, "Peer-to-Peer internet telephony using SIP," in *NOSSDAV 2005*, (Skamania, Washington), June 2005.

[119] A. Dutta, T. Zhang, S. Madhani, K. Taniuchi, K. Fujimoto, Y. Katsube, Y. Ohba, and H. Schulzrinne, "Secure universal mobility for wireless internet," *Mobile Computing and Communications Review (MC2R)*, 2005.

[120] A. Dutta, T. Zhang, Y. Ohba, K. Taniuchi, and H. Schulzrinne, "MPA assisted proactive handoff scheme," in *ACM Mobiquitous*, SIGMOBILE, ACM, 2005.

[121] A. Dutta, J. Burns, R. Jain, K. Wong, K. Young, and H. Schulzrinne, "Implementation and performance evaluation of application layer MIP-LR," in *IEEE Wirelesscom*, IEEE, IEEE, 2005.

[122] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "The virtual device: Expanding wireless communication services through service discovery and session mobility," in *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, (Montreal, Canada), IEEE, Aug. 2005.

[123] X. Wu and H. Schulzrinne, "Handling feature interactions in the language for end system services," in *International Conference on Feature Interactions in Telecommunications and Software Systems (ICFI)*, June 2005.

[124] X. Wu and H. Schulzrinne, "Service learning in internet telephony," in *ICC 2005 Next Generation Networks for Universal Services*, (Seoul, Korea), May 2005.

[125] T. Kawata, S. Shin, A. Forte, and H. Schulzrinne, "Using dynamic PCF to improve the capacity for VoIP traffic in IEEE 802.11 networks," in *IEEE WCNC*, IEEE, Mar. 2005.

[126] J. Varghese-Chennikara, A. Dutta, A. Cheng, M. Elaoud, A. McAuley, I. Sebuktekin, D. Wong, H. Schulzrinne, and K. Young, "Integrated technologies for a survivable network," in *IEEE Wireless and Communications and Networking Conference*, (New Orleans, LA, USA), IEEE, IEEE, Mar. 2005.

[127] X. Wu and H. Schulzrinne, "Location-based services in internet telephony systems," in *IEEE Consumer Communications and Networking Conference*, (Las Vegas, Nevada), Jan. 2005.

[128] X. Wu and H. Schulzrinne, "sipc, a multi-function SIP user agent," in *7th IFIP/IEEE International Conference, Management of Multimedia Networks and Services (MMNS)*, pp. 269–281, IFIP/IEEE, Springer, Oct. 2004.

[129] A. Dutta, S. Madhani, W. Chen, O. Altintas, and H. Schulzrinne, "Fast-handoff schemes for application layer mobility management,," in *IEEE PIMRC*, IEEE, IEEE, Sept. 2004.

[130] K. Arabshian and H. Schulzrinne, "GloServ: global service discovery architecture," in *First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous)*, Aug. 2004.

[131] W. Zhao and H. Schulzrinne, "Building an adaptive distributed web server system on the fly for handling web hotspots," in *ACM Symposium on Principles of Distributed Computing (PODC)*, (St. John's, Newfoundland, Canada), ACM, ACM, July 2004.

[132] B.-T. Wang and H. Schulzrinne, "A Denial-of-Service-Resistant IP traceback approach," in *The Ninth IEEE Symposium on Computers and Communications*, (Alexandria, Egypt), June 2004.

[133] B.-T. Wang and H. Schulzrinne, "A robust packet filtering method for high bandwidth aggregates," in *IEEE Canadian Conference on Electrical and Computer Engineering 2004*, (Niagara Falls, Ontario, Canada), May 2004.

[134] B.-T. Wang and H. Schulzrinne, "An IP traceback mechanism for reflective DoS attacks," in *IEEE Canadian Conference on Electrical and Computer Engineering 2004*, (Niagara Falls, Ontario, Canada), May 2004.

[135] A. Dutta, P. Agrawal, S. Das, M. Elaoud, D. Famolari, S. Madhani, A. McAuley, and B. Kim, "Realizing mobile wireless internet telephony and streaming multimedia testbed," *Computer Communications*, Vol. 27, pp. 725–738, May 2004.

[136] L. Amini, A. Shaikh, and H. Schulzrinne, "Effective peering for multi-provider content delivery services," in *IEEE Infocom 2004*, (Hong Kong), Mar. 2004.

[137] B.-T. Wang and H. Schulzrinne, "Multifunctional ICMP messages for e-services," in *IEEE International Conference on e-Technology, e-Commerce and e-Service*, (Grand Hotel, Taipei, Taiwan), pp. 355–363, IEEE, IEEE, Mar. 2004.

[138] A. Dutta, S. Das, P. Li, A. McAuley, Y. Ohba, S. Baba, and H. Schulzrinne, "Secured mobile multimedia communication for wireless internet," in *International Conference on Network Sensing and Control*, (Taipei, Taiwan), IEEE, IEEE, Mar. 2004.

[139] K. Singh, X. Wu, J. Lennox, and H. Schulzrinne, "Comprehensive multi-platform collaboration," in *Multimedia Computing and Networking*, (San Jose, California, USA), SPIE's 16th Annual Symposium, IS&T - The Society for Imaging Science and Technology, and SPIE - The International Society for Optical Engineering, Jan. 2004.

[140] B.-T. Wang and H. Schulzrinne, "Tracing high bandwidth aggregates," in *IASTED International Conference on Communication, Network, and Information Security (CNIS)*, (New York City, NY, USA), pp. 165–170, IASTED, ACTA Press, Dec. 2003.

[141] B.-T. Wang and H. Schulzrinne, "Analysis of denial-of-service attacks on denial-of-service defensive measures," in *Globecom 2003 - General Conference*, (San Francisco Marriott, CA), pp. 1339–1343, IEEE, IEEE, Dec. 2003.

[142] B.-T. Wang and H. Schulzrinne, "Detecting offensive routers: A straightforward approach," in *IEEE International Carnahan Conference on Security Technology (ICCST)*, (Grand Hotel, Taipei, Taiwan), pp. 460–467, IEEE, IEEE, Oct. 2003.

[143] D. Wong, A. Dutta, H. Schulzrinne, and K. Young, "Managing simultaneous mobility of IP hosts," in *IEEE International Military Communications Conference (MILCOM)*, (Boston, MA, USA), IEEE, IEEE, Oct. 2003.

[144] X. Fu, H. Schulzrinne, and H. Tschofenig, "Mobility support for next-generation internet signaling protocols," in *VTC 2003 - IP Mobility*, Oct. 2003.

[145] S. Berger, H. Schulzrinne, S. Sidiroglou, and X. Wu, "Ubiquitous computing using SIP," in *ACM NOSSDAV 2003*, (Monterey, California, USC), pp. 82–89, June 2003.

[146] X. Wu and H. Schulzrinne, "Programmable end system services using SIP," in *International Conference on Communications*, (Anchorage, Alaska), pp. 789–793, May 2003.

[147] W. Jiang, K. Koguchi, and H. Schulzrinne, "Qos evaluation of voip end-points," in *ICC 2003 - Communication QoS, Reliability, and Performance Modeling*, May 2003.

[148] J. Lennox and H. Schulzrinne, "A protocol for reliable decentralized conferencing," in *ACM NOSSDAV 2003*, (Monterey, California, USC), June 2003.

[149] W. Zhao and H. Schulzrinne, "Predicting the upper bound of web traffic volume using a multiple time scale approach," in *International World Wide Web Conference (WWW) (poster session)*, (Budapest, Hungary), p. 243, May 2003.

[150] P.-Y. Hsieh, A. Dutta, and H. Schulzrinne, "Application layer mobility proxy for real-time communication," in *World Wireless Congress, 3G Wireless*, (San Francisco), Delson, Delson, May 2003.

[151] K. Singh, A. Nambi, and H. Schulzrinne, "Integrating voicexml with SIP services.," in *ICC 2003 - Global Services and Infrastructure for Next Generation Networks*, (Anchorage, Alaska), May 2003.

[152] L. Amini and H. Schulzrinne, "Modeling redirection in geographically diverse server sets," in *WWW*, (Budapest, Hungary), May 2003.

[153] N. Nakajima, A. Dutta, S. Das, and H. Schulzrinne, "Handoff delay analysis and measurement for SIP based mobility in ipv6," in *ICC 2003 - Personal Communication Systems and Wireless LANs*, May 2003.

[154] P. Mendes, H. Schulzrinne, and E. Monteiro, "Signaling protocol for session-aware popularity-based resource allocation," in *IFIP/IEEE International Conference on Management of Multimedia Networks and Services*, University of Santa Barbara, Oct. 2002.

[155] A. Dutta, D. Wong, J. Burns, R. Jain, K. Young, A. McAuley, and H. Schulzrinne, "Realization of integrated mobility management for ad-hoc networks," in *IEEE Milcom*, (Annaheim, California), Oct. 2002.

[156] L. Amini and H. Schulzrinne, "On probe strategies for dynamic multimedia server selection," in *IEEE Conference on Multimedia and Expo*, IEEE, Aug. 2002.

[157] L. Amini, A. Shaikh, and H. Schulzrinne, "Issues with inferring Internet topological attributes," in *ITcom Internet Performance and Control of Network Systems*, SPIE, July 2002.

[158] H. Schulzrinne and K. Arabshian, "Emergency calls and notifications," in *ITCom*, (Boston, Massachusetts), July/August 2002.

[159] W. Zhao and H. Schulzrinne, "Selective anti-entropy," in *ACM Symposium on Principles of Distributed Computing (PODC)*, (Monterey, California), ACM, ACM, July 2002.

[160] A. Dutta, O. Altintas, W. Chen, and H. Schulzrinne, "Mobility approaches for all IP wireless networks," in *SCI*, (Orlando, Florida), July 2002.

[161] P. Koskelainen, H. Schulzrinne, and X. Wu, "A SIP-based conference control framework," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Miami Beach, Florida), pp. 53–61, May 2002.

[162] W. Jiang and H. Schulzrinne, "Speech recognition performance as an effective perceived quality predictor," in *IWQoS*, (Miami Beach), May 2002.

[163] P. Mendes, H. Schulzrinne, and E. Monteiro, "Session-aware popularity resource allocation for assured differentiated services," in *Networking*, (Pisa, Italy), May 2002.

[164] W. Jiang and H. Schulzrinne, "Comparison and optimization of packet loss repair methods on VoIP perceived quality under bursty loss," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Miami Beach, Florida), May 2002.

[165] A. Dutta, J. Chen, S. Madhani, A. McAuley, N. Nakajima, and H. Schulzrinne, "Implementing a testbed for mobile multimedia," in *Proceedings of the IEEE Conference on Global Communications (GLOBECOM)*, (San Antonio, Texas), Nov. 2001.

[166] A. Dutta, R. Jain, D. Wong, J. Burns, K. Young, and H. Schulzrinne, "Multilayered mobility management for survivable network," in *Milcom*, (Vienna, Virginia), Nov. 2001.

[167] M. Papadopouli and H. Schulzrinne, "Effects of power conservation, wireless coverage and cooperation on data dissemination among mobile devices," in *Mobihoc*, (Long Beach, California), Oct. 2001.

[168] K. Wong, H.-Y. Wei, A. Dutta, K. Young, and H. Schulzrinne, "Performance of IP micro-mobility management scheme using host based routing," in *WPMC*, (Denmark), Aug. 2001.

[169] P. Pan and H. Schulzrinne, "Processing overhead studies in resource reservation protocols," in *17th International Teletraffic Congress*, (Salvador da Bahia, Brazil), Sept. 2001.

[170] H. Schulzrinne, "Keynote: Quality of service - 20 years old and ready to get a job?," *Lecture Notes in Computer Science*, Vol. 2092, p. 1, June 2001. International Workshop on Quality of Service (IWQoS).

[171] A. Dutta and H. Schulzrinne, "A streaming architecture for next generation Internet," in *Conference Record of the International Conference on Communications (ICC)*, (Helsinki), p. 7, June 2001.

[172] A. Dutta, F. Vakil, J. Chen, M. Tauil, S. Baba, and H. Schulzrinne, "Application layer mobility management scheme for wireless Internet," in *3Gwireless*, (San Francisco), p. 7, May 2001.

[173] A. Dutta, H. Schulzrinne, W. Chen, and O. Altintas, "Mobility support for wireless streaming multimedia in marconinet," in *IEEE Broadband Wireless Summit, Interop*, (Las Vegas), p. 7, May 2001.

[174] J. Brassil and H. Schulzrinne, "Enhancing Internet streaming media with cueing protocols," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Anchorage, Alaska), Apr. 2001.

[175] X. Wang and H. Schulzrinne, "Pricing network resources for adaptive applications in a differentiated services network," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Anchorage, Alaska), Apr. 2001.

[176] W. Zhao, H. Schulzrinne, and E. Guttman, "mSLP - mesh-enhanced service location protocol," in *International Conference on Computer Communication and Network*, (Las Vegas, Nevada), Oct. 2000.

[177] X. Wang, C. Yu, H. Schulzrinne, P. Stirpe, and W. Wu, "IP multicast faulty recovery in PIM over OSPF," in *International Conference on Network Protocols (ICNP)*, (Osaka, Japan), Nov. 2000.

[178] M. Papadopouli and H. Schulzrinne, "Seven degrees of separation in mobile ad hoc networks," in *Proceedings of the IEEE Conference on Global Communications (GLOBECOM)*, (San Francisco, California), Nov. 2000.

[179] W. Jiang and H. Schulzrinne, "Analysis of on-off patterns in VoIP and their effect on voice traffic aggregation," in *International Conference on Computer Communication and Network*, (Las Vegas, Nevada), Oct. 2000.

[180] M. Papadopouli, H. Schulzrinne, P. Castro, P. Kermani, C. Bisdikian, and M. Naghshineh, "Data gathering and distribution across widely distributed devices," in *SIGCOMM Symposium on Communications Architectures and Protocols*, (Stockholm, Sweden), August/September 2000. student poster session.

[181] X. Wang and H. Schulzrinne, "Adaptive reservation: A new framework for multimedia adaptation," in *IEEE International Conference on Multimedia and Expo (ICME)*, (New York), July/August 2000.

[182] D. Sisalem and H. Schulzrinne, "The adaptive load service: An ABR-Like service for the Internet," in *5th IEEE Symposium on Computers and Communications (ISCC)*, (Juan Les Pins, France), July 2000.

[183] X. Wang, C.-M. Yu, H. Schulzrinne, P. Stirpe, and W. Wu, "IP multicast fault recovery in PIM over OSPF," in *Proceedings of the ACM Sigmetrics Conference on Measurement and Modeling of Computer Systems*, (Santa Clara, California), June 2000.

[184] X. Wang, H. Schulzrinne, D. Kandlur, and D. Verma, "Measurement and analysis of LDAP performance," in *Proceedings of the ACM Sigmetrics Conference on Measurement and Modeling of Computer Systems*, (Santa Clara, California), June 2000.

[185] J. Lennox and H. Schulzrinne, "Feature interaction in Internet telephony," in *Feature Interaction in Telecommunications and Software Systems VI*, (Glasgow, United Kingdom), May 2000.

[186] J. Rosenberg, L. Qiu, and H. Schulzrinne, "Integrating packet FEC into adaptive voice playout buffer algorithms on the Internet," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Tel Aviv, Israel), Mar. 2000.

[187] E. Wedlund and H. Schulzrinne, "Mobility support using SIP," in *2nd ACM/IEEE International Conference on Wireless and Mobile Multimedia (WoWMoM)*, (Seattle, Washington), Aug. 1999.

[188] A. Dutta and H. Schulzrinne, "Marconinet - an architecture for Internet radio and TV networks," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Basking Ridge, New Jersey), pp. 241–245, June 1999.

[189] M. Papadopouli and H. Schulzrinne, "Connection sharing in an ad hoc wireless network among collaborating hosts," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Basking Ridge, New Jersey), pp. 169–185, June 1999.

[190] X. Wang and H. Schulzrinne, "RNAP: a resource negotiation and pricing protocol," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Basking Ridge, New Jersey), pp. 77–93, June 1999.

[191] H. Schulzrinne and J. Rosenberg, "Signaling for Internet telephony," in *International Conference on Network Protocols (ICNP)*, (Austin, Texas), Oct. 1998.

[192] P. Pan and H. Schulzrinne, "YESSIR: a simple reservation mechanism for the Internet," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Cambridge, England), pp. 141–151, July 1998. also IBM Research Technical Report TC20967.

[193] H. Schulzrinne and J. Rosenberg, "A comparison of SIP and H.323 for Internet telephony," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Cambridge, England), pp. 83–86, July 1998.

[194] D. Sisalem and H. Schulzrinne, "The loss-delay adjustment algorithm: A TCP-friendly adaptation scheme," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Cambridge, England), pp. 215–226, July 1998.

[195] I. Schubert, D. Sisalem, and H. Schulzrinne, "A session floor control scheme," in *International Conference on Telecommunications*, (Chalkidiki, Greece), June 1998.

[196] D. Sisalem, F. Emanuel, and H. Schulzrinne, "The direct adjustment algorithm: A TCP-Friendly adaptation scheme," 1998. submitted for publication.

[197] J. Rosenberg and H. Schulzrinne, "Internet telephony gateway location," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (San Francisco, California), pp. 488–496, March/April 1998.

[198] J. Rosenberg and H. Schulzrinne, "Timer reconsideration for enhanced RTP scalability," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (San Francisco, California), March/April 1998.

