**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 2 OF 7 (JA0920–JA1790)

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

*Counsel for Defendants–Appellees*

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

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

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

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

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

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

# JOINT APPENDIX
## Table of Contents

## VOLUME 1

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

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

### Exhibits to Wikimedia Foundation's Motion to Compel

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

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

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

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

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

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

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

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

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

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

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

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

**Opinion & Order Denying Wikimedia Foundation's Motion to Compel**

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

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

**Exhibits to Defendants' Motion for Summary Judgment**

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

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

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

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

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

**VOLUME 2**

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

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

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

**VOLUME 3**

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

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

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

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

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

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

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

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

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

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

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

**VOLUME 4**

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

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

Exhibit 12: Wikimedia document compiling German-user-

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

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

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

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

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

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

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

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

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

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

**VOLUME 5**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Exhibit 42: Wikimedia's Supplemental Exhibit C in response

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

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

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

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

**VOLUME 6**

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

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

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

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

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

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

Exhibit 11: Relevant Portions of the Deposition of Michelle

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

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

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

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

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

**VOLUME 7**

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

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

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

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

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

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

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

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

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

**Opinion & Order Granting Defendants' Motion for Summary Judgment**

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

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

**Wikimedia Foundation's Notice of Appeal**

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

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

# Plaintiff's Exhibit 1

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

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

**DECLARATION OF SCOTT BRADNER**

**I. INTRODUCTION ..... 1**

**II. SUMMARY OF MY CONCLUSIONS ..... 2**

**III. QUALIFICATIONS ..... 4**

A. Employment ..... 5
B. Publications ..... 5
C. The Internet Engineering Task Force ..... 6
D. Involvement in Data Network Design and Operation ..... 6
E. Compensation ..... 7

**IV. BACKGROUND OF THE TECHNOLOGY IN THIS CASE ..... 7**

A. History of the Internet ..... 8
1. Pre-1960s ..... 8
2. Advanced Research Projects Agency (ARPA) ..... 9
3. The origin of Packet Data Networks ..... 10
4. Packets ..... 10
5. The ARPANET ..... 14
B. Definitions ..... 17
1. A Communication ..... 17
2. Layers, links and nodes ..... 18
3. Flow ..... 21
4. Transaction ..... 22
5. Network ..... 23
6. Network Node ..... 24
7. Circuit ..... 24
8. Packet ..... 25
9. Switch ..... 29
10. Router ..... 29
11. Mirroring ..... 29
12. Routing ..... 30
13. Internet Protocol ..... 30
14. Internet Service Provider (ISP) ..... 30
15. Proxy ..... 31
16. Tunnel ..... 31
17. Metadata ..... 31
C. The Key Internet Protocols ..... 32
1. The Internet Protocol Suite ..... 32
a. The Internet Protocol (IP) ..... 32
i. IP addresses ..... 33
ii. Viewing IP header information ..... 34
iii. Sizes of IP packets ..... 34
iv. Multiple packets in a communication ..... 35
b. Transport Protocols ..... 35
i. The User Datagram Protocol (UDP) ..... 36
ii. The Transmission Control Protocol (TCP) ..... 37
2. Application Protocols ..... 39

a. The Hypertext Transfer Protocol (HTTP) ..... 39
i. HTTP commands ..... 39
ii. Encrypted HTTP (HTTPS) ..... 39
iii. HTTPS Handshake ..... 41
iv. IP addresses in HTTP packets ..... 42
b. Email ..... 42
i. Email Header Information ..... 43
ii. Email Servers ..... 44
iii. Simple Mail Transfer Protocol (SMTP) ..... 45
(1) SMTP Metadata ..... 47
(2) IP addresses in email packets ..... 47
iv. Internet Message Access Protocol (IMAP) ..... 47
c. Telephone Calls ..... 48
3. Plain Text in Application Protocol Headers ..... 48
4. Number of Packets in a Communication ..... 49
D. Other Features of the Internet and its Architecture Relevant to this Case ..... 50
1. Internet Architecture ..... 50
2. Internet Backbone ..... 51
3. Internet Service Providers (ISPs) ..... 53
a. Address assignments for ISPs ..... 55
4. ISP Interconnection ..... 56
5. Customer Networks ..... 57
a. Address assignments for customer networks ..... 58
6. Customer Network Interconnection ..... 58
7. Network Address Translators (NATs) ..... 59
E. Routing in the Internet ..... 59
1. Autonomous System (AS) ..... 61
2. Routing an IP Packet ..... 61
3. Volatility of Routing Information ..... 64
4. Asymmetric Data Paths ..... 66
F. International Connections ..... 67
1. Details of Undersea Fiber-Optic Cables ..... 70
2. Details of Terrestrial Fiber-Optic Cables ..... 73
3. Public Internet Communications on International Fiber-Optic Cables ..... 73
4. Undersea Fiber-Optic Cable Landing Locations ..... 75
5. Terrestrial Fiber-Optic Cable Terminations ..... 77
G. Places to Monitor International Public Internet Communications ..... 78
H. Locating Network Nodes Using IP Addresses ..... 81

**V. NSA'S SECTION 702 COLLECTING OF COMMUNICATIONS ..... 82**
A. Selectors ..... 83

**VI. PRISM COLLECTION PROGRAM ..... 88**

**VII. OPINIONS A, B & C: THE NSA'S UPSTREAM COLLECTION PROGRAM INVOLVES COPYING, REASSEMBLING AND REVIEWING INTERNET TRANSACTIONS.....88**
A. Upstream Collection Program.....90
1. A Description of NSA's Upstream Collection Program.....91
2. Upstream Collection Process.....93
a. Stage 1: Copying the Packets.....94
i. Copy-Then-Filter.....96
(1) Fiber-optic splitter.....96
(2) Link-Layer Copying.....97
(3) Filtering the packets.....97
ii. In-Line Filter.....98
iii. Implementation.....98
b. Stage 2: Filtering.....101
c. Stage 3: Reassembling Transactions.....106
d. Stage 4: Reviewing Transactions.....109
i. "multiple communications transaction (MCT)" collection.....111
ii. "about" collection.....112
iii. Collection of Encrypted Internet Transactions.....114
e. Stage 5: Ingesting Transactions.....116
3. Upstream Collection Monitor Placement.....116

**VIII. OPINION D: WIKIMEDIA COMMUNICATIONS ARE TRANSPORTED ON ALL INTERNATIONAL CIRCUITS ORIGINATING OR TERMINATING IN THE UNITED STATES.....119**
A. Wikimedia.....120
1. Wikimedia Websites.....120
2. Wikimedia International Communications.....121
3. Protocol Support on Wikimedia Websites.....124

**IX. OPINION E: THE NSA HAS COPIED, REASSEMBLED AND REVIEWED WIKIMEDIA COMMUNICATIONS.....124**

**X. DR. SCHULZRINNE'S DECLARATION.....126**
A. Surveillance Configurations.....127
B. Selectively Filtering Internet Traffic.....129
C. Selectively Filtering Wikimedia IP addresses.....132
D. U.K. Surveillance Disclosures and Court Proceedings.....134

## I. INTRODUCTION

1. My name is Scott Bradner. I have been asked by the plaintiff's counsel in *Wikimedia Foundation v. National Security Agency*, No. 1:15-cv-006622-TSE (D. Md.), to provide an expert report addressing the following questions:

   a. What is the basic structure of the Internet and how do communications traverse it?

   b. How does upstream collection work, based on official government acknowledgments and my expertise in network design and operation?

   c. What is the likelihood that the government has copied and reviewed the plaintiff's international text-based Internet communications in the course of upstream collection?

2. In this declaration I will address these questions based on my own technical expertise and experience, and on relevant technical principles. The information I used to understand and explain the Section 702 collection of Internet transactions came from my review of documents provided to me by plaintiff's counsel. Counsel has informed me that all of the U.S. government documents they provided have been officially released by the government.