[199] P. Pan and H. Schulzrinne, "Staged refresh timers for RSVP," in *Proceedings of Global Internet*, (Phoenix, Arizona), Nov. 1997. also IBM Research Technical Report TC20966.

[200] H. Schulzrinne, "A comprehensive multimedia control architecture for the Internet," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (St. Louis, Missouri), May 1997.

[201] H. Schulzrinne, "Re-engineering the telephone system," in *IEEE Singapore International Conference on Networks (SICON)*, (Singapore), Apr. 1997.

[202] H. Schulzrinne, "Signaling for Internet telephony services," in *Opensig*, (New York, New York), Oct. 1996.

[203] H. Schulzrinne, "The impact of resource reservation for real-time Internet services," in *National Research Council (NRC) Workshop on Information System Trustworthiness*, (Washington, D.C.), Oct. 1996.

[204] D. Sisalem and H. Schulzrinne, "Congestion control in TCP: performance of binary congestion notification enhanced TCP compared to reno and tahoe TCP," in *International Conference on Network Protocols (ICNP)*, (Columbus, Ohio), pp. 268–275, Oct. 1996.

[205] D. Sisalem, H. Schulzrinne, and C. Sieckmeyer, "The network video terminal," in *HPDC Focus Workshop on Multimedia and Collaborative Environments (Fifth IEEE International Symposium on High Performance Distributed Computing)*, (Syracuse, New York), IEEE Computer Society, Aug. 1996.

[206] H. Schulzrinne, "The world-wide web as the universal interface to the NII," national research council (nrc) background paper, Columbia University, July 1996.

[207] D. Sisalem and H. Schulzrinne, "Binary congestion notification in TCP," in *Conference Record of the International Conference on Communications (ICC)*, (Dallas, Texas), IEEE, June 1996.

[208] D. Sisalem and H. Schulzrinne, "Switch mechanisms for the ABR service: A comparison study," in *Telecommunication Distribution Parallelism (TDP)*, (La Londes Les Maures, France), Institut National des Telecommunications, Evry, June 1996.

[209] H. Schulzrinne, M. Smirnov, R. Roth, and A. M. Wolisz, "IP multicasting over ATM: the multicube approach," in *3rd International Symposium on Interworking - INTERWORKING: High-Speed Networking and Interoperability*, (Nara, Japan), pp. 181–190, IOS Press/Ohmsha, Oct. 1996.

[210] H. Schulzrinne, "Personal mobility for multimedia services in the Internet," in *European Workshop on Interactive Distributed Multimedia Systems and Services (IDMS)*, (Berlin, Germany), Mar. 1996.

[211] D. Sisalem and H. Schulzrinne, "End-to-end rate control in ABR," in *1st Workshop on ATM Traffic Management (WATM)*, (Paris, France), pp. 281–287, IFIP WG 6.2, Dec. 1995.

[212] H. Schulzrinne, "When can we unplug the phone and the radio?," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, Lecture Notes in Computer Science (LNCS), (Durham, New Hampshire), pp. 183–184, Springer, Apr. 1995.

[213] H. Schulzrinne, "Internet services: from electronic mail to real-time multimedia," in *KIVS (Kommunikation in Verteilten Systemen)* (K. Franke, U. Hübner, and W. Kalfa, eds.), Informatik aktuell, (Chemnitz, Germany), pp. 21–34, Gesellschaft für Informatik, Springer Verlag, Feb. 1995.

[214] H. Schulzrinne, "Audio and video over packet networks — issues, architecture and protocols," in *INTEROP*, (Paris, France), Oct. 1994.

[215] H. Schulzrinne, "Conferencing and collaborative computing," in *Dagstuhl Seminar on Fundamentals and Perspectives of Multimedia Systems*, (Dagstuhl Castle, Germany), July 1994.

[216] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "An evaluation of scheduling mechanisms for providing best-effort, real-time communication in wide-area networks," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Toronto, Canada), June 1994.

[217] R. Ramjee, J. F. Kurose, D. F. Towsley, and H. Schulzrinne, "Adaptive playout mechanisms for packetized audio applications in wide-area networks," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Toronto, Canada), pp. 680–688, IEEE Computer Society Press, Los Alamitos, California, June 1994.

[218] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "Loss correlation for queues with bursty input streams," in *Conference Record of the International Conference on Communications (ICC)*, Vol. 1, (Chicago, Illinois), pp. 0219–0224 (308.4), IEEE, June 1992.

[219] H. Schulzrinne and J. F. Kurose, "Distribution of the loss period for some queues in continuous and discrete time," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, (Bal Harbour, Florida), pp. 1446–1455 (12C.1), Apr. 1991.

[220] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "Congestion control for real-time traffic in high-speed networks," in *Proceedings of the Conference on Computer Communications (IEEE Infocom)*, Vol. 2, (San Francisco, California), pp. 543–550, June 1990.

[221] H. Schulz-Rinne, "The DSP workbench: Modeling parallel architectures as concurrent processes," in *IEEE International Conference on Acoustics, Speech, and Signal Processing 1986*, (Tokyo, Japan), pp. 54.9.1–54.9.4, IEEE, Apr. 1986.

WORKSHOPS

[1] A. Y. Ding, Y. Liu, S. Tarkoma, H. Flinck, H. Schulzrinne, and J. Crowcroft, "Vision: Augmenting wifi offloading with an open-source collaborative platform," in *Proceedings of the 6th International Workshop on Mobile Cloud Computing and Services*, (Paris, France), pp. 44–48, Sept. 2015.

[2] H. Schulzrinne, K.-H. Kim, H. Nam, V. Singh, and D. Song, "QoE: A micro and macro perspective," in *NSF/FCC workshop on Tracking Quality of Experience in the Internet*, (Princeton, New Jersey), Oct. 2015.

[3] A. Y. Ding, J. Korhonen, T. Savolainen, Y. Liu, M. Kojo, S. Tarkoma, and H. Schulzrinne, "Reflections on middlebox detection mechanisms in IPv6 transition," in *Internet Architecture Board Workshop on Stack Evolution in a Middlebox Internet (IAB SEMI)*, (Zurich, Switzerland), Jan. 2015.

[4] H. Schulzrinne, "The Internet is a series of tubes," in *Towards an Affordable Internet Access for Everyone: The Quest for Enabling Universal Service Commitment (Dagstuhl Seminar 14471)* (J. Crowcroft, A. Wolisz, and A. Sathiaseelan, eds.), no. 11 in Dagstuhl Reports, pp. 78–137, Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015.

[5] A. Mehta, A. Forte, and H. Schulzrinne, "Using conference servers for SIP-based vertical handoff between IP and cellular networks," in *The 6th ACM International Workshop on Mobility Management and Wireless Access*, (Vancouver, British Columbia, Canada), Oct. 2008.

[6] S. Shin and H. Schulzrinne, "Call admission control in IEEE 802.11 WLANs using QP-CAT," in *The 27th IEEE International Conference on Computer Communications*, (Phoenix, Arizona, USA), Apr. 2008.

[7] J. Lee, H. Schulzrinne, W. Kellerer, and Z. Despotovic, "z2z: Discovering zeroconf services beyond local link," in *Globecom Workshops*, Nov. 2007.

[8] S. Srinivasan and H. Schulzrinne, "BonSwing: a GUI framework for Ad-Hoc applications using service discovery," in *CoNEXT Student Workshop*, (New York, USA), Dec. 2007.

[9] J. Lee, H. Schulzrinne, W. Kellerer, and Z. Despotovic, "Bootstrapping large-scale DHT networks," in *CoNEXT Student Workshop*, (New York, USA), Dec. 2007.

[10] O. Boyaci and H. Schulzrinne, "Application and desktop sharing," in *CoNEXT Student Workshop*, (New York, USA), Dec. 2007.

[11] V. Janardhan and H. Schulzrinne, "Peer assisted VoD for set-top box based IP network," in *P2P-TV '07: the 2007 workshop on Peer-to-peer streaming and IP-TV*, (Kyoto, Japan), Aug. 2007.

[12] H. Schulzrinne, H. Tschofenig, A. Newton, and T. Hardie, "LoST: a protocol for mapping geographic locations to public safety answering points," in *The First International Workshop on Next Generation Networks for First Responders and Critical Infrastructure*, (New Orleans, Louisiana, USA), Apr. 2007.

[13] H. Tschofenig, H. Schulzrinne, A. Newton, and M. Shanmugam, "Protecting First-Level responder resources in an IP-based emergency services architecture," in *The First International Workshop on Next Generation Networks for First Responders and Critical Infrastructure*, (New Orleans, Louisiana, USA), Apr. 2007.

[14] W. Yuen and H. Schulzrinne, "Localization for intermittently connected ad hoc networks," in *International Workshop on Intermittently Connected Mobile Ad Hoc Networks*, (Hoes Lane, Piscataway, NJ 08854), IEEE, IEEE, Mar. 2007.

[15] H. Schulzrinne, A. Forte, and S. Shin, "User mobility in IEEE 802.11 networks," in *Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture*, (San Francisco, California), pp. 7–8, ACM, Dec. 2006.

[16] M. Cristofano, A. Forte, H. Schulzrinne, and M. Longo, "A generic model for mobility management in beyond third generation networks," in *The First International Workshop on Broadband and Wireless Computing, Communication and Applications*, (Yogyakarta, Indonesia), IIWAS, Dec. 2006.

[17] S. Patnaik, E. Yardeni, H. Schulzrinne, G. Ormazabal, and D. Helms, "Securing SIP: scalable mechanisms for protecting SIP-Based VoIP systems," in *NANOG (North American Network Operators Group)*, (St. Louis, Missouri), NANOG, Oct. 2006.

[18] H. Tschofenig, H. Schulzrinne, and A. Newton, "IETF mapping protocol architecture," in *First SDO Emergency Services Coordination Workshop*, (New York, NY, USA), Oct. 2006.

[19] H. Schulzrinne, J. Polk, M. Linsner, and A. Newton, "IETF GEOPRIV: transmission of location information using DHCP," in *First SDO Emergency Services Coordination Workshop*, (New York, NY, USA), Oct. 2006.

[20] H. Schulzrinne and H. Tschofenig, "Emergency service identification," in *First SDO Emergency Services Coordination Workshop*, (New York, NY, USA), Oct. 2006.

[21] H. Tschofenig, H. Schulzrinne, A. Newton, J. Peterson, and A. Mankin, "The IETF geopriv and presence architecture focusing on location privacy," in *W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement*, (Ispra, Italy), W3C, Oct. 2006.

[22] H. Tschofenig, H. Schulzrinne, M. Linsner, J. Polk, and B. Rosen, "IETF ECRIT emergency service architecture," in *First SDO Emergency Services Coordination Workshop*, (New York, NY, USA), Oct. 2006.

[23] A. Forte, S. Shin, and H. Schulzrinne, "Improving layer 3 handoff delay in IEEE 802.11 wireless networks," in *Wireless Internet Conference (WICON)*, Aug. 2006.

[24] S. Shin and H. Schulzrinne, "Balancing uplink and downlink delay of VoIP trafc in WLANs using adaptive priority control (APC)," in *Qshine (3rd international conference on Quality of service in heterogeneous wired/wireless networks)*, Aug. 2006.

[25] K. Arabshian and H. Schulzrinne, "Distributed context-aware agent architecture for global service discovery," in *The Second International Workshop on Semantic Web Technology For Ubiquitous and Mobile Applications (SWUMA '06)*, 2006.

[26] K. Arabshian, H. Schulzrinne, D. Trossen, and D. Pavel, "GloServ: global service discovery using the OWL web ontology language," in *IEE International Workshop on Intelligent Environments (IE05)*, IEE, June 2005.

[27] C. Shen, H. Schulzrinne, S.-H. Lee, and J. Bang, "Routing dynamics measurement and detection for next step internet signaling protocol," in *IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services (E2EMON)*, IEEE/IFIP, May 2005.

[28] X. Wu, R. Shacham, M. Mintz-Habib, K. Singh, and H. Schulzrinne, "Location-based communication services," in *International Multimedia Conference, Workshop on Effective Telepresence*, pp. 55–56, ACM, Oct. 2004.

[29] A. Dutta, T. Zhang, S. Madhani, K. Taniuchi, K. Fujimoto, H. Schulzrinne, Y. Ohba, and Y. Katsube, "Secure universal mobility for wireless internet," in *The Second ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, (Philadelphia, PA,), Oct. 2004.

[30] W. Zhao and H. Schulzrinne, "DotSlash: a self-configuring and scalable rescue system for handling web hotspots effectively," in *International Workshop on Web Caching and Content Distribution (WCW)*, (Beijing, China), Oct. 2004.

[31] S. Shin, H. Schulzrinne, A. Forte, and A. Rawat, "Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs," in *ACM MobiWac (ACM International Workshop on Mobility Management and Wireless Access)*, (Philadelphia, Pennsylvania), ACM, Sept. 2004.

[32] C. Wieser, M. Laakso, and H. Schulzrinne, "SIP robustness testing for Large-Scale use," in *First International Workshop on Software Quality (SOQA)*, (Erfurt, Germany), Sept. 2004.

[33] K. Arabshian and H. Schulzrinne, "Glo-Serv: global service discovery architecture," in *MobiQuitous 2004 Services*, (Boston, Massachusetts, USA), Aug. 2004.

[34] R. Shacham, H. Schulzrinne, W. Kellerer, and S. Thakolsri, "An architecture for location-based service mobility using the SIP event model," in *ACM International Conference on Mobile Systems, Applications and Services (MobiSys), Workshop on Context Awareness*, ACM, June 2004.

[35] S. Khurana, A. Dutta, P. Gurung, and H. Schulzrinne, "XML based wide area communication with networked appliances," in *2004 IEEE Sarnoff Symposium*, (Princeton, New Jersey), Apr. 2004.

[36] K. Arabshian and H. Schulzrinne, "A generic event notification system using XML and SIP," in *New York Metro Area Networking Workshop 2003*, (Bern Dibner Library Building, LC400, Polytechnic University, 5 Metrotech Cente), Sept. 2003.

[37] B.-T. Wang and H. Schulzrinne, "A denial-of-service-resistant IP traceback approach," in *New York Metro Area Networking Workshop 2003*, (Bern Dibner Library Building, LC400, Polytechnic University, 5 Metrotech Cente), Sept. 2003.

[38] W. Jiang and H. Schulzrinne, "A black-box qos measurement methodology for voip end-points," in *New York Metro Area Networking Workshop 2003*, (Bern Dibner Library Building, LC400, Polytechnic University, 5 Metrotech Cente), Sept. 2003.

[39] K. Arabshian and H. Schulzrinne, "A sip-based medical event monitoring system," in *5th International Workshop on Enterprise Networking and Computing in Healthcare Industry (HealthCom)*, (Santa Monica, CA), June 2003.

[40] W. Jiang and H. Schulzrinne, "Assessment of voip service availability in the current internet," in *Passive & Active Measurement Workshop*, (San Diego, CA), Apr. 2003.

[41] P. Mendes, H. Schulzrinne, and E. Monteiro, "A receiver-driven adaptive mechanism based on the popularity of scalable sessions," in *COST 263 International Workshop on Quality of future Internet Services (QofIS)*, ETH Zurich, Oct. 2002.

[42] A. Dutta, H. Schulzrinne, O. Altintas, S. Das, A. McAuley, and W. Chen, "Marconinet supporting streaming media over localized wireless multicast," in *International Workshop of Mobile E-Commerce*, (Atlanta, Georgia), Sept. 2002.

[43] H. Schulzrinne and W. Jiang, "Quality of service - applications," in *NSF ITR Quality of Service Workshop*, (Annapolis, Maryland), Mar. 2002.

[44] H. Schulzrinne, "Interdomain and end-to-end QoS issues," in *NSF ITR Quality of Service Workshop*, (Annapolis, Maryland), Mar. 2002.

[45] L. Amini and H. Schulzrinne, "Observations from router-level Internet traces," in *DIMACS Workshop on Internet and WWW Measurement, Mapping and Modeling*, (Piscataway, New Jersey), Feb. 2002.

[46] K. Koguchi, W. Jiang, and H. Schulzrinne, "QoS measurement of VoIP end-points," in *IEICE Group meeting on Network Systems*, (Matsuyama, Japan), Dec. 2002.

[47] W. Zhao and H. Schulzrinne, "ARMS - automated replication for meshed servers," in *3rd NMADS (New York Metra Area Distributed Systems) Day*, (New York, NY), Apr. 2001.

[48] E. Hahne, P. Pan, and H. Schulzrinne, "Scalable resource reservation for Internet QoS," in *DIMACS Workshop on QoS*, (Rutgers University), Feb. 2001.

[49] W. Jiang, J. Lennox, H. Schulzrinne, and K. Singh, "Towards junking the PBX: deploying IP telephony," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Port Jefferson, New York), June 2001.

[50] K. Singh, G. Nair, and H. Schulzrinne, "Centralized conferencing using SIP," in *Internet Telephony Workshop*, (New York), Apr. 2001.

[51] X. Wu and H. Schulzrinne, "Where should services reside in Internet telephony systems?," in *IP Telecom Services Workshop*, (Atlanta, Georgia), pp. 35–40, Sept. 2000.

[52] K. Singh and H. Schulzrinne, "Unified messaging using SIP and RTSP," in *IP Telecom Services Workshop*, (Atlanta, Georgia), pp. 31–37, Sept. 2000.

[53] D. Sisalem and H. Schulzrinne, "The direct adjustment algorithm: A TCP-Friendly adaptation scheme," in *Quality of Future Internet Services*, (Berlin, Germany), Sept. 2000.

[54] X. Wang and H. Schulzrinne, "Performance study of congestion price based adaptive service," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Chapel Hill, North Carolina), pp. 1–10, June 2000.

[55] W. Jiang and H. Schulzrinne, "Modeling of packet loss and delay and their effect on real-time multimedia service quality," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, June 2000.

[56] H. Schulzrinne, "Internet telephony: A second chance," in *IP-Telephony Workshop (IPtel)*, (Berlin, Germany), Apr. 2000.

[57] K. Singh and H. Schulzrinne, "Interworking between SIP/SDP and H.323," in *IP-Telephony Workshop (IPtel)*, (Berlin, Germany), Apr. 2000.

[58] T. Eyers and H. Schulzrinne, "Predicting Internet telephony call setup delay," in *IP-Telephony Workshop (IPtel)*, (Berlin, Germany), Apr. 2000.

[59] J. Lennox and H. Schulzrinne, "The call processing language: User control of internet telephony services," in *Lucent Technologies XML Day*, (Murray Hill, NJ), Feb. 2000.

[60] H. Schulzrinne, "Feature interaction in Internet telephony," in *Feature Interaction in Telecommunication Networks IV*, (Montreal, Canada), p. 371, June 1997.

[61] H. Schulzrinne, "Scaling issues for the integrated services Internet," in *DIMACS: Workshop Architecture and Algorithmic Aspects of Communication Networks*, (New Brunswick, New Jersey), Jan. 1997.

[62] H. Schulzrinne and D. Sisalem, "Interaction of ATM and IP congestion control," in *Workshop on Integration of IP and ATM*, (St. Louis, Missouri), Nov. 1996.

[63] H. Schulzrinne, "Issues for session invitation protocols," in *Internet Engineering Task Force (IETF) Meeting*, (Montreal, California), June 1996.

[64] H. Schulzrinne, "Internet telephony – towards the integrated services Internet," in *IEEE Workshop on Internet Telephony*, (Utrecht, The Netherlands), Feb. 1996.

[65] H. Schulzrinne, J. Brassil, and A. K. Choudhury, "Internet access to IEEE journals: The september trial," in *Documents in Public Networks — Applications and Experiences (Dokumente in öffentlichen Netzen – Anwendungen und Erfahrungen)*, (Darmstadt, Germany), Nov. 1995.

[66] H. Schulzrinne, "Whither WWW — status, problems, directions," in *WWW für kommerzielle Anwender und kommerzielle Informationsanbieter im Internet (Supercomputer Tutorial)*, (Mannheim, Germany), June 1995.

[67] I. Busse, B. Deffner, and H. Schulzrinne, "Dynamic QoS control of multimedia applications based on RTP," in *1st International Workshop on High Speed Networks and Open Distributed Platforms*, (St. Petersburg, Russia), June 1995.

[68] H. Schulzrinne, "ATM: dangerous at any speed?," in *IEEE Gigabit Networking Workshop*, (Boston, Massachusetts), Apr. 1995.

[69] H. Schulzrinne, "QOS for real-time services: playout delay and application control," in *46th RACE Concertation Meeting (RCM)*, (Brussels, Belgium), Mar. 1995.

[70] H. Schulzrinne, "Quality of service in integrated networks." TUBKOM Seminar Series, Feb. 1995.

[71] L. Kleinrock, J. P. Sterbenz, N. F. Maxemchuk, S. S. Lam, P. Steenkiste, and H. Schulzrinne, "The national exchange for networked information systems: A white paper," in *Gigabit Networking Workshop*, (Toronto, Ontario), June 1994.

[72] H. Schulzrinne, "RTP: the real-time transport protocol," in *MCNC 2nd Packet Video Workshop*, Vol. 2, (Research Triangle Park, North Carolina), Dec. 1992.

[73] J. F. Kurose, D. F. Towsley, and H. Schulzrinne, "Scheduling policies for supporting real-time traffic in wide-area computer networks," in *Proc. International Workshop on Network and Operating System Support for Digital Audio and Video (NOSSDAV)*, (Berkeley, California), Nov. 1990. TR-90-062.

INTERNET RFCS AND DRAFTS

Note: Date shown is that of latest revision, not first version.

[1] S. Baset, H. Schulzrinne, and E. Shim, "A protocol for implementing various DHT algorithms," Internet Draft draft-baset-sipping-p2pcommon, Internet Engineering Task Force, Oct. 2006. Work in progress.

[2] G. Camarillo, H. Schulzrinne, and E. Burger, "The source and sink attributes for the session description protocol," Internet Draft draft-camarillo-mmusic-source-sink-01, Internet Engineering Task Force, Aug. 2003. Work in progress.

[3] A. Forte, S. Shin, and H. Schulzrinne, "Passive duplicate address detection for the dynamic host configuration protocol for IPv4 (DHCPv4)," Internet Draft draft-forte-dhc-passive-dad-01, Internet Engineering Task Force, Mar. 2006. Work in progress.

[4] X. Fu and M. et. al., "Mobility issues in next steps in signaling (NSIS)," Internet Draft draft-fu-nsis-mobility-01.txt,, Internet Engineering Task Force, Oct. 2003. Work in progress.

[5] H. Schulzrinne, S. Petrack, and T. Taylor, "Definition of events for Channel-Oriented telephony signalling," Internet Draft draft-ietf-avt-rfc2833biscas, IETF, Jan. 2007. Work in progress.

[6] H. Schulzrinne, S. Petrack, and T. Taylor, "Definition of events for modem, FAX, and text telephony signals," Internet Draft draft-ietf-avt-rfc2833bisdata, IETF, Feb. 2005. Work in progress.

[7] H. Schulzrinne and R. Marshall, "Requirements for emergency context resolution with internet technologies," Internet Draft draft-ietf-ecrit-requirements-12, Internet Engineering Task Force, Aug. 2006. Work in progress.

[8] H. Schulzrinne, "A uniform resource name (URN) for services," Internet Draft draft-ietf-ecrit-service-urn, Internet Engineering Task Force, Aug. 2006. Work in progress.

[9] T. Taylor, H. Tschofenig, H. Schulzrinne, and M. Shanmugam, "Security threats and requirements for emergency call marking and mapping," Internet Draft draft-ietf-ecrit-security-threats-03, Internet Engineering Task Force, July 2006. Work in progress.

[10] H. Schulzrinne, J. Polk, and H. Tschofenig, "A dynamic host configuration protocol (DHCP) based Location-to-Service translation protocol (LoST) discovery procedure," Internet Draft draft-ietf-ietf-ecrit-dhc-lost-discovery, Internet Engineering Task Force, Mar. 2007. Work in progress.

[11] H. Tschofenig and H. Schulzrinne, "GEOPRIV layer 7 location configuration protocol; problem statement and requirements," Internet Draft draft-ietf-geopriv-l7-lcp-ps, Internet Engineering Task Force, Jan. 2007. Work in progress.

[12] H. Schulzrinne and H. Tschofening, "Location types registry," Internet Draft draft-ietf-geopriv-location-types-registry-05, Internet Engineering Task Force, Mar. 2006. Work in progress.

[13] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, and J. Polk, "Policy rules for disclosure and modification of geographic information," Internet Draft draft-ietf-geopriv-policy-07, Internet Engineering Task Force, Oct. 2005. Work in progress.

[14] H. Schulzrinne, "Real time streaming protocol (RTSP)," Internet Draft draft-ietf-mmusic-rfc2326bis-05.txt,.ps,, Internet Engineering Task Force, Oct. 2003. Work in progress.

[15] H. Schulzrinne and R. Hancock, "GIMPS: general internet messaging protocol for signaling," Internet Draft draft-ietf-nsis-ntlp-11, Internet Engineering Task Force, Aug. 2006. Work in progress.

[16] H. Schulzrinne, "is-composing indication for instant messaging using the session initiation protocol (SIP)," Internet Draft draft-ietf-simple-iscomposing, Internet Engineering Task Force, Mar. 2004. Work in progress.

[17] J. Rosenberg, "Guidelines for authors of extensions to the session initiation protocol (SIP)," Internet Draft draft-ietf-sip-guidelines-07, Internet Engineering Task Force, Oct. 2003. Work in progress.

[18] H. Schulzrinne, "Emergency services URI for the session initiation protocol," Internet Draft draft-ietf-sipping-sos-00, Internet Engineering Task Force, Feb. 2004. Work in progress.

[19] J. Rosenberg, H. Schulzrinne, and B. Suter, "Wide area network service location," internet draft, Internet Engineering Task Force, Dec. 1997. Work in progress.

[20] J. Lee and H. Schulzrinne, "SIP URI service discovery using DNS-SD," Internet Draft draft-lee-sip-dns-sd-uri, Internet Engineering Task Force, Feb. 2007. Work in progress.

[21] J. Lennox, H. Schulzrinne, J. Nieh, and R. Baratto, "Protocols for application and desktop sharing," Internet Draft draft-lennox-avt-app-sharing, IETF, Dec. 2004. Work in progress.

[22] S. Narayanan, H. Schulzrinne, and A. Kundaje, "A diameter accounting application for the session initiation protocol," internet draft, Internet Engineering Task Force, Aug. 2002. Work in progress.

[23] P. Pan and H. Schulzrinne, "An evaluation on RSVP transport mechanism," internet draft, Internet Engineering Task Force, Mar. 2003. Work in progress.

[24] P. Pan, E. Hahne, and H. Schulzrinne, "BGRP: a framework for scalable resource reservation," internet draft, Internet Engineering Task Force, Jan. 2000. Work in progress.

[25] J. Rosenberg, J. Weinberger, and H. Schulzrinne, "NAT friendly SIP," internet draft, Internet Engineering Task Force, July 2001. Work in progress.

[26] J. Rosenberg, D. Drew, and H. Schulzrinne, "Getting SIP through firewalls and NATs," internet draft, Internet Engineering Task Force, Feb. 2000. Work in progress.

[27] H. Schulzrinne *et al.*, "RADIUS accounting for SIP servers," internet draft, Internet Engineering Task Force, Feb. 2002. Work in progress.

[28] H. Schulzrinne, "Synchronizing Location-to-Service translation (LoST) servers," Internet Draft draft-schulzrinne-ecrit-lost-sync, Internet Engineering Task Force, Nov. 2006. Work in progress.

[29] H. Schulzrinne, "A location reference event package for the session initiation protocol (SIP)," Internet Draft draft-schulzrinne-geopriv-locationref, Internet Engineering Task Force, Oct. 2006. Work in progress.

[30] H. Schulzrinne, "RELO: retrieving end system location information," Internet Draft draft-schulzrinne-geopriv-relo, Internet Engineering Task Force, Mar. 2007. Work in progress.

[31] H. Schulzrinne, "Composing presence information," Internet Draft draft-schulzrinne-simple-composition-00, Internet Engineering Task Force, July 2005. Work in progress.

[32] H. Schulzrinne, J. Lennox, J. Nieh, and R. Baratto, "Sharing and remote access to applications," Internet Draft draft-schulzrinne-mmusic-sharing, IETF, Sept. 2004. Work in progress.

[33] H. Schulzrinne, "Requirements for session initiation protocol (SIP)-based emergency calls," internet draft, Internet Engineering Task Force, Feb. 2003. Work in progress.

[34] H. Schulzrinne and B. Rosen, "Emergency services for internet telephony systems," Internet Draft draft-schulzrinne-sipping-emergency-arch-00, Internet Engineering Task Force, Feb. 2004. Work in progress.

[35] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "Session initiation protocol (SIP) session mobility," Internet Draft draft-shacham-sipping-session-mobility, IETF, Feb. 2005. Work in progress.

[36] C. Shen, H. Schulzrinne, S.-H. Lee, and J. Bang, "Internet routing dynamics and NSIS related considerations," internet draft, IETF, Oct. 2004. Work in progress.

[37] C. Shen, H. Schulzrinne, S.-H. Lee, and J. Bang, "NSIS operation over IP tunnels," Internet Draft draft-shen-nsis-tunnel-02, Internet Engineering Task Force, Mar. 2006. Work in progress.

[38] V. Singh, H. Schulzrinne, and H. Tschofenig, "Dynamic feature extensions to the presence information data format location object (PIDF-LO)," Internet Draft draft-singh-geopriv-pidf-lo-dynamic, Internet Engineering Task Force, Feb. 2007. Work in progress.

[39] K. Singh and H. Schulzrinne, "Data format and interface to an external peer-to-peer network for SIP location service," Internet Draft draft-singh-p2p-sip, Internet Engineering Task Force, Dec. 2006. Work in progress.

[40] V. Singh, H. Schulzrinne, and P. Boni, "Vehicle info event package," Internet Draft draft-singh-simple-vehicle-info, Internet Engineering Task Force, Mar. 2007. Work in progress.

[41] K. Singh and H. Schulzrinne, "Interworking between SIP/SDP and H.323," internet draft, Internet Engineering Task Force, May 2000. Work in progress.

[42] H. Tschofenig, D. Wing, H. Schulzrinne, T. Froment, and G. Dawirs, "Anti-SPIT : A document format for expressing Anti-SPIT authorization policies," Internet Draft draft-tschofenig-sipping-spit-policy, Internet Engineering Task Force, Feb. 2007. Work in progress.

[43] H. Tschofenig, H. Schulzrinne, D. Wing, J. Rosenberg, and D. Schwartz, "A framework to tackle spam and unwanted communication for internet telephony," Internet Draft draft-tschofenig-sipping-framework-spit-reduction, Internet Engineering Task Force, Jan. 1993.

[44] H. Tschofenig, G. Dawirs, T. Froment, D. Wing, D. Wing, and H. Schulzrinne, "Requirements for authorization policies to tackle spam and unwanted communication for internet telephony," Internet Draft draft-froment-sipping-spit-requirements, Internet Engineering Task Force, Feb. 2008.

[45] D. Trossen and H. Schulzrinne, "On-Demand access authorization for SIP event=20 subscriptions," Internet Draft draft-trossen-sipping-ondemand-00, Internet Engineering Task Force, Oct. 2003. Work in progress.

[46] S. Tsang, "Requirements for networked appliances: Wide-Area access, control, and interworking," internet draft, Internet Engineering Task Force, Sept. 2000. Work in progress.

[47] S. Tsang, "SIP extensions for communicating with networked appliances," internet draft, Internet Engineering Task Force, Nov. 2000. Work in progress.

[48] H. Tschofenig and H. Schulzrinne, "RSVP domain of interpretation for ISAKMP," Internet Draft draft-tschofenig-rsvp-doi-01, Internet Engineering Task Force, Oct. 2003. Work in progress.

[49] X. Wu and H. Schulzrinne, "Location-switch for call processing language (CPL)," internet draft, Internet Engineering Task Force, Feb. 2004. Work in progress.

[50] X. Wu, H. Schulzrinne, J. Lennox, and J. Rosenberg, "CPL extensions for presence," internet draft, Internet Engineering Task Force, June 2001. Work in progress.

[51] W. Zhao and H. Schulzrinne, "Locating IP-to-Public switched telephone network (PSTN) telephony gateways via SLP," internet draft, Internet Engineering Task Force, Feb. 2004. Work in progress.

[52] W. Zhao and H. Schulzrinne, "Enabling global service attributes in the service location protocol," internet draft, Internet Engineering Task Force, Oct. 2005. Work in progress.

[53] H. Schulzrinne, L. Liess, H. Tschofenig, B. Stark, and A. KÃ¼tt, "Location hiding: Problem statement and requirements," Internet Draft draft-schulzrinne-ecrit-location-hiding-req, Internet Engineering Task Force, Mar. 2008.

[54] H. Schulzrinne, S. McCann, G. Bajko, and H. Tschofenig, "Extensions to the emergency services architecture for dealing with unauthenticated and unauthorized devices," Internet Draft draft-schulzrinne-ecrit-unauthenticated-access-02, Internet Engineering Task Force, Feb. 2008.

[55] H. Schulzrinne, "Applications and media information (AMI) extension to the presence information data format," Internet Draft draft-schulzrinne-simple-ami-00, Internet Engineering Task Force, Nov. 2007.

[56] R. Barnes, M. Lepinski, H. Tschofenig, and H. Schulzrinne, "Security requirements for the geopriv location system," Internet Draft draft-barnes-geopriv-lo-sec-02, Internet Engineering Task Force, Feb. 2008.

[57] M. Barnes, C. Boulton, and H. Schulzrinne, "Centralized conferencing manipulation protocol," Internet Draft draft-barnes-xcon-ccmp-04, Internet Engineering Task Force, Feb. 2008.

[58] S. Baset, H. Schulzrinne, and M. Matuszewski, "Peer-to-Peer protocol (P2PP)," Internet Draft draft-baset-p2psip-p2pp, Internet Engineering Task Force, Nov. 2007.

[59] C. Jennings, B. Lowekamp, E. Rescorla, J. Rosenberg, S. Baset, and H. Schulzrinne, "REsource LOcation and discovery (RELOAD)," Internet Draft draft-bryan-p2psip-reload, Internet Engineering Task Force, Feb. 2008.

[60] A. Dutta, H. Yokota, T. Chiba, and H. Schulzrinne, "ProxyMIP extension for InterMAG route optimization," Internet Draft draft-dutta-netlmm-pmipro-00, Internet Engineering Task Force, Feb. 2008.