3. A list of the documents provided to me by plaintiff's counsel is attached as Appendix B.

4. After explaining my conclusions, I address the declaration of Dr. Henning Schulzrinne, filed in support of the government's motion for summary judgment.

5. In this declaration, I refer to actions such as copying, reassembling and reviewing as if they were wholly performed by the NSA. But in doing so, I am specifically including the possibility that some or all of those actions are performed by

others at the direction of the NSA. In addition, when I refer to "copying," as in "copying a packet," I am including any process which results in one or more duplicate copies of the original packet, for example, splitting a beam of light and reconstructing packets from each portion of the split light beam, as well as using an electronic device to produce a copy of a packet it received on a network.

## II. SUMMARY OF MY CONCLUSIONS

6. After reviewing the materials available to me in this case I have concluded the following. These conclusions apply both before and after the "about" collection was stopped:

a. It is my opinion that, to conduct upstream collection of international Internet communications traversing any particular circuit, as this operation has been described by the government, the NSA must be copying at an absolute minimum the packets constituting the transactions it wishes to review for the presence of selectors. Based on other practical necessities I describe below, it is also my opinion that the NSA is almost certainly either (1) copying all packets traversing that circuit or (2) copying all of the packets that an IP address filter test determines are not part of a wholly domestic transaction.

b. It is my opinion that, in order to review Internet transactions to determine if a selector tasked for collection is present, the NSA must be reassembling the packets of the transactions it intends to review.

c. It is my opinion that the NSA must review the reassembled Internet transactions in order to identify those that include a tasked selector and thus are subject to collection under the upstream collection program.

d. It is my opinion that it is virtually certain that Wikimedia's international communications traverse every circuit carrying public Internet traffic on every international cable connecting the U.S. to other countries.

e. It is my opinion that it is virtually certain that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications.

7. I have carefully reviewed the declaration of Dr. Schulzrinne, and nothing in it alters the above conclusions. I will address parts of his declaration at various places in my declaration and more fully at the end of my declaration. In summary, I conclude as follows:

a. Dr. Schulzrinne does not directly address the likelihood that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications. Accordingly, he does not deny that it is virtually certain that the NSA has, in fact, done so.

b. Dr. Schulzrinne speculates that the NSA could, in theory, have designed its upstream collection program to have avoided the copying, reassembly and review of *any* of Wikimedia's communications, but as I explain in detail below, his speculation is technically inaccurate and it is, as a practical matter, simply implausible that the NSA designed and operated its upstream collection program as Dr. Schulzrinne speculates it could have to avoid such copying, reassembly and review. For example, he speculates that the NSA could have been and is "blacklisting" Wikimedia's IP addresses or could have been and is filtering out all web traffic from upstream collection. Blacklisting

Wikimedia's IP addresses would not in fact avoid the copying, reassembly or review of Wikimedia's communications, as I explain below. Moreover, there is no reason to believe that the NSA has been or is currently attempting to filter out Wikimedia's traffic, and there are compelling reasons to believe that it isn't. Finally, it strains credulity to suggest that the NSA is, in the course of an Internet surveillance program, deliberately filtering out all *web activity*, one of the most common modes of communication on the Internet. (The NSA has in any event confirmed that it monitors web activity under upstream collection, as I note below.)

c. For these reasons, Dr. Schulzrinne's speculation about technically possible but exceedingly unlikely measures the NSA might have been taking or might currently be taking to avoid Wikimedia's communications do not alter my conclusion that it is a virtual certainty that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications.

8. I rely on my own knowledge as well as public technical publications for the background of the technology section and on the documents supplied to me by Wikimedia's counsel to understand the NSA's upstream collection program and to support these opinions.

## III. QUALIFICATIONS

9. My background and expertise that qualify me as an expert in the technical issues in this case are as follows:

**A. Employment**

10. I worked at Harvard University ("Harvard") in a number of information technology roles, from 1966 to 2016, at which time I retired. My last role at Harvard was as a Senior Technology Consultant in the office of the Harvard University Chief Technology Officer (CTO) where I worked on identity management projects. Before joining the Harvard CTO's office I was the Harvard University Technology Security Officer (UTSO) for 8 years. I currently teach courses on *Technology, Security, Privacy, and the Realities of the Cyber World* at the Harvard University Extension School and have supervised masters and Ph.D. theses for students in Harvard University itself and in the Harvard University Extension School. In the past I have taught classes for undergraduate and graduate students at Harvard University and multi-day tutorials in the 1990s to thousands of students at the largest U.S. Internet-related trade show as well as at a number of major technology companies including IBM, Oracle and Nortel. I have also consulted for many technology companies, a number of universities and for multiple departments within the U.S. government.

**B. Publications**

11. I have authored or co-authored 4 books and over 90 articles or other publications in peer-reviewed journals, conference proceedings, popular publications, monographs and standards organizations. These publications span a range of topics including analyzing network hardware, Internet technology, technology policy and standards processes. In addition, between 1992 and 2013 I wrote a regular column in the technical journal *Network World*, which was read around the world.

### C. The Internet Engineering Task Force

12. The Internet Engineering Task Force (IETF) is a primary standards creation and maintenance body for the Internet. The work of the IETF is conducted in Working Groups and IETF Working Groups are organized into Areas. Each of the technical areas in the IETF is managed by one to three Area Directors. At various times I served as the Director or co-Director of the IETF's Operational Requirements, Operations and Management, IP Next Generation, Transport and Sub-IP areas. As an Area Director, I served as one of the members of the Internet Engineering Steering Group (IESG), the IETF's standards approval and general management committee from 1993 to 2003. As a member of the IESG, I reviewed and evaluated hundreds of IETF working documents that were proposed by IETF working groups or IETF participants to be approved as IETF standards. The documents I was involved in approving covered all areas of IETF technology and included all aspects of Internet design, operation and evolution. I will note in passing that I worked often with Dr. Schulzrinne in the IETF.

### D. Involvement in Data Network Design and Operation

13. I was involved in the design, operation and use of data networks at Harvard University since the early 1970s, and was involved in the design, implementation and operation of the original Harvard data networks, the Longwood Medical Area network (LMAnet) and the New England Academic and Research Network (NEARnet).

14. Additionally, I was the founding chair of the technical committees of LMAnet, NEARnet and the Corporation for Research and Enterprise Network (CoREN). I was involved in the day-to-day operation of these networks as well as their evolution.

15. I have also served as a consultant on network design, management and security to educational institutions, federal agencies, international telecommunications enterprises and commercial organizations ranging from Fortune 500 companies to small businesses, from 1989 to the present. I have served as an expert witness in the Communications Decency Act challenge (*Reno v. ACLU*, 521 U.S. 844 (1997)) in U.S. federal court and in a number of patent cases.

16. In addition, I have also served on the technical advisory boards of about two-dozen companies in various technology fields, mostly relating to the Internet and other data networks, and I have been a frequent speaker at technical conferences.

17. My CV and list of previous cases is attached to this declaration as Appendix A.

### E. Compensation

18. I am not being compensated for my work in this case other than for travel expenses, if any.

## IV. BACKGROUND OF THE TECHNOLOGY IN THIS CASE

19. I agree in general with the background information Dr. Schulzrinne provides in ¶¶ 16-44 of his declaration. I note below where we disagree. The following involves more detail and sometimes a different focus from Dr. Schulzrinne's background section.

20. This case involves communications over the Internet. The Internet is the world-wide collection of interconnected networks that operate following the standards that define the Internet Protocol. The different networks that make up the Internet are operated independently. There is no overall manager of the Internet, nor is there any general form of governance of the Internet. The Internet operates by mutual agreement

among the companies that produce the computers that connect to the Internet and the companies that operate the independent networks that make up the Internet to implement the same set of technical standards in the software of the computers and to operate the networks in ways that are consistent with generally ad-hoc operational standards. See below for a fuller description of the Internet.

21. To put the relevant technologies and concepts in context, I will provide a brief history of the Internet, define some of the terms I will be using, explain the key protocols in use on the Internet today, and describe other key features of the Internet and its architecture relevant to this case.

### A. History of the Internet

22. I will now provide a short history of the Internet as a way to introduce the technology of the Internet that is relevant to this case.

#### *1. Pre-1960s*

23. The wiring of the world started with the Samuel Morse patent for the telegraph in 1847 and accelerated with the Alexander Graham Bell telephone patent in 1876. Until the late 1960s the networks that supported the telegraph and telephone services only supported those services—that is, they were specific-purpose not general-use networks. In describing the environment that led to the Internet, I will focus on the telephone network.

24. By the beginning of the 1960s, telephone networks had evolved into a general hierarchical hub-and-spoke architecture. The telephones in an area, for example a town, were connected to a telephone switch in a local central telephone office in that town with dedicated pairs of wires. As many as tens of thousands of telephones could be connected to each of these local central telephone switches. These local central office

telephone switches were connected to a more central telephone switch, which, in turn, was connected to an even more central switch.

25. To make a telephone call, a caller would dial a telephone number. The telephone number was sent, digit-by-digit, to the local central office telephone switch over the dedicated pair of wires. Using this telephone number, the local central office switch would then cause a dedicated path to be set up between itself and the local central office telephone switch connected to the telephone assigned the telephone number the caller had dialed. The path might traverse a number of telephone switches. The dialed telephone would then ring and, if someone picked up the dialed phone, a conversation could be held over the dedicated path. When the caller or called person hung up, the dedicated path established to support the call would be "torn down"—that is, the individual wires that had been used to make up the path would be released to be used for future telephone calls.

26. Two significant limitations of this telephone system architecture included:

a. That the wire between the telephone and the local central office telephone switch could only be used for one thing, a single telephone call, at a time.

b. That the failure of a telephone switch or of a connection between pairs of telephone switches would terminate all telephone calls whose paths went through the switch or link that failed.

***2. Advanced Research Projects Agency (ARPA)***

27. Parallel developments in the Cold War between the U.S. and the Soviet Union set the stage for the development of the modern Internet. In the 1950s and 1960s, in that context, the launch of the Sputnik spacecraft by the Soviet Union on October 4, 1957 was a profound shock to the U.S. scientific and political establishment. In direct

response to the launch of the Sputnik, President Dwight David Eisenhower established the Advanced Research Projects Agency (ARPA) in the U.S. Department of Defense within three months of the launch. ARPA was established with a very broad mandate to undertake advanced research in any area that might be helpful to the U.S. military and, hopefully, to minimize the chance of another Sputnik-like surprise. ARPA came to play an important role in the development of the Internet.

***3. The origin of Packet Data Networks***

28. ARPA was not alone in supporting advanced research within the U.S. Department of Defense. Relevant to this history, the U.S. Air Force supported research efforts at RAND Corporation. One of the researchers at RAND was Paul Baran. Mr. Baran was very worried about the survivability of the telephone system that the U.S. military would need to use for communication in the aftermath of a nuclear attack on the U.S. Mr. Baran developed an alternative architecture that would have a much better chance of surviving mass destruction. That alternative architecture became the basis of today's Internet.

***4. Packets***

29. As noted above in ¶ 26, one of the issues with the architecture of the telephone system in the 1960s was that the failure or destruction of a single one of the large telephone switches or links between switches would terminate any call currently running though that switch or link. Mr. Baran developed the idea of using a large number of small switching nodes interconnected by links as a redundant array. The switching systems are represented by the dots and the links by the interconnecting lines in the sample distributed network shown in the figure below from Mr. Baran's 1962 paper *On Distributed Communications Networks*:

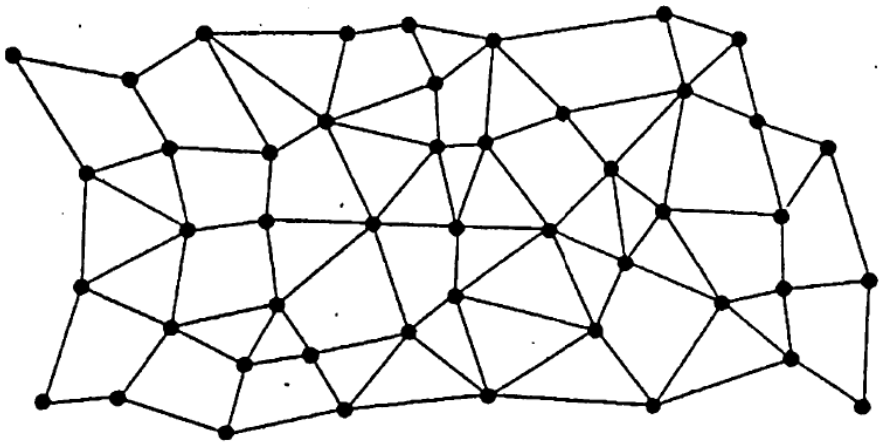


**Figure 1**[1]

30. With this type of redundant architecture, connections can get rerouted in case of a failure of a link or of a switching node. The following figure shows a sample path (green line) that could be used through a network. The path traverses a number of switching nodes and links:

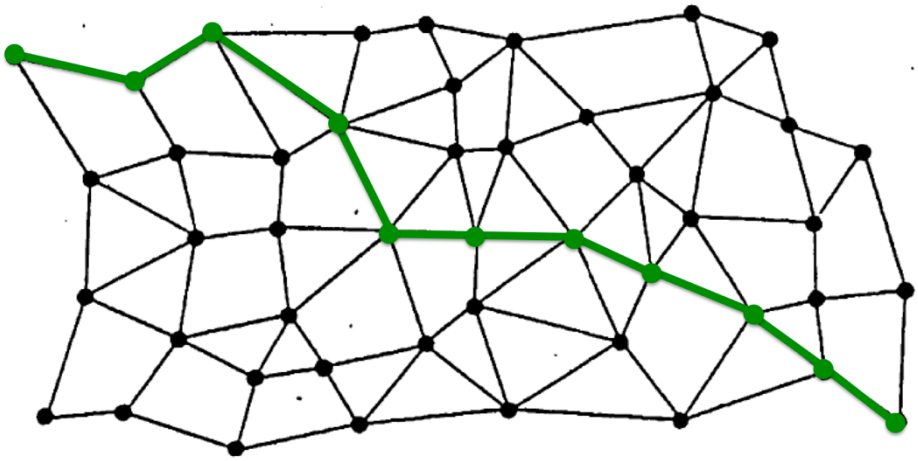


**Figure 2**

[1] Appendix G at 5 (Paul Baran, RAND Corp., *On Distributed Communications Networks* at 4 (Sept. 1962)).

31. The following is the same network showing a sample path after the failure of a switching node in the network (marked by the red X).