[61] A. Forte and H. Schulzrinne, "Location-to-Service translation protocol (LoST) extensions," Internet Draft draft-forte-ecrit-lost-extensions, Internet Engineering Task Force, Mar. 2008.

[62] M. GarcÃa-MartÃn, H. Tschofenig, and H. Schulzrinne, "Indirect presence publication with the session initiation protocol (SIP)," Internet Draft draft-garcia-simple-indirect-presence-publish, Internet Engineering Task Force, Feb. 2008.

[63] V. Hilt, I. Widjaja, and D. Malas, "Session initiation protocol (SIP) overload control," Internet Draft draft-hilt-sipping-overload, Internet Engineering Task Force, Feb. 2008.

[64] A. Houri, S. Parameswar, E. Aoki, V. Singh, and H. Schulzrinne, "Scaling requirements for presence in SIP/SIMPLE," Internet Draft draft-houri-sipping-presence-scaling-requirements, Internet Engineering Task Force, Nov. 2007.

[65] B. Rosen, H. Schulzrinne, B. Rosen, and A. Newton, "Framework for emergency calling using internet multimedia," Internet Draft draft-ietf-ecrit-framework, Internet Engineering Task Force, Feb. 2008.

[66] A. Houri, E. Aoki, S. Parameswar, T. Rang, V. Singh, and H. Schulzrinne, "Presence interdomain scaling analysis for SIP/SIMPLE," Internet Draft draft-ietf-simple-interdomain-scaling-analysis, Internet Engineering Task Force, Feb. 2008.

[67] A. Houri, S. Parameswar, E. Aoki, V. Singh, and H. Schulzrinne, "Scaling requirements for presence in SIP/SIMPLE," Internet Draft draft-ietf-sipping-presence-scaling-requirements, Internet Engineering Task Force, Feb. 2008.

[68] A. Dutta, V. Fajardo, Y. Ohba, K. Taniuchi, and H. Schulzrinne, "A framework of Media-Independent Pre-Authentication (MPA) for inter-domain handover optimization," Internet Draft draft-irtf-mobopts-mpa-framework, Internet Engineering Task Force, Feb. 2008.

[69] A. Melnikov, H. Schulzrinne, and Q. Sun, "Sieve notification mechanism: SIP MESSAGE," Internet Draft draft-melnikov-sieve-notify-sip-message, Internet Engineering Task Force, Feb. 2008.

[70] J. Seedorf, S. Niccolini, and H. Schulzrinne, "Spam score for SIP: a proposal for semantics," Internet Draft draft-seedorf-sipping-spam-score-semantics, Internet Engineering Task Force, Feb. 2008.

[71] H. Tschofenig, J. Ott, H. Schulzrinne, T. Henderson, and G. Camarillo, "Interaction between SIP and HIP," Internet Draft draft-tschofenig-hiprg-host-identities, Internet Engineering Task Force, Feb. 2008.

[72] B. Rosen, H. Schulzrinne, and H. Tschofenig, "Session initiation protocol (SIP) event package for the common alerting protocol (CAP)," Internet Draft draft-rosen-sipping-cap, Internet Engineering Task Force, May 2008.

[73] J. Winterbottom, H. Tschofenig, H. Schulzrinne, M. Thomson, and M. Dawson, "An HTTPS location dereferencing protocol using HELD," Internet Draft draft-winterbottom-geopriv-deref-protocol, Internet Engineering Task Force, Nov. 2007.

[74] D. Wong, A. Dutta, and H. Schulzrinne, "Simultaneous mobility problem statement," Internet Draft draft-wong-mext-simultaneous-ps, Internet Engineering Task Force, Feb. 2008.

[75] M. GarcÃa-MartÃn and H. Schulzrinne, "Notification of general events using the session initiation protocol (SIP) event notification framework," Internet Draft draft-garcia-sipping-general-events, Internet Engineering Task Force, May 2007.

[76] S. Greco Polito and H. Schulzrinne, "Authentication, authorization, accounting and billing of roaming users using SAML," Internet Draft draft-greco-sipping-roaming, Internet Engineering Task Force, July 2007.

[77] R. Shacham and H. Schulzrinne, "HTTP header for future correspondence addresses," Internet Draft draft-shacham-http-corr-uris, Internet Engineering Task Force, May 2007.

[78] H. Tschofenig and H. Schulzrinne, "Emergency services architecture overview: Sharing responsibilities," Internet Draft draft-tschofenig-ecrit-architecture-overview, Internet Engineering Task Force, July 2007.

[79] H. Tschofenig and H. Schulzrinne, "A GEOPRIV HTTPS using protocol," Internet Draft draft-tschofenig-geopriv-http-using-protocol, Internet Engineering Task Force, July 2007.

[80] A. Forte and H. Schulzrinne, "Classification of location-based services," Internet Draft draft-forte-ecrit-service-classification, Internet Engineering Task Force, May 2008.

[81] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: a transport protocol for Real-Time applications," RFC 1889, Internet Engineering Task Force, Jan. 1996.

[82] H. Schulzrinne, "RTP profile for audio and video conferences with minimal control," RFC 1890, Internet Engineering Task Force, Jan. 1996.

[83] H. Schulzrinne, A. Rao, and R. Lanphier, "Real time streaming protocol (RTSP)," RFC 2326, Internet Engineering Task Force, Apr. 1998.

[84] H. Lu, M. Krishnaswamy, L. Conroy, S. M. Bellovin, F. Burg, A. DeSimone, K. Tewani, and P. J. Davidson, "Toward the PSTN/Internet Inter-Networking–Pre-PINT implementations," RFC 2458, Internet Engineering Task Force, Nov. 1998.

[85] M. Handley, H. Schulzrinne, E. M. Schooler, and J. Rosenberg, "SIP: session initiation protocol," RFC 2543, Internet Engineering Task Force, Mar. 1999.

[86] J. Rosenberg and H. Schulzrinne, "An RTP payload format for generic forward error correction," RFC 2733, Internet Engineering Task Force, Dec. 1999.

[87] J. Rosenberg and H. Schulzrinne, "Sampling of the group membership in RTP," RFC 2762, Internet Engineering Task Force, Feb. 2000.

[88] J. Lennox and H. Schulzrinne, "Call processing language framework and requirements," RFC 2824, Internet Engineering Task Force, May 2000.

[89] H. Schulzrinne and S. Petrack, "RTP payload for DTMF digits, telephony tones and telephony signals," RFC 2833, Internet Engineering Task Force, May 2000.

[90] J. Rosenberg and H. Schulzrinne, "A framework for telephony routing over IP," RFC 2871, Internet Engineering Task Force, June 2000.

[91] J. Rosenberg and H. Schulzrinne, "Registration of parityfec MIME types," RFC 3009, Internet Engineering Task Force, Nov. 2000.

[92] J. Lennox, H. Schulzrinne, and J. Rosenberg, "Common gateway interface for SIP," RFC 3050, Internet Engineering Task Force, Jan. 2001.

[93] C. E. Perkins, J. Rosenberg, and H. Schulzrinne, "RTP testing strategies," RFC 3158, Internet Engineering Task Force, Aug. 2001.

[94] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. R. Johnston, J. Peterson, R. Sparks, M. Handley, and E. M. Schooler, "SIP: session initiation protocol," RFC 3261, Internet Engineering Task Force, June 2002.

[95] J. Rosenberg and H. Schulzrinne, "Reliability of provisional responses in session initiation protocol (SIP)," RFC 3262, Internet Engineering Task Force, June 2002.

[96] J. Rosenberg and H. Schulzrinne, "Session initiation protocol (SIP): locating SIP servers," RFC 3263, Internet Engineering Task Force, June 2002.

[97] J. Rosenberg and H. Schulzrinne, "An Offer/Answer model with session description protocol (SDP)," RFC 3264, Internet Engineering Task Force, June 2002.

[98] H. Schulzrinne and B. Volz, "Dynamic host configuration protocol (DHCPv6) options for session initiation protocol (SIP) servers," RFC 3319, Internet Engineering Task Force, July 2003.

[99] H. Schulzrinne, D. Oran, and G. Camarillo, "The reason header field for the session initiation protocol (SIP)," RFC 3326, Internet Engineering Task Force, Dec. 2002.

[100] H. Schulzrinne, "Dynamic host configuration protocol (DHCP-for-IPv4) option for session initiation protocol (SIP) servers," RFC 3361, Internet Engineering Task Force, Aug. 2002.

[101] G. Camarillo, G. Eriksson, J. Holler, and H. Schulzrinne, "Grouping of media lines in the session description protocol (SDP)," RFC 3388, Internet Engineering Task Force, Dec. 2002.

[102] W. Zhao, H. Schulzrinne, E. Guttman, C. Bisdikian, and W. Jerome, "Select and sort extensions for the service location protocol (SLP)," RFC 3421, Internet Engineering Task Force, Nov. 2002.

[103] B. Campbell, J. Rosenberg, and Y. E. E. Liu, eds., "Session initiation protocol (SIP) extension for instant messaging," RFC 3428, Internet Engineering Task Force, Dec. 2002.

[104] H. Schulzrinne, "Requirements for resource priority mechanisms for the session initiation protocol (SIP)," RFC 3487, Internet Engineering Task Force, Feb. 2003.

[105] W. Zhao, H. Schulzrinne, and E. Guttman, "Mesh-enhanced service location protocol (mSLP)," RFC 3528, Internet Engineering Task Force, Apr. 2003.

[106] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: a transport protocol for Real-Time applications," RFC 3550, Internet Engineering Task Force, July 2003.

[107] H. Schulzrinne and S. Casner, "RTP profile for audio and video conferences with minimal control," RFC 3551, Internet Engineering Task Force, July 2003.

[108] J. Rosenberg and H. Schulzrinne, "An extension to the session initiation protocol (SIP) for symmetric response routing," RFC 3581, Internet Engineering Task Force, Aug. 2003.

[109] J. Rosenberg, J. Peterson, H. Schulzrinne, and G. Camarillo, "Best current practices for third party call control (3pcc) in the session initiation protocol (SIP)," RFC 3725, Internet Engineering Task Force, Apr. 2004.

[110] W. Zhao, H. Schulzrinne, E. Guttman, C. Bisdikian, and W. Jerome, "Remote service discovery in the service location protocol (SLP) via DNS SRV," RFC 3832, Internet Engineering Task Force, July 2004.

[111] J. Rosenberg, P. Kyzivat, and H. Schulzrinne, "Indicating user agent capabilities in the session initiation protocol (SIP)," RFC 3840, Internet Engineering Task Force, Aug. 2004.

[112] J. Rosenberg, H. Schulzrinne, and P. Kyzivat, "Caller preferences for the session initiation protocol (SIP)," RFC 3841, Internet Engineering Task Force, Aug. 2004.

[113] J. Lennox, X. Wu, and H. Schulzrinne, "Call processing language (CPL): a language for user control of internet telephony services," RFC 3880, Internet Engineering Task Force, Oct. 2004.

[114] G. Camarillo and H. Schulzrinne, "Early media and ringing tone generation in the session initiation protocol (SIP)," RFC 3960, Internet Engineering Task Force, Dec. 2004.

[115] H. Schulzrinne, "The tel URI for telephone numbers," RFC 3966, Internet Engineering Task Force, Dec. 2004.

[116] H. Schulzrinne, "Indication of message composition for instant messaging," RFC 3994, Internet Engineering Task Force, Jan. 2005.

[117] G. Camarillo, E. W. Burger, H. Schulzrinne, and A. van Wijk, "Transcoding services invocation in the session initiation protocol (SIP) using third party call control (3pcc)," RFC 4117, Internet Engineering Task Force, June 2005.

[118] H. Schulzrinne and C. Agboh, "Session initiation protocol (SIP)-H.323 interworking requirements," RFC 4123, Internet Engineering Task Force, July 2005.

[119] J. Rosenberg, H. Schulzrinne, and G. Camarillo, "The stream control transmission protocol (SCTP) as a transport for the session initiation protocol (SIP)," RFC 4168, Internet Engineering Task Force, Oct. 2005.

[120] J. Rosenberg, H. Schulzrinne, and R. Mahy, "An INVITE-Initiated dialog event package for the session initiation protocol (SIP)," RFC 4235, Internet Engineering Task Force, Nov. 2005.

[121] P. Koskelainen, J. Ott, H. Schulzrinne, and X. Wu, "Requirements for floor control protocols," RFC 4376, Internet Engineering Task Force, Feb. 2006.

[122] H. Schulzrinne and J. Polk, "Communications resource priority for the session initiation protocol (SIP)," RFC 4412, Internet Engineering Task Force, Feb. 2006.

[123] Y. Nomura, R. Walsh, J.-P. Luoma, H. Asaeda, and H. Schulzrinne, "A framework for the usage of internet media guides (IMGs)," RFC 4435, Internet Engineering Task Force, Apr. 2006.

[124] Y. Nomura, R. Walsh, J.-P. Luoma, J. Ott, and H. Schulzrinne, "Requirements for internet media guides (IMGs)," RFC 4473, Internet Engineering Task Force, May 2006.

[125] R. J. Sparks, A. Hawrylyshen, A. Johnston, J. Rosenberg, and H. Schulzrinne, "Session initiation protocol (SIP) torture test messages," RFC 4475, Internet Engineering Task Force, May 2006.

[126] H. Schulzrinne, V. Gurbani, P. Kyzivat, and J. Rosenberg, "RPID: rich presence extensions to the presence information data format (PIDF)," RFC 4480, Internet Engineering Task Force, July 2006.

[127] H. Schulzrinne, "Timed presence extensions to the presence information data format (PIDF) to indicate status information for past and future time intervals," RFC 4481, Internet Engineering Task Force, July 2006.

[128] H. Schulzrinne, "CIPID: contact information for the presence information data format," RFC 4482, Internet Engineering Task Force, July 2006.

[129] J. Rosenberg and H. Schulzrinne, "Guidelines for authors of extensions to the session initiation protocol (SIP)," RFC 4485, Internet Engineering Task Force, May 2006.

[130] H. Schulzrinne and H. Tschofenig, "Location types registry," RFC 4589, Internet Engineering Task Force, July 2006.

[131] H. Schulzrinne, "Dynamic host configuration protocol (DHCPv4 and DHCPv6) option for civic addresses configuration information," rfc, Internet Engineering Task Force, Oct. 2006.

[132] H. Schulzrinne and T. Taylor, "RTP payload for DTMF digits, telephony tones, and telephony signals," RFC 4733, Internet Engineering Task Force, Dec. 2006.

[133] H. Schulzrinne and T. Taylor, "Definition of events for modem, fax, and text telephony signals," RFC 4734, Internet Engineering Task Force, Dec. 2006.

[134] H. Schulzrinne, H. Tschofenig, J. Morris, J. R. Cuellar, J. Polk, and J. Rosenberg, "Common policy: A document format for expressing privacy preferences," RFC 4745, Internet Engineering Task Force, Feb. 2007.

[135] H. Schulzrinne, "Dynamic host configuration protocol (DHCPv4 and DHCPv6) option for civic addresses configuration information," RFC 4776, Internet Engineering Task Force, Nov. 2006.

[136] H. Schulzrinne and R. S. Marshall, "Requirements for emergency context resolution with internet technologies," RFC 5012, Internet Engineering Task Force, Jan. 2008.

[137] H. Schulzrinne, "A uniform resource name (URN) for emergency and other Well-Known services," RFC 5031, Internet Engineering Task Force, Jan. 2008.

[138] T. Taylor, H. Tschofenig, H. Schulzrinne, and M. Shanmugam, "Security threats and requirements for emergency call marking and mapping," RFC 5069, Internet Engineering Task Force, Jan. 2008.

[139] T. Hardie, A. L. Newton, H. Schulzrinne, and H. Tschofenig, "LoST: a Location-to-Service translation protocol," RFC 5222, Internet Engineering Task Force, Aug. 2008.

[140] H. Schulzrinne, J. Polk, and H. Tschofenig, "Discovering Location-to-Service translation (LoST) servers using the dynamic host configuration protocol (DHCP)," RFC 5223, Internet Engineering Task Force, Aug. 2008.

[141] H. Schulzrinne and T. Taylor, "Definition of events for Channel-Oriented telephony signalling," RFC 5244, Internet Engineering Task Force, June 2008.

[142] H. Schulzrinne, "Location-to-URL mapping architecture and framework," RFC 5582, Internet Engineering Task Force, Sept. 2009.

[143] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "Session initiation protocol (SIP) session mobility," RFC 5631, Internet Engineering Task Force, Oct. 2009.

[144] H. Tschofenig and H. Schulzrinne, "GEOPRIV layer 7 location configuration protocol: Problem statement and requirements," RFC 5687, Internet Engineering Task Force, Mar. 2010.

[145] H. Schulzrinne, E. Marocco, and E. Ivov, "Security issues and solutions in Peer-to-Peer systems for realtime communications," RFC 5765, Internet Engineering Task Force, Feb. 2010.

[146] G. Camarillo and H. Schulzrinne, "The session description protocol (SDP) grouping framework," RFC 5888, Internet Engineering Task Force, June 2010.

[147] H. Schulzrinne, V. K. Singh, H. Tschofenig, and M. Thomson, "Dynamic extensions to the presence information data format location object (PIDF-LO)," RFC 5962, Internet Engineering Task Force, Sept. 2010.

[148] H. Schulzrinne and R. E. Hancock, "GIST: general internet signalling transport," RFC 5971, Internet Engineering Task Force, Oct. 2010.