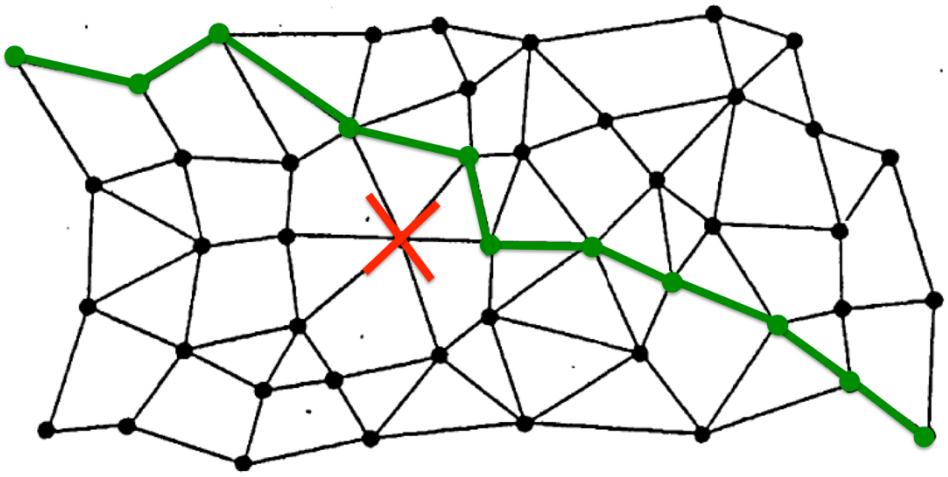


**Figure 3**

32. But redundancy, by itself, is not sufficient. A communication, such as a voice call, would be disrupted during any reroute of the communication path. So Mr. Baran developed the concept of breaking each communication up into multiple autonomous chunks, which he called message blocks but which are now known as "packets", the term which I will use in this report. Mr. Baran's diagram of a packet is shown in the following figure from his 1962 paper:

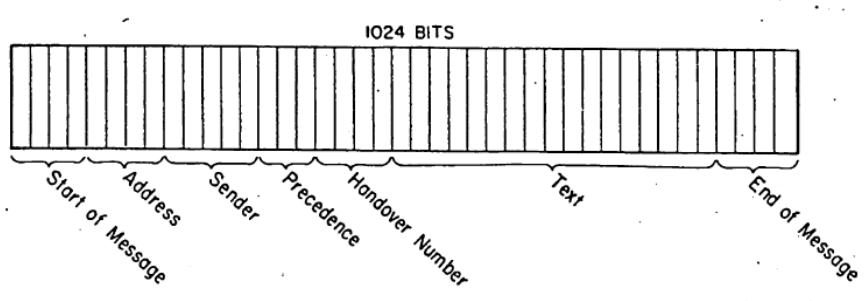


**Figure 4**[2]

33. Each of the packets includes a field at the start of the packet that tells the network to which network node this packet is to be delivered (the "Address" field), a field that says what network node sent the packet (the "Sender" field), some other control information (the "Precedence" and "Handover Number" fields) and a payload field which contains the chunk of information being transported in the packet (the "Text" field).

34. These same types of fields are present in the packets that traverse today's Internet. For example, the following figure shows the format of an Internet Protocol version 4 (IPv4) packet:

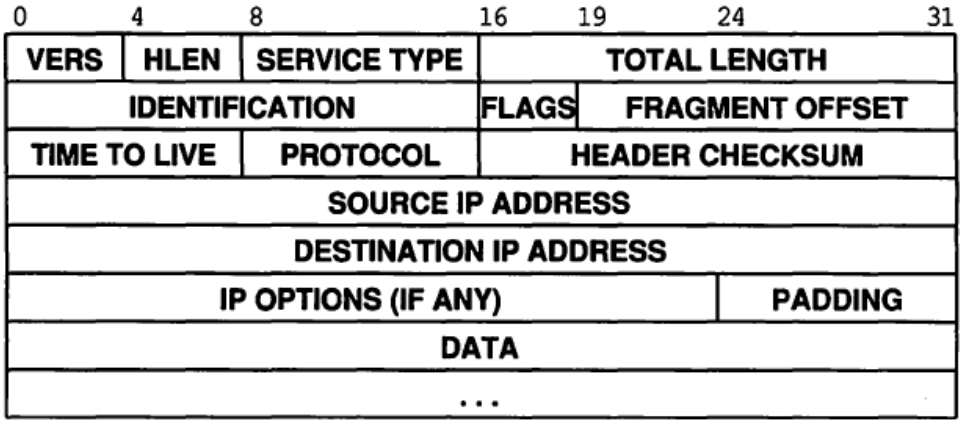



**Figure 5** — IP packet format[3]

35. IPv4 is the version of the Internet Protocol (IP) that was deployed in 1983 and is still the predominant version in use today. A revised version of IP, known as IPv6, is being deployed but is not yet in general use. The IPv4 and IPv6 headers differ but not in ways that alter this discussion.

[2] Appendix G at 27 (Baran, *supra* note 1, at 26).

[3] Douglas E. Comer, *Internetworking with TCP/IP: Principles, Protocols, and Architecture* (2nd ed. 1991).

36. The figure above shows a "source IP address" field (Baran's "sender" field), a "destination IP address" field (Baran's "address" field), a number of fields that correspond to Baran's control information (e.g., "service type", "protocol", etc.) and a "data" field (Baran's "text" field). (See ¶¶ 95-104 for a fuller discussion of the Internet Protocol.)

37. Breaking the communication into packets means that only a small part, if any, of the communication will get lost, and perhaps have to be retransmitted, if the path is disrupted by some failure rather than having the whole communication be terminated.

38. Another big advantage of using packets to carry communications is that multiple communications can be run over the same link at the same time by intermingling packets from different communications. Many, even hundreds or thousands, of separate communications can be running over a single link at the same time, and if the link is in the center of a network, such as the network shown in the Baran figure, these communications can be to and from many different sending and receiving nodes.

***5. The ARPANET***

39. Meanwhile, back at ARPA, there was an interest in sharing big research computers among multiple researchers located around the country or even outside of the country. At that time computers that were needed for large-scale computation were physically very large and very expensive—much too expensive for the government to be able to provide a computer for each research institution. Thus ARPA had an interest in making it possible for researchers at different locations to be able to share the use of the large computers.

40. The approach ARPA decided to take was to build a nation-wide network to interconnect the big computers and the institutions where the researchers were located. ARPA also decided to use the basic concepts that Mr. Baran had developed, even though ARPA at that time was more interested in sharing computing resources than surviving nuclear attacks. The same technology, packet-based data networking, would support both types of needs.

41. The initial parts of the resultant network, known as the ARPANET, were installed in four locations on the U.S. west coast in late 1969. Within a few years the network had been extended to the U.S. east coast and to dozens of nodes. A few years later there were a few hundred ARPANET nodes including a few in the U.K. and Europe.

42. The original ARPANET design had a significant limitation. The ARPANET operated using the Network Control Protocol (NCP). NCP was designed to interconnect network nodes, generally a single node at a location such as a university but occasionally two or three. Bob Kahn realized that, in order to be able to grow, the design had to be changed such that the ARPANET would interconnect networks rather than nodes. Each location, such as Harvard, could have its own network with as many nodes as it wanted to have. The nodes on the networks at multiple sites could then communicate with nodes at other sites with an almost unlimited ability to grow the number of nodes.

43. Dr. Kahn enlisted the help of Dr. Vint Cerf, and together they developed the Internet Protocol. IP defines a way to interconnect networks (thus “inter-net”) such that a node on one network can communicate with another node on the same network or with a node on a different network. The Internet Protocol specifications define the

format of Internet Protocol packets, and, in a general way, how packets are constructed, transported and processed.

44. The ARPANET transitioned from NCP to the Internet Protocol starting on January 1, 1983. This was the start of the Internet, as the concept is understood today.

45. ARPA operated the ARPANET as a backbone network—i.e., a network that interconnected other networks—until 1990. Note that the ARPANET did not have a single link that was its backbone carrying all of its traffic. Instead, as shown in Figure 6 from October 1980, the ARPANET, like Internet Service Providers these days, had a mesh-like set of links that provided for redundancy and shared the traffic load. Traffic would only traverse as much of the ARPANET links as it needed to in order to reach its destination.

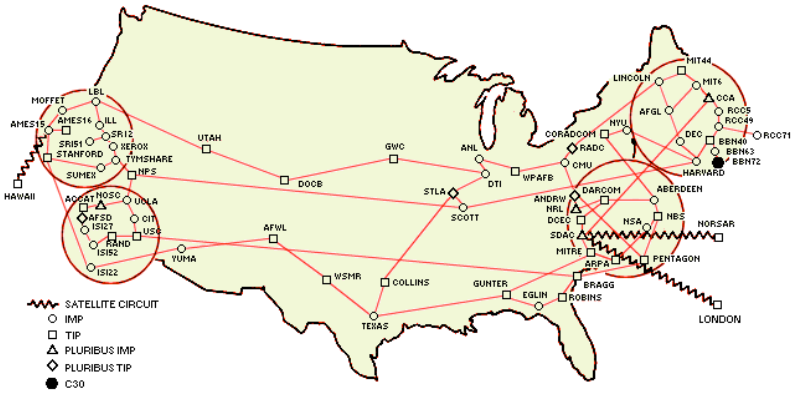



**Figure 6** — The ARPANET in October 1980[4]

46. By the time ARPA shut down the ARPANET, the U.S. National Science Foundation (NSF) was operating its own backbone network (NSFNET) to interconnect networks at NSF-sponsored universities and research centers. The NSF replaced the ARPANET until the NSFNET was closed down in 1995.

[4] *Internet Technology*, Technology UK, http://www.technologyuk.net/telecommunications/internet/internet-technology.shtml.

47. Starting in the late 1980s, commercial Internet service providers operating in parallel to the NSFNET began to appear. By the mid-1990s there were thousands of small local ISPs and a growing number of nation-wide ISPs. By the end of the 1990s, a few of the U.S. ISPs had expanded internationally.

**B. Definitions**

48. The Internet today remains a packet data network, following Baran's original concept of redundant network connections and autonomously routed chunks of data called packets. Before explaining the key protocols and architecture of the Internet today, I will first specify what I mean by the terms that I will be using in this report. Unless otherwise noted, these definitions are widely accepted and consistent with the use of these terms by experts in the field of Internet communications and architectures.

***1. A Communication***

49. The term ***communication*** does not have a single precise definition in the field of Internet communications, but in the context of this report I will generally use the term "communication" to mean data exchanged between a pair of nodes on a network. Communications include phone calls, email messages, data files, requests for web pages and web pages. Communications are broken up into chunks, called ***packets***, for transmission over the network. Communications are bidirectional with packets flowing in both directions even when a user is viewing a web page.

### *2. Layers, links and nodes*

50. Networks are organized into ***layers*** to simplify design and operation. Each layer provides services to the layer above it and shields the layer above it from the complexities of providing that service. The Internet follows the 4-layer model shown in the following figure:

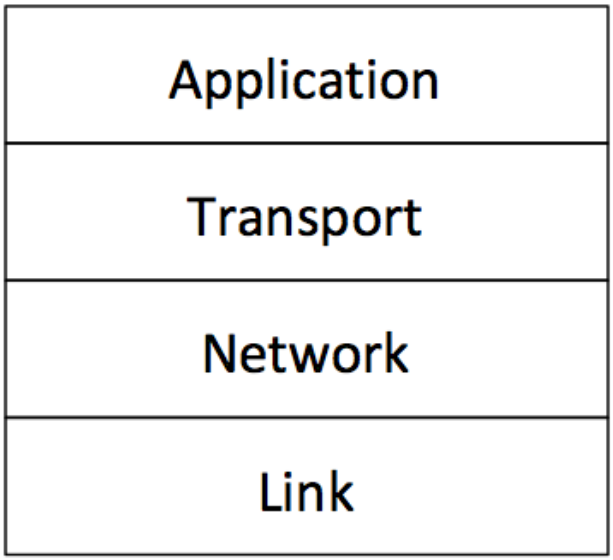



**Figure 7** — Internet 4-layer model

51. The above figure is consistent with the description in ¶ 27 of Dr. Schulzrinne's report except that he includes the physical network that the packets ride on as a layer below the data-link layer.

52. The ***Link Layer***, also known as the ***Data-Link Layer***, is responsible for delivering data in the form of packets over a physical or virtual network link between network devices. A ***physical network link*** is a direct connection between two network devices using a physical medium such as copper wire or fiber optic cable. Another type of network link I will mention later is a virtual network link. A ***virtual network link*** appears to the two nodes communicating over the virtual link to be a physical network

link, but the virtual network link is not restricted to being a physical connection just between the two nodes. Instead it can be implemented as a continuous communication over a network consisting of multiple physical network links. See, for example, the discussion of ***tunnel*** below.

53. One example of a physical network link is Ethernet, the most common type of physical network link used in enterprise data networks. Another example is WiFi, a radio-based equivalent of Ethernet used with portable network devices such as laptops and smartphones. A third example is fiber-optic cable. Short fiber-optic cables are used between buildings in a campus network, longer ones are used between cities and very long fiber-optic cables are used to interconnect continents. A fiber-optic cable contains multiple individual optical fibers. Each individual fiber in a fiber-optic cable can be used as a network link, or individual fibers can be divided up into many different colors of light, known as ***lambdas***. An individual lambda can be used as a network link or multiple lambdas can be combined into a network link.

54. Those network links, such as Ethernet and WiFi, which can interconnect more than two network devices, make use of ***link-layer addresses*** to specify the source and destination of the packets making up communications running over the link-layer network. A link-layer address is a numerical value that uniquely identifies a node on a particular network. The network links that only interconnect two devices, such as lambdas in an optical fiber, generally do not need such addresses since there is only one possible source and one possible destination on any particular link.

55. Sets of interconnected network links are often referred to as ***Local Area Networks*** (***LANs***). If a LAN consists of more than a single network link, the individual

network links in the LAN are interconnected with switches. See below for a description of switches.

56. The ***Network Layer*** is responsible for delivering data between network devices on different LANs. The Internet Protocol defines the network layer in the Internet. See ¶¶ 94-104 for more information about IP. The network layer uses network addresses, rather than link-layer addresses to specify the source and destination of the packets running over a network layer network. A ***network address*** is a numerical value that uniquely identifies a node on a particular network. If the network is the Internet, the network address must be unique across the Internet. The network addresses used in the Internet are ***Internet Protocol (IP) addresses***. See below in ¶¶ 97-98 for a discussion of IP addresses.

57. Devices on the Internet normally have both a link-layer and network address. The link-layer address is used to deliver the packet to the correct device on a particular LAN, and the network address is used to get the packet to the correct LAN. I will describe this further below.

58. The Internet is composed of LANs interconnected with routers. See below in ¶¶ 84, 86 for a description of routers.

59. The ***Transport Layer*** is responsible for managing the flow of packets in each direction that make up a communication between two network devices. As part of this function the transport layer is responsible for splitting the data into packets for transmission and reassembling them into continuous data when they are received. The Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP) are the two

most common transport layer protocols used in the Internet. See the discussions on TCP (¶¶ 110-115), flows (¶ 62) and packets (¶¶ 74-82) below.

60. The ***Application Layer*** is responsible for handling an Internet data flow in a way defined for the specific application the flow is a part of. Applications are the way that people use the Internet. Internet applications most relevant to this case include electronic mail (email) and the world wide web. See below for discussions of these Internet applications.

61. Portions of every packet transferred across the Internet provide support for each of the above layers. See the description of a packet below in ¶¶ 74-82.

***3. Flow***

62. A ***flow*** is a set of packets that are part of a single communication and that are transported from one network node to another network node. While communications are generally bidirectional, flows are unidirectional. The packets that make up a flow are distinguished from other packets when the following five fields in a packet are identical between the packets: the source and destination IP addresses, the protocol field and the source and destination port numbers. This information is often called a ***five tuple*** (or ***5-tuple***). See below for a discussion of packets that includes a discussion of these fields.

#### *4. Transaction*

63. The government's response to the Foreign Intelligence Surveillance Court's Briefing Order of May 9, 2011 defines ***transaction*** as follows:

> *a complement of 'packets' traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device.*[5]

64. The government's use of the term "transaction" is not a common way that the term is understood in Internet communications. Merriam-Webster's definition of "transaction" relating to communications is the more common understanding:

> *a communicative action or activity involving two parties or things that reciprocally affect or influence each other.*[6]

65. But I will adopt the government's definition for the term "transaction" for this report where the term is used in regards to upstream collection. In practice, a "transaction", as defined by the government, appears synonymous with a "flow" as I define the term above in ¶ 62.