[149] C. Shen, H. Schulzrinne, S.-H. Lee, and J. H. Bang, "NSIS operation over IP tunnels," RFC 5979, Internet Engineering Task Force, Mar. 2011.

[150] A. Dutta, V. Fajardo, Y. Ohba, K. Taniuchi, and H. Schulzrinne, "A framework of media-independent pre-authentication (mpa) for inter-domain handover optimization," Request for Comments 6252, Internet Engineering Task Force, June 2011.

[151] R. Barnes, M. Lepinski, A. Cooper, J. Morris, H. Tschofenig, and H. Schulzrinne, "An architecture for location and location privacy in internet applications," Request for Comments 6280, Internet Engineering Task Force, July 2011.

[152] B. Rosen, H. Schulzrinne, J. Polk, and A. Newton, "Framework for emergency calling using Internet multimedia," Request for Comments 6443, Internet Engineering Task Force, Dec. 2011.

[153] A. Forte and H. Schulzrinne, "Location-to-service translation (LoST) protocol extensions," Request for Comments 6451, Internet Engineering Task Force, Dec. 2011.

[154] M. Barnes, C. Boulton, S. P. Romano, and H. Schulzrinne, "Centralized conferencing manipulation protocol," Request for Comments 6503, Internet Engineering Task Force, Mar. 2012.

[155] H. Schulzrinne and H. Tschofenig, "Synchronizing service boundaries and <mapping> elements based on the location-to-service translation (LoST) protocol," Request for Comments 6739, Internet Engineering Task Force, Oct. 2012.

[156] J. Winterbottom, H. Tschofenig, H. Schulzrinne, and M. Thomson, "A location dereference protocol using HTTP-enabled location delivery (HELD)," Request for Comments 6753, Internet Engineering Task Force, Oct. 2012.

[157] H. Schulzrinne, H. Tschofenig, J. R. Cuellar, J. Polk, J. B. Morris, and M. Thomason, "Geolocation policy: A document format for expressing privacy preferences for location information," Request for Comments 6772, Internet Engineering Task Force, Jan. 2013.

[158] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset, and H. Schulzrinne, "Resource location and discovery (RELOAD) base protocol," Request for Comments 6940, Internet Engineering Task Force, Jan. 2014.

[159] H. Schulzrinne, H. Tschofenig, C. Holmberg, and M. Patel, "Public safety answering point (PSAP) callback," Request for Comments 7090, Internet Engineering Task Force, Apr. 2014.

[160] C. Shen, H. Schulzrinne, and A. Koike, "A session initiation protocol (SIP) load-control event package," Request for Comments 7200, Internet Engineering Task Force, Apr. 2014.

[161] V. Gurbani, V. Hilt, and H. Schulzrinne, "Session Initiation Protocol (SIP) overload control," Request for Comments 7339, Internet Engineering Task Force, Sept. 2014.

[162] J. Peterson, H. Schulzrinne, and H. Tschofenig, "Secure telephone identity problem statement and requirements," Request for Comments 7340, Internet Engineering Task Force, Sept. 2014.

[163] H. Tschofenig, H. Schulzrinne, and B. Aboba, "Trustworthy location," Request for Comments 7378, Internet Engineering Task Force, Dec. 2014.

[164] H. Schulzrinne, S. McCann, G. Bajko, H. Tschofenig, and D. Kroeselberg, "Extensions to the emergency services architecture for dealing with unauthenticated and unauthorized devices," Request for Comments 7406, Internet Engineering Task Force, Dec. 2014.

[165] H. Schulzrinne, A. Rao, R. Lanphier, M. Westerlund, and M. Stiemerling, "Real-time streaming protocol version 2.0," Request for Comments 7826, Internet Engineering Task Force, Dec. 2016.

[166] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset, H. Schulzrinne, and T. Schmidt, "A SIP usage for REsource LOcation And Discovery (RELOAD)," Request for Comments 7904, Internet Engineering Task Force, Oct. 2016.

[167] H. Schulzrinne, "A SIP response code for unwanted calls," Request for Comments 8197, Internet Engineering Task Force, July 2017.

[1] H. Schulzrinne, "The Internet is a series of tubes," Technical Report cucs-027-14, Department of Computer Science, Columbia University, New York, New York, Nov. 2014.

[2] H. Nam, K.-H. Kim, D. Calin, and H. Schulzrinne, "Towards dynamic network condition-aware video server selection algorithms over wireless networks," Technical Report cucs-001-14, Department of Computer Science, Columbia University, New York, New York, Jan. 2014.

[3] H. Nam, K. H. Kim, B. H. Kim, D. Calin, and H. Schulzrinne, "Towards a dynamic QoS-aware over-the-top video streaming in LTE," Technical Report cucs-002-14, Department of Computer Science, Columbia University, New York, New York, Jan. 2014.

[4] A. Singh, G. Ormazabal, S. Addepalli, and H. Schulzrinne, "Heterogeneous access: Survey and design considerations," Technical Report cucs-028-13, Department of Computer Science, Columbia University, New York, New York, Oct. 2013.

[5] H. Nam, B. H. Kim, D. Calin, and H. Schulzrinne, "A mobile video traffic analysis: Badly designed video clients can waste network bandwidth," Technical Report cucs-018-13, Department of Computer Science, Columbia University, New York, New York, July 2013.

[6] H. Nam, J. Janak, and H. Schulzrinne, "Connecting the physical world with Arduino in SECE," Technical Report cucs-013-13, Department of Computer Science, Columbia University, New York, New York, May 2013.

[7] J. Marasevic, J. Janak, H. Schulzrinne, and G. Zussman, "WiMAX in the classroom: Designing a cellular networking hands-on lab," Technical Report 2013-03-14, Department of Electrical Engineering, Columbia University, New York, New York, Mar. 2013.

[8] W. Song, J. W. Lee, B. S. Lee, and H. Schulzrinne, "Finding 9-1-1 callers in tall buildings," Technical Report cucs-001-13, Columbia University, New York, New York, Jan. 2013.

[9] W. Song, J. W. Lee, B. S. Lee, and H. Schulzrinne, "Improving vertical accuracy of indoor positioning for emergency communication," Technical Report cucs-016-12, Columbia University, New York, New York, Oct. 2012.

[10] J. W. Lee, R. Francescangeli, W. Song, E. Maccherani, J. Janak, S. Srinivasan, M. S. Kester, S. A. Baset, and H. Schulzrinne, "NetServ: Reviving active networks," Technical Report cucs-001-12, Columbia University, New York, New York, Jan. 2012.

[11] J. Janak, J. W. Lee, and H. Schulzrinne, "GRAND: Git revisions as named data," Technical Report cucs-047-11, Columbia University, New York, New York, Dec. 2011.

[12] S. Srinivasan, J. W. Lee, D. Batni, and H. Schulzrinne, "ActiveCDN: Cloud computing meets content delivery networks," Technical Report cucs-045-11, Columbia University, New York, New York, Nov. 2011.

[13] E. Maccherani, J. W. Lee, M. Femminella, G. Reali, and H. Schulzrinne, "NetServ on OpenFlow 1.0," Technical Report cucs-036-11, Columbia University, New York, New York, Sept. 2011.

[14] S. Seo, J. Janak, and H. Schulzrinne, "Columbia University WiMAX campus deployment and installation," Technical Report cucs-032-11, Columbia University, New York, New York, June 2011.

[15] K. H. Kim, V. K. Singh, and H. Schulzrinne, "DYSWIS: collaborative network fault diagnosis - of end-users, by end-users, for end-users," Tech. Rep. cucs-017-11, Columbia University, May 2011.

[16] J. W. Lee, R. Francescangeli, W. Song, J. Janak, S. Srinivasan, M. Kester, S. A. Baset, E. Liu, H. Schulzrinne, V. Hilt, Z. Despotovic, and W. Kellerer, "NetServ framework design and implementation 1.0," Tech. Rep. cucs-016-11, Columbia University, May 2011.

[17] A. Srivastava, J. W. Lee, and H. Schulzrinne, "Implementing zeroconf in linphone," Tech. Rep. cucs-011-11, Columbia University, Mar. 2011.

[18] M. Kester, E. Liu, J. W. Lee, and H. Schulzrinne, "NetServ: early prototype experiences," Tech. Rep. cucs-031-10, Columbia University, Dec. 2010.

[19] H. Cui, S. Srinivasan, and H. Schulzrinne, "ONEChat: enabling group chat and messaging in opportunistic networks," Tech. Rep. cucs-001-10, Columbia University, Jan. 2010.

[20] S. G. Hong, H. Schulzrinne, and S. Weiland, "PBS: signaling architecture for network traffic authorization," Tech. Rep. cucs-045-09, Columbia University, Oct. 2009.

[21] C. Shen and H. Schulzrinne, "On TCP-based SIP server overload control," Tech. Rep. cucs-048-09, Columbia University, Nov. 2009.

[22] C. Shen, E. Nahum, H. Schulzrinne, and C. Wright, "The impact of TLS on SIP server performance," Tech. Rep. cucs-022-09, Columbia University, May 2009.

[23] K. Ono and H. Schulzrinne, "Have i met you before? using Cross-Media relations to reduce SPIT," Tech. Rep. cucs-020-09, Columbia University, Apr. 2009.

[24] S.-G. Hong, S. Srinivasan, and H. Schulzrinne, "Measurements of multicast service discovery in a campus wireless network," Tech. Rep. cucs-050-08, Columbia University, Nov. 2008.

[25] S. Subramanya, X. Wu, and H. Schulzrinne, "VoIP-based air traffic controller training," Tech. Rep. cucs-043-08, Columbia University, Sept. 2008.

[26] S. Shin and H. Schulzrinne, "Towards the quality of service for VoIP traffic in IEEE 802.11 wireless networks," Tech. Rep. cucs-035-08, Columbia University, July 2008.

[27] C. Shen, H. Schulzrinne, and E. Nahum, "SIP server overload control: Design and evaluation," Tech. Rep. cucs-031-08, Columbia University, June 2008.

[28] A. Forte, S. Shin, and H. Schulzrinne, "IEEE 802.11 in the large: Observations at an IETF meeting," Tech. Rep. cucs-025-08, Columbia University, May 2008.

[29] E. Brosh, S. Baset, V. Misra, D. Rubenstein, and H. Schulzrinne, "The Delay-Friendliness of TCP," Tech. Rep. cucs-014-08, Columbia University, Mar. 2008.

[30] S. Abdul Baset, E. Brosh, V. Misra, D. Rubenstein, and H. Schulzrinne, "The Delay-Friendliness of TCP," Tech. Rep. cucs-023-07, Columbia University, June 2007.

[31] K. Ono and H. Schulzrinne, "The impact of SCTP on server scalability and performance," Tech. Rep. cucs-012-08, Columbia University, Feb. 2008.

[32] K. Ono and H. Schulzrinne, "One server per city: Using TCP for very large SIP servers," Tech. Rep. cucs-009-08, Columbia University, Feb. 2008.

[33] K. Arabshian, C. Dickmann, and H. Schulzrinne, "Service composition in a global service discovery system," Tech. Rep. cucs-033-07, Columbia University,, Sept. 2007.

[34] S. Hong, S. Srinivasan, and H. Schulzrinne, "Accelerating service discovery in Ad-Hoc zero configuration networking," Technical Report cucs-009-07, Columbia University, New York, Feb. 2007.

[35] A. Forte and H. Schulzrinne, "Cooperation between stations in wireless networks," arXiv report cs.NI/0701046, arXiv, Jan. 2007.

[36] K. Arabshian and H. Schulzrinne, "Combining ontology queries with text search in service discovery," Tech. Rep. cucs-006-07, Columbia University, New York, NY, Jan. 2007.

[37] O. Boyaci and H. Schulzrinne, "Measurements of DNS stability," Tech. Rep. cucs-045-06, Columbia University, New York, Dec. 2006.

[38] A. Forte, S. Shin, and H. Schulzrinne, "IEEE 802.11 in the large: Observations at an IETF meeting," tech. rep., Columbia University, Dec. 2006.

[39] A. Forte and H. Schulzrinne, "Cooperation between stations in wireless networks," Tech. Rep. cucs-044-06, Columbia University, New York, Dec. 2006.

[40] V. Singh, H. Schulzrinne, M. Isomaki, and P. Boni, "Presence traffic optimization techniques," Tech. Rep. cucs-041-06, Columbia University, New York, Nov. 2006.

[41] C. Shen and H. Schulzrinne, "A VoIP privacy mechanism and its application in VoIP peering for voice service provider topology and identity hiding," Tech. Rep. cucs-039-06, Columbia University, New York, Oct. 2006.

[42] S. Baset and H. Schulzrinne, "A common protocol for implementing various DHT algorithms," Tech. Rep. cucs-040-06, Columbia University, New York, Oct. 2006.

[43] C. Shen and H. Schulzrinne, "Measurement and evaluation of ENUM server performance," Tech. Rep. cucs-029-06, Columbia University, New York, Sept. 2006.

[44] S. Shin, A. Forte, and H. Schulzrinne, "Seamless layer-2 handoff using two radios in IEEE 802.11 wireless networks," Tech. Rep. cucs-018-06, Columbia University, Computer Science Department, Apr. 2006.

[45] A. Forte, S. Shin, and H. Schulzrinne, "Passive duplicate address detection for dynamic host configuration protocol (DHCP)," Tech. Rep. cucs-011-06, Columbia University, Computer Science Department, Mar. 2006.

[46] K. Singh and H. Schulzrinne, "Using an external DHT as a SIP location service," Technical Report CUCS-007-06, Columbia University, Computer Science Department, New York, NY, Feb. 2006.

[47] V. Singh and H. Schulzrinne, "A survey of security issues and solutions in presence," Tech. Rep. cucs-019-06, Columbia University, New York, Feb. 2006.

[48] V. Singh and H. Schulzrinne, "SIMPLEstone - benchmarking presence server performance," Tech. Rep. cucs-023-06, Columbia University, New York, Feb. 2006.

[49] M. Cristofano, A. Forte, and H. Schulzrinne, "Generic models for mobility management in next generation networks," Tech. Rep. cucs-031-05, Columbia University, Computer Science Department, Aug. 2005.

[50] K. Arabshian and H. Schulzrinne, "Hybrid hierarchical and Peer-to-Peer ontology-based global service discovery system," Tech. Rep. CUCS-016-05, Columbia University, Apr. 2005.

[51] C. Shen, H. Schulzrinne, S.-H. Lee, and J. Bang, "Internet routing dynamics and NSIS related considerations," Technical Report CUCS-007-05, Columbia University, New York, Feb. 2005.

[52] R. Shacham, H. Schulzrinne, S. Thakolsri, and W. Kellerer, "The virtual device: Expanding wireless communication services through service discovery and session mobility," Technical Report CUCS-001-05, Department of Computer Science, Columbia University, New York, NY, Jan. 2005.

[53] X. Wu and H. Schulzrinne, "End system service examples," Tech. Rep. CUCS-048-04, Columbia University Department of Computer Science, New York, New York, Dec. 2004.

[54] S. Baset and H. Schulzrinne, "An analysis of the Skype Peer-to-Peer internet telephony protocol," arXiv report cs.NI/0412017, arXiv, Dec. 2004. CUCS-039-04.

[55] K. Srivastava and H. Schulzrinne, "Preventing spam for SIP-based instant messages and sessions," Technical Report CUCS-042-04, Department of Computer Science, Columbia University, New York, NY, Oct. 2004.

[56] K. Singh and H. Schulzrinne, "Peer-to-Peer internet telephony using SIP," Tech. Rep. CUCS-044-04, Department of Computer Science, Columbia University, New York, NY, Oct. 2004.

[57] X. Wu and H. Schulzrinne, "Service learning in internet telephony," technical report, Department of Computer Science, Columbia University, Oct. 2004.

[58] X. Zhang and H. Schulzrinne, "Voice over TCP and UDP," Technical Report CUCS-033-04, Columbia University Department of Computer Science, Sept. 2004.

[59] K. Singh and H. Schulzrinne, "Failover and load sharing in SIP telephony," Tech. Rep. CUCS-011-04, Columbia University, Computer Science Department, New York, NY, USA, Mar. 2004.

[60] X. Wu and H. Schulzrinne, "Feature interactions in internet telephony end systems," tech. rep., Department of Computer Science, Columbia University, Jan. 2004.

[61] H. Schulzrinne, "9-1-1 calls for voice-over-ip," Ex-parte filing to the Federal Communications Commission cucs-022-03, Department of Computer Science, Columbia University, New York, New York, Aug. 2003.

[62] C. Wieser, M. Laakso, and H. Schulzrinne, "Security testing of SIP implementations," Technical Report CUCS-024-03, Department of Computer Science, Columbia University, New York, Aug. 2003.

[63] K. Singh, X. Wu, J. Lennox, and H. Schulzrinne, "Comprehensive multi-platform collaboration," Tech. Rep. CUCS-027-03, Dept. of Computer Science, Columbia University, New York, New York, Dec. 2003.

[64] K. Singh, W. Jiang, J. Lennox, S. Narayanan, and H. Schulzrinne, "CINEMA: columbia internet extensible multimedia architecture," technical report CUCS-011-02, Department of Computer Science, Columbia University, New York, New York, May 2002.

[65] H. Schulzrinne and K. Arabshian, "Providing emergency services in Internet telephony," technical report, Department of Computer Science, Columbia University, New York, NY, Apr. 2002.

[66] P. Mendes, H. Schulzrinne, and E. Monteiro, "Session-aware popularity-based resource allocation across several differentiated service domains," Technical Report CUCS-009-02, Columbia University, Apr. 2002.