66. The NSA also talks about ***multi-communication transactions*** (***MCTs***), which contain more than one individual communication, such as more than one email message, not all of which would be proper candidates for collection on their own:

> *NSA Defendants respond that to their understanding (i) the term "single communication transaction," when used in reference to Upstream Internet collection, meant in unclassified terms an Internet transaction that contained only a single, discrete communication, and (ii) the term "multi-*

[5] Appendix C at 1 (FISC Submission (June 1, 2011)).

[6] *Transaction*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/transaction.

> *communication transaction" meant, in unclassified terms, an Internet transaction that contained multiple discrete communications.*[7]

67. The NSA says that an MCT might consist of, for example, multiple email messages.[8]

68. The NSA says that it is not technically feasible to only collect the individual transactions in an MCT that qualify for collection under the upstream collection program:

> *The NSA's acquisition of MCTs is a function of the collection devices it has designed. Based on government representations, the FISC has stated that the "NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which are to, from, or about a tasked selector."*[9]

69. Also see below at ¶¶ 316-320.

***5. Network***

70. A ***network*** consists of a set of computers and the network links and routers and switches that permit the computers to exchange communications. The Internet is a network of networks.

[7] Appendix D at 13 (NSA Response to Plaintiff's Interrogatory No. 8 (Dec. 22, 2017)).

[8] Appendix E at 15-16 n.17 (FISC Opinion (Apr. 26, 2017)).

[9] Appendix F at 45 (Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* at 40 (July 2, 2014) ("PCLOB Report")).

### *6. Network Node*

71. A ***network node*** is a computer connected to a network. Network nodes include the ***end-systems*** between which communications are exchanged and the network nodes (such as switches and routers) that forward the packets that make up a communication between the end-systems. Such end-systems include user desktop or laptop computers and smartphones as well as computers that provide services to the users such as web servers—for example www.cnn.com and www.wikipedia.org.

### *7. Circuit*

72. In its response to one of Plaintiff's interrogatories, the NSA described a ***circuit*** as follows:

> *NSA Defendants respond that to their understanding a "circuit," within the context of Internet communications, traditionally consists of two stations, each capable of transmitting and receiving analog or digital information, and a medium of signal transmission connecting the two stations. The medium of signal transmission can be electrical wire or cable, optical fiber, electromagnetic fields (e.g., radio transmission), or light. Individual circuits may be subdivided further to create multiple "virtual circuits" through application of various technologies including but not limited to multiplexing techniques.*[10]

73. This description is consistent with the definition for "network link" I provided above in ¶¶ 52-55, with the addition of the nodes at each end of the link. I will adopt the government's definition of circuit for the purpose of this report.

[10] Appendix D at 6 (NSA Response to Plaintiff's Interrogatory No. 2 (Dec. 22, 2017)).

***8. Packet***

74. A ***packet*** is a chunk of a communication. Packets in the Internet can vary in size and are autonomous, meaning that they can be processed independently by devices within the network (explained below). An example Internet packet is shown in the following figure. As explained below, each layer in this figure depicts the corresponding layer within the four-layer model of the Internet, described above in ¶¶ 50-61:

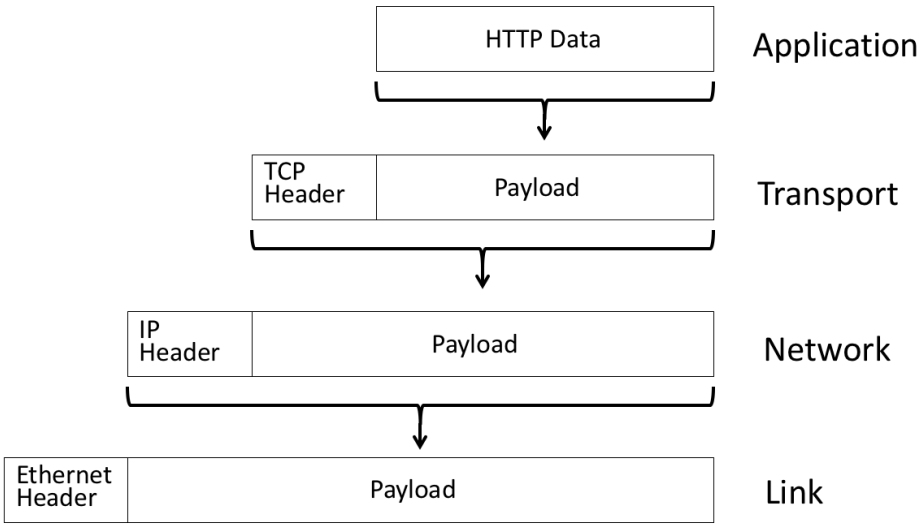



**Figure 8** — Packet format showing web data over Ethernet

75. Figure 7 shows an Internet packet as I described above in the definition of layer. In this case, the figure shows an Ethernet packet that is transporting world wide web (HTTP) data.

76. The lowest pair of boxes represents an Ethernet packet (also known as a ***frame***). The left box is the Ethernet header and the right box is the Ethernet payload, which is the entire IP packet. An Ethernet header is shown in the following figure:




**Figure 9** — Ethernet header

77. The information is transmitted onto the Ethernet starting with the left edge of the figure. The first information transmitted is the link-layer destination address, followed by the link-layer source address, then finally the type field. The link-layer destination address specifies the specific network device on the LAN to which this packet is to be delivered. The link-layer source address contains the link-layer address of the network device that is sending the packet. Finally, the value of x800 in the type field identifies the payload in this Ethernet packet as an IP packet.

78. The IP part of the packet is shown in the two connected boxes above the Ethernet packet in Figure 7. The format of an Internet Protocol (IP) version 4 packet is shown in the following figure (which is the same as Figure 5, above):

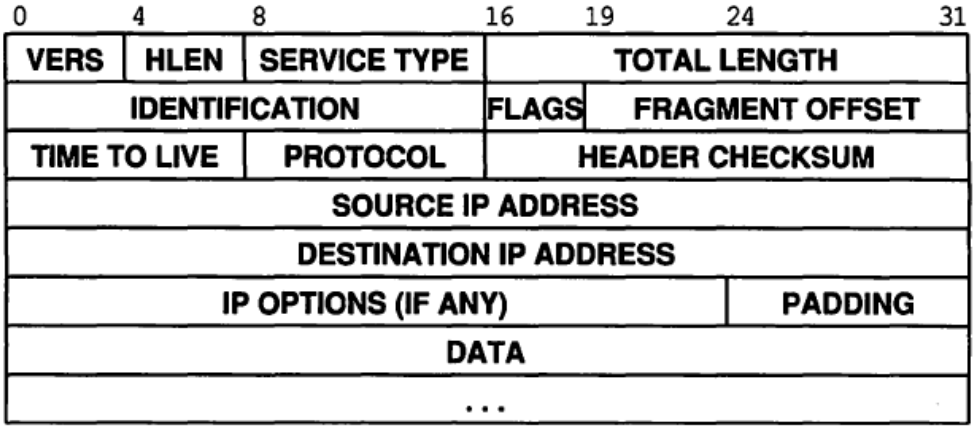



**Figure 10** — IP packet format[11]

79. Information is sent on the Ethernet starting in the upper left box of the figure and continuing, row by row, to the lower right. Figure 10 shows the source and destination IP addresses. These are the addresses described above in the definition of layer as network addresses. See below for a fuller description of IP addressing. In this example case, the protocol field will be set to a value of 6 to indicate that the payload of the IP packet (labeled as "data" in the figure) is a TCP packet.

[11] Comer, *supra* note 3.