[67] H. Schulzrinne, S. Narayanan, J. Lennox, and M. Doyle, "SIPstone - benchmarking SIP server performance," Technical Report CUCS-005-02, Department of Computer Science, Columbia University, New York, New York, Mar. 2002.

[68] W. Zhao and H. Schulzrinne, "A flexible and efficient protocol for multi-scope service registry replication," Tech. Rep. CUCS-016-02, Dept. of Computer Science, Columbia University, New York, New York, Mar. 2002.

[69] G. Camarillo, H. Schulzrinne, and R. Kantola, "Signalling transport protocols," Technical report CUCS-002-02, Dept. of Computer Science, Columbia University, New York, Feb. 2002.

[70] M. Papadopouli and H. Schulzrinne, "Performance of data dissemination and message relaying in mobile ad hoc networks," Technical Report CUCS-004-02, Dept. of Computer Science, Columbia University, New York, New York, Feb. 2002.

[71] S. Krishnan and H. Schulzrinne, "On buffered clos switches," Tech. Rep. CUCS-023-02, Dept. of Computer Science, Columbia University, New York, New York, Nov. 2002.

[72] P. Mendes, H. Schulzrinne, and E. Monteiro, "Multi-layer utilization maximal fairness for multi-rate multimedia sessions," Technical Report CUCS-008-01, Dept. of Computer Science, Columbia University, New York, New York, July 2001.

[73] M. Papadopouli and H. Schulzrinne, "Performance of data dissemination among mobile devices," technical report CUCS-005-01, Dept. of Computer Science, Columbia University, New York, New York, July 2001.

[74] P. Pan and H. Schulzrinne, "PF_IPOPTION: a kernel extension for IP option packet processing," Technical Memorandum 10009669-02TM, Bell Labs, Lucent Technologies, Murray Hill, NJ, June 2000.

[75] P. Pan and H. Schulzrinne, "Lightweight resource reservation signaling: Design, performance and implementation," Technical Memorandum 10009669-03TM, Bell Labs, Lucent Technologies, Murray Hill, NJ, June 2000.

[76] D. Rubenstein, J. Lennox, J. Rosenberg, and H. Schulzrinne, "Bell labs/columbia/umass RTP library internal function descriptions," Tech. Rep. 99-76, University of Massachusetts, Amherst, Massachusetts, Nov. 1999.

[77] W. Jiang and H. Schulzrinne, "QoS measurement of Internet real-time multimedia services," Technical Report CUCS-015-99, Columbia University, New York, New York, Dec. 1999.

[78] J. Rosenberg, J. Lennox, and H. Schulzrinne, "Programming Internet telephony services," Technical Report CUCS-010-99, Columbia University, New York, New York, Mar. 1999.

[79] J. Lennox, H. Schulzrinne, and T. L. Porta, "Implementing intelligent network services with the session initiation protocol," Technical Report CUCS-002-99, Columbia University, New York, New York, Jan. 1999.

[80] H. Schulzrinne and J. Rosenberg, "Signaling for Internet telephony," Technical Report CUCS-005-98, Columbia University, New York, New York, Feb. 1998.

[81] H. Schulzrinne, B. Deffner, D. Sisalem, and T. Friedman, "Architecture of a teleteaching application for testing resource reservation and adaptive applications in integrated networks," Project Report MMTng M-1, GMD Fokus, Berlin, Germany, Nov. 1995.

[82] I. Busse, B. Deffner, D. Cochrane, B. Gorman, H. Schulzrinne, P. Demestichas, Y. Manolessos, and K. Kassapakis, "Dynamic QoS management framework for IBC networks (D12)," Deliverable R2116/CRAY/WP2/DS/R/, RACE Project 2116 (TOMQAT), Nov. 1995.

[83] I. Busse, B. Deffner, H. Schulzrinne, P. Demestichas, Y. Manolessos, K. Kassapakis, G. D. Stamoulis, and G. Seehase, "TOMQAT test system user manual (D11)," Deliverable R2116/TELMAT/WP3/DS/, RACE Project 2116 (TOMQAT), Sept. 1995.

[84] I. Busse, B. Deffner, H. Schulzrinne, P. Demestichas, Y. Manolessos, K. Kassapakis, G. D. Stamoulis, and G. Seehase, "Preliminary test report and QoS verification document (D9)," Deliverable R2116/TUB/WP3/DS/P/0, RACE Project 2116 (TOMQAT), Aug. 1995.

[85] I. Busse, B. Deffner, H. Schulzrinne, P. Demestichas, Y. Manolessos, K. Kassapakis, G. D. Stamoulis, and G. Seehase, "Definition of conceptual framework for QoS management (D8)," Deliverable R2116/NTUA/WP2/DS/P/, RACE Project 2116 (TOMQAT), Feb. 1995.

[86] I. Busse, D. Cochrane, B. Deffner, P. Demestichas, B. Evans, W. Grupp, N. Karatzas, and K. Kassapakis, "Quality module specification (D7)," Deliverable R2116/ISR/WP2/DS/S/0, RACE Project 2116 (TOMQAT), Dec. 1994.

[87] H. Almus, H. Buschermoehle, I. Busse, B. Deffner, P. H. Georgatsos, W. Grupp, N. Karatzas, and K. Kassapaskis, "Architecture of the TOMQAT system and definition of net infrastructure (D6)," Deliverable R2116/TUB/WP2/DS/P/0, RACE Project 2116 (TOMQAT), Aug. 1994.

[88] D. Cochrane, P. Demestichas, A. Gehring, P. H. Georgatsos, J. Kawalek, N. Karatzas, K. Kassapakis, and P. Legand, "Requirement analysis and approach to dynamic total quality management (D5)," Deliverable R2116/ICOM/WP2/DS/P/, RACE Project 2116 (TOMQAT), Aug. 1994.

[89] A. Gehring, J. Kuwalek, P. Legand, Z. Lioupas, Y. Manolessos, K. Nagel, E. Papachristou, and I. Schieferdecker, "Requirement analysis and approach for dynamic total quality management (D4)," Deliverable R2116/ICOM/WP2/DSR/0, RACE Project 2116 (TOMQAT), June 1994.

[90] H. Almus, H. Buschermöhle, I. Busse, P. H. Georgatsos, W. Grupp, K. Kassapakis, P. Legand, and Z. Lioupas, "Architecture of the TOMQAT system and definition of net infrastructure (D3)," Deliverable R2116/GMD/WP2/DS/P/0, RACE Project 2116 (TOMQAT), May 1994.

[91] L. Kleinrock, J. P. Sterbenz, N. F. Maxemchuk, S. S. Lam, H. Schulzrinne, and P. Steenkiste, "The national exchange for networked information systems: a white paper," Technical Report CSD-930039, University of California (UCLA), Los Angeles, California, Nov. 1993.

[92] H. Schulzrinne, "Issues in designing a transport protocol for audio and video conferences and other multiparticipant real-time applications." expired Internet draft, Oct. 1993.

[93] A. M. Lapone, N. Maxemchuk, and H. Schulzrinne, "The bell laboratories network emulator," Technical Memorandum BL0113820-930913-64T, AT&T Bell Laboratories, Murray Hill, New Jersey, Sept. 1993.

[94] H. Schulzrinne, *Reducing and characterizing packet loss for high-speed computer networks with real-time services*. PhD thesis, University of Massachusetts, Amherst,

Massachusetts, May 1993. also: Technical Report 93-54, Department of Computer Science, University of Massachusetts at Amherst.

[95] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "Loss correlation for queues with single and multiple input streams," Technical Report TR 92-53, Department of Computer Science, University of Massachusetts, Amherst, Massachusetts, July 1992.

[96] H. Schulzrinne, "Voice communication across the internet: A network voice terminal," Technical Report TR 92-50, Dept. of Computer Science, University of Massachusetts, Amherst, Massachusetts, July 1992.

[97] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "Distribution of the loss period for some queues in continuous and discrete time," Technical Report TR 91-03, Department of Computer and Information Science, University of Massachusetts, Amherst, Massachusetts, July 1991.

[98] H. Schulzrinne, J. F. Kurose, and D. F. Towsley, "Congestion control for real-time traffic in high-speed networks," Technical Report TR 89-92, Department of Computer and Information Science, University of Massachusetts, Amherst, Massachusetts, Mar. 1991.

[99] H. Schulzrinne, "SIMUL simulation system manual." internal memorandum, Feb. 1989.

[100] H. Schulz-Rinne, "Multistage vector quantization for speech and image waveform coding; the DSP workbench: Distributed multiprocess system simulation," Master's thesis, University of Cincinnati, Cincinnati, Ohio, Aug. 1987.

MASTERS THESES SUPERVISED

[1] R. Bollow, "Video transmission using the available bit rate service," Master's thesis, Berlin University of Technology, Berlin, Germany, Jan. 1997.

[2] C. Zahl, "Aufbau und konfiguration von internet-multimedia-konferenzen über verbindungen niedriger bandbreite (setup and configuration of Internet multimedia conferences using low-bandwidth links)," Master's thesis, Berlin University of Technology, Berlin, Germany, Feb. 1997. Diplomarbeit.

[3] F. Oertel, "Integration von ISDN-Teilnehmern in internet-multimedia-konferenzen (integration of ISDN subscribers into Internet multimedia conferences)," Master's thesis, Berlin University of Technology, Berlin, Germany, Feb. 1997. Diplomarbeit.

[4] C. Zahl, "Entwicklung einer internet-multimedia-telekommunikations-anlage (development of an Internet multimedia telecommunications system)," Studienarbeit, Department of Communication Networks, TU Berlin, Berlin, Germany, Nov. 1995.

[5] F. Oertel, "Aufbau und konfiguration lokaler multimedia konferenz-umgebungen (setup and configuration of local multimedia conferencing environments)," Studienarbeit, Department of Communication Networks, TU Berlin, Berlin, Germany, Nov. 1995.

[6] C. Sieckmeyer, "Bewertung von adaptiven ausspielalgorithmen für paketvermittelte audiodaten (evaluation of adaptive playout algorithms for packet audio)," Studienarbeit, Dept. of Electrical Engineering, TU Berlin, Berlin, Germany, Oct. 1995.

[7] B. Rathke, "Evaluation of a distance-vector based multicast-routing protocol for datagram internetworks," Diplomarbeit, Department of Telecommunications, TU Berlin, Berlin, Germany, Oct. 1995.

[8] I. Demirel, "Eine SDL-Spezifikation des core based tree (CBT) multicast-routing-protokolls (an SDL specification of the core-based tree (CBT) multicast routing protocol)," Studienarbeit, Dept. of Electrical Engineering, TU Berlin, Berlin, Germany, Sept. 1995.

[9] D. Sisalem, "Rate based congestion control and its effects on TCP over ATM," Diplomarbeit, School of Engineering, TU Berlin, Berlin, June 1995.

[10] S. Portner, "Verbindungsverwaltung in hochgeschwindigkeitsnetzen (connection management in high speed networks)," Studienarbeit, Institut für Fernmeldetechnik, TU Berlin, Berlin, Germany, Dec. 1994.

PHD THESES SUPERVISED

Jonathan Rosenberg, Xin Wang, Maria Papadopouli, Ping Pan, Wenyu Jiang, Lisa Amini, Jonathan Lennox, Kundan Singh, Santosh Krishnan, Weibin Zhao (2006), Xiaotao Wu (2007), Sangho Shin (2008), Knarig Arabshian (2008), Charles Shen (2010), Ashutosh Dutta (2010), Salman Baset (2010), Omer Boyaci (2011), Se Gi Hong (2011), Arezu Moghadam (2011), Jae Woo Lee (2012), Kumiko Ono (2012), Wonsang Song (2014), Jong Yul Kim (2015), Hyunwoo Nam (2015), Suman Srinivasan (2016), Kyung-Hwa Kim (2017).

CURRENT PHD STUDENTS

Jan Janak.

NON-US THESIS COMMITTEES

Ralf Ackermann (Technische Universität Darmstadt, July 2003), Paulo Mendes (University of Coimbra, Portugal, January 2004), Cristian Hesselman (University of Twente, Holland, May 2005), Martin Krebs (RWTH Aachen University, May 2010), Ian Marsh (KTH, Sweden, June 2009), Tommy Ou (University of Oulu, Finland, August 2010), Antti Mäkelä (Aalto University, Finland, August 2012), Erkki Harjula (University of Oulu, Finland, June 2016).

November 10, 2018

**DECLARATION OF DR. HENNING G. SCHULZRINNE**
***WIKIMEDIA FOUND. V. NSA*, NO. 1:15-CV-00662-TSE (D. MD.)**

# EXHIBIT B

**DOCUMENTS PROVIDED BY DEPARTMENT OF JUSTICE**
**FOR CONSIDERATION IN PREPARATION OF DECLARATION**

1. NSA Director of Civil Liberties and Privacy Office Report, NSA's Implementation of FISA Section 702 (Apr. 16, 2014), https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/nsa_report_on_section_702_program.pdf.

2. Privacy & Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf

3. Office of the Director of National Intelligence, Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act

4. The National Security Agency: Missions, Authorities, Oversight and Partnerships (Aug. 9, 2013), https://fas.org/irp/nsa/nsa-story.pdf

5. The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act (attachment to https://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf)

6. *Wikimedia Found. v. NSA*, 143 F. Supp. 3d 344 (D. Md. 2015)

7. *Wikimedia Found. v. NSA*, 857 F.3d 193 (4th Cir. 2017)

8. Declaration of Robert T. Lee, ECF No. 77-3, *Wikimedia Found. v. NSA*, No. 1:15-cv-00662-TSE (D. Md.)

9. [*Redacted Caption*], Memorandum Opinion and Order (F.I.S.C. Apr. 26, 2017) (public redacted version), https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf

10. [*Redacted Caption*], 2011 WL 10945618 (F.I.S.C. Oct. 3, 2011) (public redacted version)

11. Wikimedia Foundation Inc.'s Responses and Objections to National Security Agency's First Set of Interrogatories (Jan. 11, 2018)

12. Wikimedia Foundation Inc.'s Responses and Objections to United States Department of Justice's First Set of Interrogatories (Jan. 11, 2018)

13. Wikimedia Foundation Inc.'s Responses and Objections to the Office of the Director of National Intelligence's First Set of Interrogatories (Jan. 11, 2018)

14. Documents produced in discovery by Plaintiff Wikimedia Foundation, beginning with Bates-stamp nos.: WIKI0001412, 1458, 1474, 1545, 1950, 1956, 1957, 1960, 2097, 2301, 2316, 2344, 2358, 2429, 2459, 2479, 2483, 5174, 5466, 5500, 5577, 5693, 5832, 5978, 6363, 6505, 6508, 6536, 6543, 6564, 6662, 6700, 6836, 6872, 7093, 7108, 7115, 7347, 7351, 7382, 8108, 9269

15. Exhibit 1 to Wikimedia Foundation, Inc.'s Amended Responses and Objections to Office of the Director of National Intelligence's Interrogatory No. 19 (Apr. 6, 2018), and Exhibits A-G thereto

16. Deposition of Michelle S. Paulson (Apr. 13, 2018)

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE |

# Attachment D

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE<br><br>[redacted] |

# EXHIBIT 2



USCA4 Appeal: 20-1191 Doc: 18-1 Filed: 07/01/2020 Pg: 829 of 931

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | No. 1:15-cv-0662 (TSE)<br><br>~~FILED UNDER SEAL~~ |

Declaration of James J. Gilligan

Pursuant to 28 U.S.C. § 1746, I, James J. Gilligan, hereby declare:

1. I am an attorney in the United States Department of Justice, Civil Division, Federal Programs Branch. I serve as lead counsel for the Government Defendants in the above-captioned case. The statements made herein are based on my personal knowledge, and on information made available to me in the course of my duties and responsibilities as Government counsel in this case.

2. I submit this declaration in support of the Defendants' concurrently-filed motion for summary judgment.

3. Filed as Exhibits 3-5 attached to the Defendants' motion for summary judgment are true and correct copies of the following documents:

| Exhibit No. | Exhibit Name |
|---|---|
| 3 | Wikimedia Foundation, Inc.'s Amended and Supplemental Responses and Objections to NSA's First Set of Interrogatories, dated March 23, 2018 |
| 4 | Wikimedia Foundation, Inc.'s Amended Responses and Objections to ODNI's Interrogatory No. 19, dated April 6, 2018, including Exhibit 1, "Technical Statistics Chart" |
| 5 | Wikimedia Foundation, Inc.'s Responses and Objections to NSA's First Set of Interrogatories, dated January 11, 2018 |



USCA4 Appeal: 20-1191 Doc: 18-1 Filed: 07/01/2020 Pg: 830 of 931

I declare under penalty of perjury that the foregoing is true and correct. Executed in Washington, D.C., this 13th day of November, 2018.