80. The TCP part of the packet is shown in the two connected boxes above the IP part of the packet in Figure 7. The format of a TCP packet is shown in the following figure:

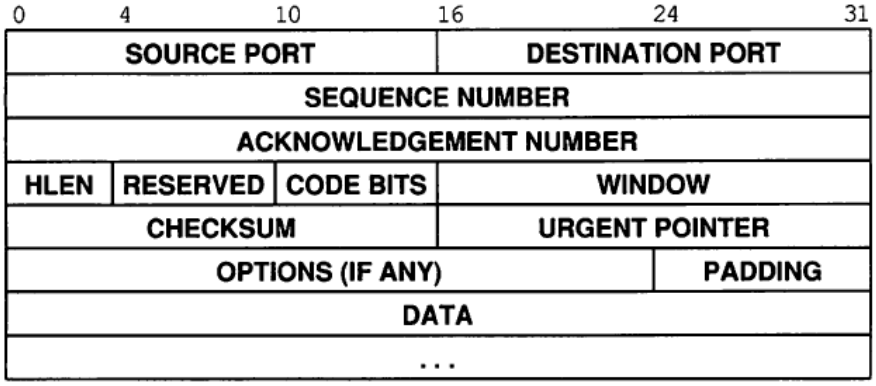



**Figure 11** — TCP packet format[12]

81. Information in a TCP packet is sent following the same pattern as with the IP packet. The only field important for this section of this report is the Destination Port field. Since this example packet is carrying world wide web data, the destination port field will be set to a value of 80 or 443. (See below in ¶¶ 110-115 for a fuller description of TCP.) The value 80 in the destination port field indicates that the payload portion (labeled "data" in the figure) is HTTP (world wide web) information and the value 443 indicates that the payload portion (labeled "data" in the figure) is HTTPS, the encrypted version of HTTP.

82. The HTTP part of the packet is shown as the box above the TCP part of the packet in Figure 8. See ¶¶ 117-124 for a fuller description of HTTP.

[12] Comer, *supra* note 3.

***9. Switch***

83. A ***switch*** is a network node that is connected to two or more network links. A switch receives packets on these network links and forwards each of the packets it receives onto one or more of the other network links based on the destination link-layer address in the link layer of a packet received by the switch. Thus switches are used to forward packets *within* a LAN. Typically there would be an Ethernet switch in some central location on a floor of an office building. Ethernet links would then connect individual desktop computers to the switch.

***10. Router***

84. A ***router*** is a network node that, like a switch, is connected to two or more network links. A router receives packets on these network links and forwards each of the packets it receives onto one or more of the other network links based on the destination Internet address in the network layer of the packet received by the router. Thus a router is used to forward packets *between* LANs.

***11. Mirroring***

85. Some switches and some routers have the ability to make copies of some or all of the traffic sent or received on one network link and send that traffic out of a second network link. This is the copying function Dr. Schulzrinne describes in ¶ 58 of his report.

### *12. Routing*

86. ***Routing*** is the process by which a router in a network decides onto which network link the router should forward a packet it has received in order to get the packet closer to the packet's destination, where the destination is represented by the destination Internet address in the received packet. Routers decide where to forward the packets they receive in one of three ways:

a. Routers can be manually configured to determine a forwarding decision.

b. Routers can exchange information with other routers to build a dynamic database of information on which to make forwarding decisions.

c. Routers can be configured to use a combination of the two.

87. See ¶¶ 175-199 for additional discussion on routing in the Internet.

### *13. Internet Protocol*

88. The ***Internet Protocol*** is defined by a set of standards that specify the format of packets in the Internet and how the packets are to be generated by the sender of the packet and processed by the receiver of the packet to enable the transfer of communications between nodes in the Internet. See below for a fuller description of the Internet Protocol.

### *14. Internet Service Provider (ISP)*

89. An ***Internet service provider*** (***ISP***) is a company that provides connectivity between a set of customers and the rest of the Internet. The customers could be individuals using smartphones or computers in their own homes or in enterprises that run their own Internet Protocol-compatible enterprise networks. ISPs range from ones

that service a small part of a small town to ISPs that service customers around the globe. See below for a fuller description of ISPs.

***15. Proxy***

90. A ***proxy*** is a network node that serves as a forwarding agent for communications between other Internet nodes. In most cases a proxy rewrites the IP packet header information in the communication such that the proxy appears to be the origin or destination of the communication rather than the network node the proxy is serving.

***16. Tunnel***

91. A ***tunnel*** is a type of virtual network link used to establish what appears to be a direct network link between network nodes by transporting packets flowing between the two nodes within other packets. The transporting packets may traverse multiple network nodes, both switches and routers, on a path between the two tunnel nodes. In many cases the packets being transported over a tunnel are encrypted. An example of an encrypted tunnel is a ***virtual private network*** (***VPN***) that a traveler uses to connect his or her laptop computer in a coffee shop back to his or her employer's enterprise network. Such VPNs are used to protect communications between the laptop and an enterprise network from eavesdropping and to protect communications between enterprise networks.

***17. Metadata***

92. ***Metadata*** is information about a communication that is not within the communication itself. Examples of metadata include the source and destination IP addresses for a communication, and the time the communication starts and ends.

### C. The Key Internet Protocols

93. In the following section, I will describe the key protocols that are used in the Internet today (i.e., the Internet Protocol Suite) and several of the most common ***application protocols*** used on the Internet (i.e., HTTP/HTTPS for web access and IMAP/SMTP for email).

#### *1. The Internet Protocol Suite*

94. Kahn and Cerf defined more than just the format of IP packets and how IP packets were created and processed; they defined a suite of protocols. The suite includes the Internet Protocol itself as well as a few "higher-level" protocols that use IP packets for transport and that define ways to support specific types of communication between network nodes. I will describe the Internet Protocol more fully and then mention two of those higher-level protocols below.

##### a. The Internet Protocol (IP)

95. As mentioned above, there is a defined format for IPv4 packets, which is shown in the following figure which I repeat from above to make it convenient for the reader:

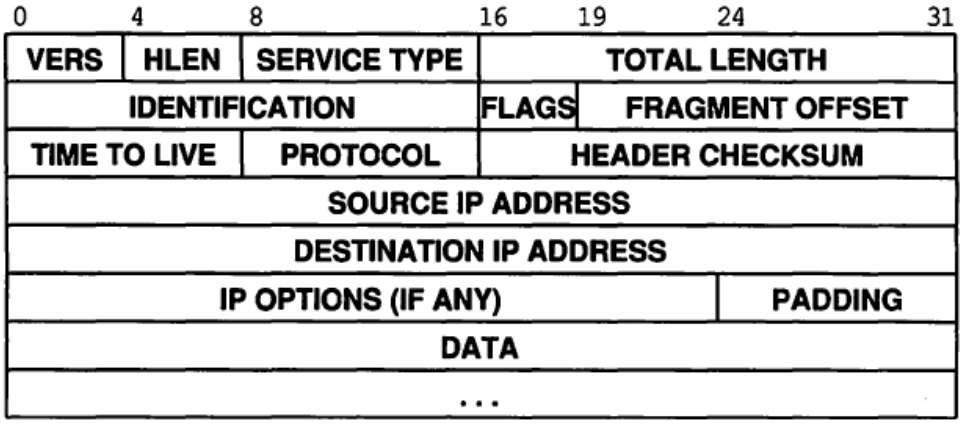


**Figure 12** — An IP packet[13]

96. The first part of an IP packet is known as the ***IP header***. The IP header comprises the fields shown in Figure 12 through the optional "padding" field (that is, the first six rows). In addition to the source and destination IP address fields in the IP header that I have already described, there is one other field in the IP header that is relevant to this case. The "protocol" field is used to indicate what higher-level protocol is using the IP packet for transport. When an IP packet is created and sent by a network node, for example by a user's personal computer, the node will put its own IP address into the Source IP Address field and the IP address of the node that it wants to send the packet to into the Destination IP Address field. The computer will also put a value in the protocol field so that the receiving node will know what to do with the packet when it is received.

i. IP addresses

97. An ***IP address*** is a number that is used to identify a particular network device on a network that is using the Internet Protocol for communication. IPv4 addresses are 32-bits long and can identify about 4 billion individual network devices. IPv6 addresses are 128-bits long and can identify trillions of trillions of individual network devices. I will focus on IPv4 in this report, but when I use the term "IP address" it should be taken to mean the type of IP address used in the version of IP in use in the particular situation.