JAMES J. GILLIGAN
Special Litigation Counsel
United States Department of Justice
Civil Division, Federal Programs Branch



USCA4 Appeal: 20-1191 Doc: 18-1 Filed: 07/01/2020 Pg: 831 of 931

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE |

# Attachment E

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE<br><br>~~FILED UNDER SEAL~~ |

# EXHIBIT 3

**IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND**

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

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

**PROPOUNDING PARTY:** NATIONAL SECURITY AGENCY

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

**SET NUMBER:** ONE

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

## I. GENERAL RESPONSES.

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

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

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

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

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

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

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

## II. GENERAL OBJECTIONS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## III. DEFINITIONAL OBJECTIONS.

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

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

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

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

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

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

## IV. INSTRUCTIONAL OBJECTIONS

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

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

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

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

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

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

## V. SPECIFIC OBJECTIONS AND RESPONSES TO INTERROGATORIES.

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

**INTERROGATORY NO. 2:**

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

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

**RESPONSE TO INTERROGATORY NO. 2:**

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

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

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

The bases for Plaintiff's contention include the following:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 2:**

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

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

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

**INTERROGATORY NO. 3:**

Please identify each category of Wikimedia international, text-based, Internet communications that Plaintiff contends, for purposes of establishing jurisdiction, is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, including but not limited to, user visits to Wikimedia sites; contributions and edits to Wikimedia websites;

Wikimedia discussion forums; Wikimedia discussion pages; e mail sent via Wikimedia among registered users; communications "over wikis" among small or limited groups of users; mailing lists with restricted membership; other use of Wikimedia Projects, websites, and webpages by "community members" to interact with one another; internal log communications; "Community Consultations;" solicitations of user input and preferences; and other communications sent and received by Wikimedia staff in carrying out Wikimedia's work. *See* Amended Complaint ¶¶ 79, 84, 86, 92, 93, 102.

**RESPONSE TO INTERROGATORY NO. 3:**

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows. As explained in Wikimedia's First Amended Complaint, Wikimedia contends that Upstream surveillance implicates at least three categories of communications (Am. Compl. ¶ 86): (1) Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other. Examples of these communications include, but are not limited to, page views to Wikimedia websites, edits and contributions to Wikimedia websites, emails between registered Wikimedia users and emails on Wikimedia's mailing lists.

(2) Wikimedia's internal log communications.

(3) Electronic communications of Wikimedia staff. Examples of these communications include, but are not limited to, Gmail, Google chat, Internet Relay Chat, and Slack. Additionally, Wikimedia staff members use a variety of third-party tools to conduct their work, including, but

not limited to, Google Apps/G Suite, Trello, Sugar, Qualtrics, User Testing and Salesforce.

**SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 3:**

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

As stated above, Wikimedia contends that Upstream surveillance implicates at least three categories of communications (Am. Compl. ¶ 86). The first category involves Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other. Examples of these communications include, but are not limited to, page views to Wikimedia websites, edits and contributions to Wikimedia websites, private and semi-private "wikis" that only certain users can read or edit, questions, comments, or complaints that community members submit to Wikimedia about the performance and operation of its websites, private deliberations of user-community leaders who help administer the Wikimedia websites, emails between registered Wikimedia users, and emails on Wikimedia's mailing lists.

**INTERROGATORY NO. 5:**

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify the Internet circuits entering or exiting the United States that have carried that category of communication in the past 24 months. To identify a circuit means to state its location of entry to or exit from the United States, to state its country (or, if unknown, global region(s)) of origin or termination abroad, and to identify the person(s) owning or controlling it.

**RESPONSE TO INTERROGATORY NO. 5:**

In addition to the General Objections above which are incorporated herein, Plaintiff also objects that this Interrogatory is overbroad and unduly burdensome. Plaintiff further objects that this Interrogatory seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff further objects that this Interrogatory seeks information that is within Defendants' control.

Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

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

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

**SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 5:**

Subject to and without waiving any of these General or Specific Objections and reserving the right to further supplement as discovery in this case continues, Plaintiff supplements its response as follows: As Wikimedia exchanges more than one trillion communications each year with users scattered across the global network, its communications are routed across virtually every major circuit carrying public Internet traffic between the United States and the rest of the world.

**INTERROGATORY NO. 6:**

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied,

and reviewed by the NSA in the course of Upstream surveillance, please identify each foreign country to or from which such Wikimedia communications were sent in the past 24 months.

**RESPONSE TO INTERROGATORY NO. 6:**

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

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

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

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

**(3) Electronic communications of Wikimedia staff.** Between January 1, 2015 and

December 12, 2017, Wikimedia's office network router located in the United States sent Internet communications to at least approximately 221 non-U.S. countries, territories and regions.

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

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

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

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

**AMENDED RESPONSE TO INTERROGATORY NO. 6:**

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

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

in the United States.

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

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

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

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

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

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

**INTERROGATORY NO. 7:**

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

**RESPONSE TO INTERROGATORY NO. 7:**

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

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

**(1) Wikimedia communications with its community members.** Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received over 500 billion HTTPS requests from users outside of the United States. Each HTTPS request generates a corresponding response: thus Wikimedia exchanged over 1 trillion HTTPS requests and responses with its users between April 23, 2017 and December 31, 2017. These figures are estimates that were derived

using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

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

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

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

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

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

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

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

**AMENDED RESPONSE TO INTERROGATORY NO. 7:**

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

**(1) Wikimedia communications with its community members.** Between April 23, 2017 and December 31, 2017, Wikimedia's U.S. servers received approximately over 511 billion HTTP/S requests from users outside of the United States. Each HTTP/S request generates a corresponding response; thus Wikimedia exchanged over 1 trillion HTTP/S requests and responses with its users between April 23, 2017 and December 31, 2017.

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

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

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

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

This figure represents the total number of Internet outbound connections sent via the

following Internet protocols: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

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

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

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

**INTERROGATORY NO. 8:**

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

**RESPONSE TO INTERROGATORY NO. 8:**

In addition to the General Objections above which are incorporated herein, Plaintiff

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

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

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

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

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

regions. A list of the numbers of these communications broken down by country, territory, or region will be produced to Defendants.

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

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

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

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

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

**AMENDED RESPONSE TO INTERROGATORY NO. 8:**

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

**(1) Wikimedia communications with its community members.** The number of HTTP/S requests that Wikimedia's U.S. servers received from users in each country, territory, or

region between April 23, 2017 and December 31, 2017 is attached as Amended Exhibit B. Each HTTP/S request generates a corresponding response that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTP/S request transmitted to Wikimedia's servers in the United States.

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

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

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

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

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

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

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

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

**INTERROGATORY NO. 11:**

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

**RESPONSE TO INTERROGATORY NO. 11:**

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

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

users around the world. Wikimedia publishes current monthly page view statistics by country (*available* at https://stats.wikimedia.org/wikimedia/squids/SquidReportPageViewsPerCountryOverview.htm), and maintains an archive with analogous data for past months (*available* at https://stats.wikimedia.org/archive/squid_reports/).

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

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

**SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 11:**

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

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

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

Wikimedia contractors); WIKI0002407 (listing 288 Wikipedia language editions); WIKI0002416 (listing Wikimedia movement affiliates); WIKI0006369 (listing page views for virtually every country on earth); WIKI0002360, WIKI0002365, WIKI0002367, WIKI0002389, WIKI0002396 (noting countries involved in user grants and scholarships); WIKI0006295 (listing funded grants by country).

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

**INTERROGATORY NO. 13:**

Please identify each of the international Internet "backbone chokepoints," whether cables, circuits, or other communications facilities, at which Plaintiff contends, in paragraph 66 of the Amended Complaint, the NSA must be conducting Upstream surveillance, stating for each such "backbone chokepoint" the basis of Plaintiff's contention.

**RESPONSE TO INTERROGATORY NO. 13:**

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff also objects that this Interrogatory seeks information that is within Defendants' control. Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

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

An NSA document states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *See* NSA Staff Processing Form, Subject: SSO's Support to the

FBI for Implementation of their Cyber FISA Orders.

The "chokepoints" at which the NSA conducts Upstream surveillance have included the "seven access sites" identified in an NSA document, reproduced at paragraph 68 of Plaintiff's First Amended Complaint (ECF No. 70-1).

Additional reporting after the filing of the Amended Complaint states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. *See* Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents, one of which describes the surveillance of hundreds of circuits at a specific AT&T trans-Pacific cable site); Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents); Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents) (describing surveillance on AT&T's network, including on "OC-192 and 10GE peering circuits"; describing surveillance on Verizon's network, including at a cable-landing site called BRECKENRIDGE).

**SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 13:**

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

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

**INTERROGATORY NO. 15:**

Please state the basis of Plaintiff's contentions regarding the manner in which the alleged

copying, filtering, and content-review processes referred to in paragraph 49 of the Amended Complaint are carried out.

**RESPONSE TO INTERROGATORY NO. 15:**

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

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

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

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

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

Additionally, Upstream surveillance involves the retention of communications that contain targeted selectors. To retain a communication in transit, an eavesdropper must copy and reassemble the packets constituting the communication. But because an eavesdropper cannot

know in advance which packets in transit are part of a communication containing a targeted selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

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

Other bases of Plaintiff's contentions include:

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

- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)
- Charlie Savage, *Power Wars* (2015)

**SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 15:**

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

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

**INTERROGATORY NO. 21:**

To the extent not already stated or identified in response to Interrogatory Nos. 13-20, above, or in response to Defendant United States Department of Justice's First Set of Interrogatories, Interrogatory Nos. 1-6, please state the basis of Plaintiff's contention that the NSA is intercepting, copying, and reviewing at least some of its communications.

**RESPONSE TO INTERROGATORY NO. 21:**

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff also objects that this Interrogatory seeks information that is the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff also objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants.

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

Plaintiff's contention is based on the volume and distribution of its communications, basic principles governing the routing and transmission of Internet communications, and basic principles governing how surveillance on a packet-switched network operates.

**SUPPLEMENTAL RESPONSE TO INTERROGATORY NO. 21:**

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

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

- Exhibits A–F to Plaintiff's First Set of Requests for Admission
- WIKI0008024 (slide deck from which Exhibit B to Plaintiff's First Set of Requests for Admission was excerpted, entitled "XKEYSCORE for Counter-CNE")
- Glenn Greenwald, *Xkeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, The Guardian, July 31, 2013 (and associated documents).
- Barton Gellman, Julie Tate, & Ashkan Soltani, *In NSA-intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post, July 5, 2014.

Dated: March 23, 2018

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

*Counsel for Plaintiff Wikimedia Foundation, Inc.*

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE |

# Attachment F

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE<br><br>~~FILED UNDER SEAL~~ |

# EXHIBIT 4

**IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND**

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

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

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

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

**SET NUMBER:** **THREE**

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

## I. GENERAL RESPONSES.

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

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

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

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

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

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

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

## II. GENERAL OBJECTIONS.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## III. DEFINITIONAL OBJECTIONS.

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

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

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

## IV. INSTRUCTIONAL OBJECTIONS

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

agents, and employees.

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

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

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

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

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

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

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

**INTERROGATORY NO. 19:**

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

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

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

**RESPONSE TO INTERROGATORY NO. 19:**

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

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

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

**AMENDED RESPONSE TO INTERROGATORY NO. 19:**

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

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

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

Dated: April 6, 2018

/s/ Ashley Gorski

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

*Counsel for Plaintiff*

# EXHIBIT 1

USCA4 Appeal: 20-1191 Doc: 18-1 Filed: 07/01/2020 Pg: 886 of 931

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



[redacted]

[redacted]

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





USCA4 Appeal: 20-1191 Doc: 18-1 Filed: 07/01/2020 Pg: 887 of 931

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE |

# Attachment G

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| WIKIMEDIA FOUNDATION,<br><br>Plaintiff,<br><br>v.<br><br>NATIONAL SECURITY AGENCY, *et al.*,<br><br>Defendants. | Civil Action No. 1:15-cv-00662-TSE<br><br>~~FILED UNDER SEAL~~ |

# EXHIBIT 5

**IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND**

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

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

**PROPOUNDING PARTY:** **NATIONAL SECURITY AGENCY**

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

**SET NUMBER:** **ONE**

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

## I. GENERAL RESPONSES.

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

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

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

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

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

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

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

## II. GENERAL OBJECTIONS.

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

response to each Interrogatory, to each instruction, definition, and Interrogatory made in Defendant's Interrogatories:

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

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

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

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

**5.** Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information that is available through or from public sources or records, or that are otherwise equally available to Defendant, on the ground that such instructions, definitions, and/or Interrogatories unreasonably subject Plaintiff to undue annoyance,

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

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

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

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

**9.** Plaintiff objects to the Interrogatories in their entirety to the extent any such instruction, definition, or Interrogatory seeks information or production of documents protected from disclosure by any right to privacy or any other applicable privilege or protection, including the right to confidentiality or privacy of third parties, any right of confidentiality provided for by Plaintiff's contracts or agreements with such third parties, or by Plaintiff's obligations under

applicable law or contract to protect such confidential information. Plaintiff reserves the right to withhold any responsive information or documents governed by a third-party confidentiality agreement until such time as the appropriate notice can be given or the appropriate permissions can be obtained. Plaintiff also objects generally to all instructions, definitions, or Interrogatories to the extent they seek disclosure of trade secrets and other confidential research or analyses, development, or commercial information of Plaintiff or any third party.

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

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

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

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

## III. DEFINITIONAL OBJECTIONS.

**1.** Plaintiff objects to definition number one (1) to the extent it defines "Plaintiff" and "Wikimedia" to include Plaintiff's "parent, subsidiary, and affiliated organizations, and all persons

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

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

**3.** Plaintiff objects to definition number five (5) as unduly burdensome in that it purports to require Plaintiff to "identify" each "natural person" by providing information including "her most current home and business addresses, telephone numbers, and e-mail addresses, the name of her current employer, and her title."

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

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

## IV. INSTRUCTIONAL OBJECTIONS

**1.** Plaintiff objects to instruction number one (1) to the extent it purports to request "knowledge or information" from Wikimedia's "parent, subsidiary, or affiliated organizations, and their officials, agents, employees, attorneys, consultants, and any other person acting on their behalf." Said request is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, seeks information outside Plaintiff's possession, custody, or control, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden and

expense. Moreover, said request is vague and ambiguous in that it cannot be determined what is meant by the term "affiliated organizations" and "any other person acting on their behalf." Where an Interrogatory requests knowledge or information of Plaintiff, Plaintiff shall construe such request to mean knowledge or information from Wikimedia, and its present officers, directors, agents, and employees.

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

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

**4.** Plaintiff objects to instruction number five (5) to the extent it defines "the time period for which each interrogatory seeks a response" as "the period from July 10, 2008 (the date of enactment of the FISA Amendments Act of 2008, Pub. L. 110-261, 121 Stat. 522) until the date

of Plaintiff's response." This definition is overly broad, seeks irrelevant information not calculated to lead to the discovery of admissible evidence, and would subject Plaintiff to unreasonable and undue annoyance, oppression, burden, and expense. Where appropriate, Plaintiff has defined the specific time period encompassed by specific responses.

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

## V. SPECIFIC OBJECTIONS AND RESPONSES TO INTERROGATORIES.

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

### ALLEGED NSA INTERCEPTION OF SUBSTANTIALLY ALL INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS

**INTERROGATORY NO. 1:**

Notwithstanding the holding of the Court of Appeals in this case that "Plaintiffs lack standing to sue … under the Dragnet Allegation because they can't plausibly show that the NSA is intercepting their communications via a dragnet," Wikimedia Found. v. NSA, 857 F.3d 193, 216 (4th Cir. 2017), does Plaintiff still contend, for the purpose of establishing jurisdiction, that NSA Upstream surveillance involves the interception, copying, and review (as those terms are used in paragraph 56 of the Amended Complaint) of all or substantially all international Internet text-based

communications?

**RESPONSE TO INTERROGATORY NO. 1:**

In addition to the General Objections above which are incorporated herein, Plaintiff also objects that this Interrogatory seeks a statement of Plaintiff's legal strategy or information that is protected by the attorney-client privilege or the attorney work product doctrine. Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

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

**INTERROGATORY NO. 2:**

Unless Plaintiff's response to Interrogatory No. 1, above, is an unequivocal "no," then please state the basis of Plaintiff's contention that NSA Upstream surveillance involves the interception, copying, and review of all or substantially all international Internet text-based communications, including, but not limited to, the contentions that "Upstream surveillance is intended to enable the comprehensive monitoring of international internet traffic," see Amended Complaint ¶ 48; that "the NSA is temporarily copying and then sifting through the contents of what is apparently most e mails and other text-based communications that cross the border," see id. ¶ 69; that "it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data," see Pl.'s Opp. to Defs.' MTD at 18-19; and that the U.S. Government "has acknowledged … that the NSA … examines the full contents of essentially everyone's communications to determine whether they include references to the NSA's search terms," *see id*. at 10.

**RESPONSE TO INTERROGATORY NO. 2:**

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

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

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

The bases for Plaintiff's contention include the following:

- Basic principles underlying how Internet communications are transmitted and how surveillance on a packet-switched network operates.
- Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (2014) ("PCLOB Report"), including pages 7–10, 12–13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica (June 4, 2015) (and associated documents)

- Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on Vast Scale*, N.Y. Times, Aug. 15, 2015 (and associated documents)
- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)
- Charlie Savage, *Power Wars* (2015)

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

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

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

selector, the eavesdropper must create a temporary copy of all packets that might be a part of such a communication.

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

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

added).

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

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

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

communications of so many targets scattered around the world will travel many different routes across the Internet backbone, based on the locations of those various targets, their individual movements over time, and changes in network conditions. These communications will be intermingled with those of the general population in the flow of Internet traffic. An intelligence agency that seeks to reliably intercept communications to, from, or about its targets, could do so only by searching substantially all text-based communications entering or leaving the country.

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

> "Computer scientists said that it would be difficult to systematically search the contents of the communications without first gathering nearly all cross-border text-based data; fiber-optic networks work by breaking messages into tiny packets that flow at the speed of light over different pathways to their shared destination, so they would need to be captured and reassembled."

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

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

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

NSA documents published in the press show that the NSA has installed surveillance equipment at many major chokepoints on the Internet backbone. One of these NSA documents states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter and leave the United States." *See* Plaintiff's First Amended Complaint ¶ 69. Another shows that just one of those participating providers has facilitated Upstream surveillance at seven major international chokepoints in the United States. *Id.* ¶ 68. Additional reporting states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents).

**ALLEGED VOLUME AND GLOBAL DISTRIBUTION OF WIKIMEDIA'S INTERNATIONAL, TEXT-BASED, INTERNET COMMUNICATIONS**

**INTERROGATORY NO. 3:**

Please identify each category of Wikimedia international, text-based, Internet communications that Plaintiff contends, for purposes of establishing jurisdiction, is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, including but not limited to, user visits to Wikimedia sites; contributions and edits to Wikimedia websites; Wikimedia discussion forums; Wikimedia discussion pages; e mail sent via Wikimedia among registered users; communications "over wikis" among small or limited groups of users; mailing lists with restricted membership; other use of Wikimedia Projects, websites, and webpages by "community members" to interact with one another; internal log communications; "Community Consultations;" solicitations of user input and preferences; and other communications sent and received by Wikimedia staff in carrying out Wikimedia's work. *See* Amended Complaint ¶¶ 79, 84, 86, 92, 93, 102.

**RESPONSE TO INTERROGATORY NO. 3:**

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court.

Subject to and without waiving any of these General or Specific Objections, Plaintiff responds as follows. As explained in Wikimedia's First Amended Complaint, Wikimedia contends that Upstream surveillance implicates at least three categories of communications (Am. Compl. ¶ 86): (1) Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other. Examples of these communications include, but are not limited to, page views to Wikimedia websites, edits and contributions to Wikimedia websites, emails between

registered Wikimedia users and emails on Wikimedia's mailing lists.

(2) Wikimedia's internal log communications.

(3) Electronic communications of Wikimedia staff. Examples of these communications include, but are not limited to, Gmail, Google chat, Internet Relay Chat, and Slack. Additionally, Wikimedia staff members use a variety of third-party tools to conduct their work, including, but not limited to, Google Apps/G Suite, Trello, Sugar, Qualtrics, User Testing and Salesforce.

**INTERROGATORY NO. 4:**

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify the submarine or terrestrial cables entering or exiting the United States that have carried that category of Wikimedia communications in the past 24 months. To identify a submarine or terrestrial cable means to state its originating or terminating location in the United States, to state its terminating or originating location abroad, and to identify the person(s) owning or controlling it.

**RESPONSE TO INTERROGATORY NO. 4:**

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad and unduly burdensome. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants and as ordered by the Court, and is not reasonably calculated to lead to the discovery of admissible evidence. Specifically, the categories of Plaintiff's communications subject to Upstream surveillance are not relevant to Plaintiff's standing. Plaintiff further objects that this Interrogatory seeks information that is within Defendants' control.

Plaintiff also objects that this Interrogatory is improperly compound in that it contains

multiple subparts. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

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

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

To a near certainty, Plaintiff's communications traverse all submarine and major terrestrial cables carrying public Internet data into and out of the United States. Publicly available data shows that submarine cables include those listed in Exhibit A. (Exhibit A was created in reliance on publicly available data that Plaintiff has not independently verified.)

**INTERROGATORY NO. 5:**

For each category of Wikimedia international, text-based, Internet communications identified in response to Interrogatory No. 3, above, that Plaintiff contends is intercepted, copied, and reviewed by the NSA in the course of Upstream surveillance, please identify the Internet circuits entering or exiting the United States that have carried that category of communication in the past 24 months. To identify a circuit means to state its location of entry to or exit from the United States, to state its country (or, if unknown, global region(s)) of origin or termination abroad, and to identify the person(s) owning or controlling it.

**RESPONSE TO INTERROGATORY NO. 5:**

In addition to the General Objections above which are incorporated herein, Plaintiff also objects that this Interrogatory is overbroad and unduly burdensome. Plaintiff further objects that this Interrogatory seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff further objects that this Interrogatory seeks information that is

within Defendants' control.

Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

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

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

**INTERROGATORY NO. 6:**

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

**RESPONSE TO INTERROGATORY NO. 6:**

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

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

**(1) Wikimedia communications with its community members.** Between April 23, 2017

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

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

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

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

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

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

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

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

**INTERROGATORY NO. 7:**

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

**RESPONSE TO INTERROGATORY NO. 7:**

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

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

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

geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

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

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

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

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

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

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

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

**INTERROGATORY NO. 8:**

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

**RESPONSE TO INTERROGATORY NO. 8:**

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

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

**(1) Wikimedia communications with its community members.** The number of HTTPS requests that Wikimedia's U.S. servers received from users in each country, territory, or region between April 23, 2017 and December 31, 2017 is attached as Exhibit B and will be included in a forthcoming production to Defendants. Each HTTPS request generates a corresponding response

that is not reflected in the figures included in this analysis. These figures are estimates that were derived using MaxMind geolocation data to determine the country associated with the client IP of each HTTPS request transmitted to Wikimedia's servers in the United States.

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

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

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

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

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

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

engaged over 80 contractors, located across more than 30 different countries.

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

**INTERROGATORY NO. 9:**

Please identify the location, by (i) nation, (ii) state, province, or the equivalent, as applicable, and (iii) city, town, or county, as applicable, of each of Wikimedia's servers on which one or more of its "wiki"-based Projects and other related websites and pages (see Amended Complaint ¶ 78), is or since 2008 has been hosted, specifying which of Wikimedia's Projects, sites, or pages is hosted in whole or in part on each server.

**RESPONSE TO INTERROGATORY NO. 9:**

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is overbroad, unduly burdensome and seeks information that is not reasonably calculated to lead to the discovery of admissible evidence. Plaintiff additionally objects that this Interrogatory is impracticable in that it requests the identification of each webpage that has been hosted by a particular server. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects that the term "server" and the phrases "in whole or in part" are vague and ambiguous in the context of this Interrogatory. Plaintiff further objects that this Interrogatory seeks information that exceeds the scope of jurisdictional discovery as defined by Defendants, *see* ECF No. 116 at 4, and as ordered by the Court.

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

The following is a list of the locations of each Wikimedia server on which one more of its

"wiki"-based Projects and other related websites and pages is or at some point in time between 2008 and the present has been hosted.

- United States
  - Ashburn, Virginia
  - Carrollton, Texas
  - Chicago, Illinois
  - Dallas, Texas
  - San Francisco, California
  - Tampa, Florida
- The Netherlands
  - Amsterdam, North Holland
  - Haarlem, North Holland
- South Korea
  - Seoul

For purposes of this response, Wikimedia construes the term "server" to mean any public facing Internet access point operated by Wikimedia.

The remainder of this Interrogatory calls for information that exceeds the scope of jurisdictional discovery and Plaintiff therefore will not provide a response at this time.

**INTERROGATORY NO. 10:**

Please state the number of "logs" or "log entries" (or, if not equivalent, both) contained in each "log communication" sent from Wikimedia servers abroad to Wikimedia servers in the United States, and the frequency with which such log communications are sent. *See* Amended Complaint ¶ 93.

**RESPONSE TO INTERROGATORY NO. 10:**

In addition to the General Objections above which are incorporated herein, Plaintiff further objects that this Interrogatory is vague and ambiguous, overbroad, and not reasonably limited in time. Plaintiff also objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff additionally objects to this Interrogatory as duplicative of other written discovery propounded by Defendants.

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

One log or log entry is contained in a single communication. The frequency of log communications transmitted to Wikimedia's servers from outside of the United States is set forth in Plaintiff's response to Interrogatory No. 8.

**INTERROGATORY NO. 11:**

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

**RESPONSE TO INTERROGATORY NO. 11:**

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

Numerous facts support Wikimedia's allegations that its "community of volunteers, contributors, and readers consists of individuals in virtually every country on earth" and that

Wikimedia engages in "communications . . . with individuals in virtually every country on earth." As explained in Wikimedia's responses to NSA Interrogatory Nos. 6-8, Wikimedia users from all over the world read and contribute to Wikimedia's Project pages. This analysis is further supported by statistics showing that Wikimedia's Project pages are edited and viewed by millions of users around the world. Wikimedia publishes current monthly page view statistics by country (*available* at https://stats.wikimedia.org/wikimedia/squids/SquidReportPageViewsPerCountryOverview.htm), and maintains an archive with analogous data for past months (*available* at https://stats.wikimedia.org/archive/squid_reports/).

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

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

**INTERROGATORY NO. 12:**

Please state the basis of Plaintiff's allegation, in paragraph 61 of the Amended Complaint, that "Plaintiff['s] communications almost certainly traverse every international backbone link connecting the United States with the rest of the world," and the related contention that "Plaintiff['s] communications almost certainly traverse every major internet circuit connecting the United States with the rest of the world," see Pl.'s Opp. to Defs.' MTD at 23, including as part of the response a specification of what Plaintiff means by the term "link" and "circuit" and the

identification by location and ownership or control of each such international backbone link or circuit that Wikimedia communications allegedly traverse.

**RESPONSE TO INTERROGATORY NO. 12:**

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

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

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

The bases of Plaintiff's allegations are the scope and distribution of Plaintiff's international Internet communications.

According to the Foreign Intelligence Surveillance Court and the Privacy and Civil Liberties Oversight Board, Upstream surveillance is directed at "circuits" or "international Internet link[s]" on the Internet backbone. *See* PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of FISA 36–37 (2014) ("PCLOB Report"); [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). The NSA's Section 702 targeting procedures have similarly described how the NSA targets Internet "links." *See* Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended (July 2009), *available at*

https://www.aclu.org/files/natsec/nsa/20130816/FAA%20Targeting%20Procedures.pdf.

Plaintiff's understanding is that a "circuit" or "link" is a pathway between devices in telecommunications networks. These circuits are carried on, for example, physical media such as cables and fibers, but there is not necessarily a one-to-one correspondence between each circuit and its underlying means of transmission. For example, multiple circuits may traverse a single fiber, and a single circuit may span multiple fibers.

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

**INTERROGATORY NO. 13:**

Please identify each of the international Internet "backbone chokepoints," whether cables, circuits, or other communications facilities, at which Plaintiff contends, in paragraph 66 of the Amended Complaint, the NSA must be conducting Upstream surveillance, stating for each such "backbone chokepoint" the basis of Plaintiff's contention.

**RESPONSE TO INTERROGATORY NO. 13:**

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is improperly compound in that it contains multiple subparts. Plaintiff also objects that this Interrogatory seeks information that is within Defendants' control. Plaintiff further objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

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

An NSA document states that the NSA has established interception capabilities on "many of the chokepoints operated by U.S. providers through which international communications enter

and leave the United States." *See* NSA Staff Processing Form, Subject: SSO's Support to the FBI for Implementation of their Cyber FISA Orders.

The "chokepoints" at which the NSA conducts Upstream surveillance have included the "seven access sites" identified in an NSA document, reproduced at paragraph 68 of Plaintiff's First Amended Complaint (ECF No. 70-1).

Additional reporting after the filing of the Amended Complaint states that the NSA has installed surveillance equipment in at least 17 "internet hubs" operated by another major U.S. telecommunications provider. *See* Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents, one of which describes the surveillance of hundreds of circuits at a specific AT&T trans-Pacific cable site); Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents); Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents) (describing surveillance on AT&T's network, including on "OC-192 and 10GE peering circuits"; describing surveillance on Verizon's network, including at a cable-landing site called BRECKENRIDGE).

**INTERROGATORY NO. 14:**

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

**RESPONSE TO INTERROGATORY NO. 14:**

In addition to the General Objections above which are incorporated herein, Plaintiff objects

that this Interrogatory is duplicative of other written discovery propounded by Defendants. Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

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

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

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

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

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

In addition, a *New York Times* report from August 2013 states, based on a review of NSA documents and interviews with senior intelligence officials, that "the N.S.A. is temporarily

copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border." Charlie Savage, *N.S.A Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013; *see* also Charlie Savage, *Power Wars* 207–11 (2015).

**INTERROGATORY NO. 15:**

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

**RESPONSE TO INTERROGATORY NO. 15:**

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

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

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

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

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

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

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

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

Other bases of Plaintiff's contentions include:

- The PCLOB Report, including pages 7–10, 12–13, 22, 30–41 & n.157, 79, 111 n.476, 120–22, 125, 143, and official government sources concerning Upstream surveillance cited therein.
- [*Redacted*], No. [Redacted], 2011 WL 10945618 (FISC Oct. 3, 2011)
- 50 U.S.C. §§ 1801, 1881a.
- David S. Kris & J. Douglas Wilson, *National Security Investigations and Prosecutions* § 17.5 (July 2015)

- Julia Angwin et al., *NSA Spying Relies on AT&T's 'Extreme Willingness to Help'*, ProPublica, Aug. 15, 2015 (and associated documents)
- Julia Angwin & Jeff Larson, *New Snowden Documents Reveal Secret Memos Expanding Spying*, ProPublica, June 4, 2015 (and associated documents)
- Jeff Larson et al., *A Trail of Evidence Leading to AT&T's Partnership with the NSA*, ProPublica, Aug. 15, 2015 (and associated documents)
- PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI)
- Charlie Savage, *Power Wars* (2015)

**INTERROGATORY NO. 16:**

Please state the basis of Plaintiff's allegations in paragraph 59 of the Amended Complaint, including the allegations that "[t]he NSA could readily configure its [alleged] surveillance equipment to ignore" Internet traffic that is "not amenable to … text-based searches;" that such traffic "is likely of no foreign-intelligence interest to the government;" and that "ignor[ing]" such traffic would result in "substantial efficiency gains."

**RESPONSE TO INTERROGATORY NO. 16:**

In addition to the General Objections above which are incorporated herein, Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time.

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

Subject to and without waiving any of these General or Specific Objections, Plaintiff

responds as follows.

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

Plaintiff's allegations are also based on the fact that a substantial percentage of Internet traffic consists of video traffic; and that video traffic from major video-traffic providers, such as Netflix, is likely of little foreign-intelligence interest to the government because it reflects only movie- and television-viewing habits.

**INTERROGATORY NO. 17:**

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

**RESPONSE TO INTERROGATORY NO. 17:**

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

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

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

**INTERROGATORY NO. 18:**

Please state the basis of Plaintiff's allegation, in paragraph 63 of the Amended Complaint, that "[t]o search the contents of any text-based communication for instances of the NSA's 'selectors' as that communication traverses a particular backbone link, the government must first copy and reassemble all of the packets that make up that communication."

**RESPONSE TO INTERROGATORY NO. 18:**

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory seeks information that is the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

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

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

**INTERROGATORY NO. 19:**

Please state with particularity what Plaintiff means by the term "reliably" as used in

paragraphs 62, 63, and 66 of the Amended Complaint in the phrases "reliably obtain communications," and "reliably intercept … communications," and as the term "reliably," or its equivalent, may be used in Plaintiff's response to any of Defendants' other interrogatories.

**RESPONSE TO INTERROGATORY NO. 19:**

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is compound, vague, ambiguous and overly burdensome in that it requests that Plaintiff define its use of the word "reliably" in a variety of discrete contexts, and in that it calls for a subjective judgment about what terms are "equivalent" to the term "reliably." Plaintiff additionally objects that these matters may be the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery.

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

The PCLOB has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10. And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can *reliably* acquire data packets associated with the proper communications." *Id*. at 143 (emphasis added).

Plaintiff's complaint uses the term "reliably" in different ways depending on context. For example, in paragraphs 62 and 63 of the Amended Complaint, Plaintiff uses the term "reliably" to signify that the government could not conduct Upstream surveillance as it has publicly described

it without undertaking certain steps. Paragraph 66 of Plaintiff's complaint quotes the PCLOB's use of the term "reliably."

**INTERROGATORY NO. 20:**

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

**RESPONSE TO INTERROGATORY NO. 20:**

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

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

The PCLOB has described the use of Upstream surveillance to collect "about" communications as "an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10. And it has said about Upstream surveillance more generally that this method's "success . . . depends on collection devices that can *reliably* acquire data packets associated with the proper communications." *Id*. at 143 (emphasis added); *see also* PCLOB, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 26:15–18 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI).

**INTERROGATORY NO. 21:**

To the extent not already stated or identified in response to Interrogatory Nos. 13-20, above, or in response to Defendant United States Department of Justice's First Set of Interrogatories, Interrogatory Nos. 1-6, please state the basis of Plaintiff's contention that the NSA is intercepting, copying, and reviewing at least some of its communications.

**RESPONSE TO INTERROGATORY NO. 21:**

In addition to the General Objections above which are incorporated herein, Plaintiff objects that this Interrogatory is a contention Interrogatory that is premature at this stage in the litigation. Plaintiff also objects that this Interrogatory seeks information that is the subject of expert reports and testimony, as to which Plaintiff will provide discovery at the appropriate time. Plaintiff therefore specifically reserves the right to supplement and amend its response based on further investigation and discovery. Plaintiff also objects that this Interrogatory is overbroad and duplicative of other written discovery propounded by Defendants.

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

Plaintiff's contention is based on the volume and distribution of its communications, basic principles governing the routing and transmission of Internet communications, and basic principles governing how surveillance on a packet-switched network operates.

Dated: January 11, 2018

*/s/Ashley Gorski*

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

*Counsel for Plaintiff Wikimedia Foundation, Inc.*