[13] Comer, *supra* note 3.

98. An IPv4 address is represented as a set of 4 numbers separated by periods. For example, the IP address for the web server I run in my house is 173.166.5.74 and, as of this writing, one of the IP addresses of the University of Oxford's website, www.ox.ac.uk, was 129.67.242.155.

ii. Viewing IP header information

99. The IP header information is visible throughout the path a packet takes through the Internet. Except in the cases where the IP addresses are modified in transit, (I will mention some cases of this below), the actual source and destination of each packet in the Internet can be determined by just looking into its IP header.

100. The IP header information must be unencrypted even when the information being transported is encrypted. To transport an email message, for example, the IP header information for the packets that make up the email must be unencrypted so that the routers forwarding the packets know where to send them and so that the receiving node knows what to do with them.

101. Information beyond the IP addresses and protocol can be observed in IP packets by looking further into the packet to get the port numbers and application-specific information. The function of looking into packets to better understand the application-level communications they transport is often referred to as "deep packet inspection (DPI)." I will discuss DPI further below.

iii. Sizes of IP packets

102. IP packets in the Internet are variable in length. They range from a minimum size of 68 bytes long to 1,500 bytes long. The 1,500 byte limit derives from the maximum packet size that is supported on Ethernet, the most common type of local

physical network. A 1,500 byte packet is big enough to transport the body of an email message of up to a thousand characters—about 200 four-letter words (including spaces between each word).

iv. Multiple packets in a communication

103. A particular communication will be broken up into multiple packets by the sending node if the communication cannot fit in a single large (1,500 byte) packet. The packets are reassembled into the communication by the destination node in order to recover the originally transmitted message.

104. The reassembly must be done by the destination node because the Internet does not guarantee that all of the packets that make up a particular communication will be present at any other place along the path from sender to receiver. Two features of the Internet cause this to be the case:

a. The paths that packets take through the Internet can change at any time, even between successive packets in a single communication.

b. The paths packets take are asymmetric, in that packets in a two-way communication traveling in one direction will generally not follow the same path as packets traveling in the opposite direction.

**b. Transport Protocols**

105. As described above in ¶¶ 50-61, ***transport protocols*** are used to break communications into packets and to provide the desired level of reliability. The two transport protocols I will describe here are the User Datagram Protocol and the Transmission Control Protocol. These are the dominant transport protocols currently in general use on the Internet.

i. The User Datagram Protocol (UDP)

106. The ***User Datagram Protocol*** (***UDP***) provides a way to send packets from one network node to another network node over IP packets. Many applications use UDP for transport, including certain voice and video streaming applications, tunneling protocols, and domain name lookups (see ¶ 184 for a description of how to do domain name lookups).

107. UDP information is carried in the "data" portion of those IP packets that make up a communication using UDP as its transport. UDP has its own header as shown in the figure below:

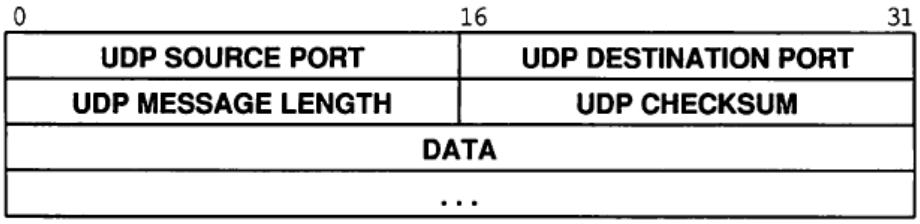



**Figure 13** — The UDP header[14]

108. The destination UDP port field is used to specify the application that is running over UDP. Hundreds of applications have been defined to date, many in "open" standards but quite a few in non-public and proprietary ones.

109. UDP port numbers can range from 1 to 65,535. UDP port numbers 1 to 49,151 are "registered" for use by particular applications. Port numbers between 49,152 and 65,535 are "unassigned" and open for use by any application, although the node that receives a UDP packet using an unassigned port number must have been preconfigured to know what to do with a packet with that unassigned destination port number. Note that

[14] Comer, *supra* note 3.

port number assignments are, in a way, advisory. As long as the two ends of a communication agree on which port numbers to use, any port numbers will work, even port numbers that have already been assigned to specific applications. Thus, by changing the port numbers in use, someone can change the apparent application being used. For example, quite a few applications use ports 80 or 443, the ports nominally assigned to the world wide web, because these ports are often passed by firewalls that would block unassigned ports.

ii. The Transmission Control Protocol (TCP)

110. Whereas UDP is used to just deliver packets from one network node to another without worrying about the rate of transmission or even if the packet in fact makes it to the destination network node, ***Transmission Control Protocol*** (***TCP***) is used to provide a *reliable data stream* between network nodes. TCP is used by most major Internet applications including email, the world wide web, file transfer and the control channel of Internet calling protocols such as Skype. TCP has its own header that is present in all packets in a communication making use of TCP:

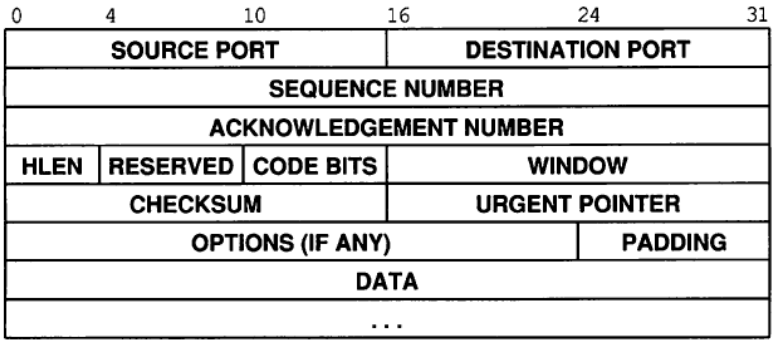



**Figure 14** — The TCP header[15]

[15] Comer, *supra* note 3.

111. Two network nodes can use TCP to create and maintain a two-way communications session, to control the rate of packet transmission as appropriate, and to ensure that all of the information in the session will be reliably delivered.

112. TCP can be used to transport a discrete piece of information such as an email message. It can also be used to support continuous streams of information such as a telephone call, although UDP can also be used to transport information streams, including phone calls.

113. Ports in the TCP header are assigned and used in the same way as ports are used in UDP, except that source ports are required. The set of information in the (1) Source and (2) Destination IP addresses fields and the (3) protocol field in the IP header, along with the information in the (4) source and (5) destination port fields in the TCP header, uniquely identifies packets that are part of a particular TCP communication between two network nodes. As explained in ¶ 62, this information is often called a five tuple (or 5-tuple).

114. The sequence number field in the TCP header is used to ensure that all of the packets comprising a communication have been received and that they are in the correct order. This is important because IP networks do not guarantee that packets will not be lost, duplicated or reordered during their travel though the Internet.

115. The Internet protocol suite includes the Internet Protocol itself plus the transport protocols TCP and UDP as well as other signaling protocols and is frequently referred to as "TCP/IP."

### *2. Application Protocols*

116. UDP and TCP are used to transport packets that implement Internet applications. I will discuss a few of the hundreds of applications that have been defined for the Internet.

#### a. The Hypertext Transfer Protocol (HTTP)

117. The ***Hypertext Transfer Protocol*** (***HTTP***) is used to transport web page content between web servers and web browser software on user computers.

##### i. HTTP commands

118. HTTP consists of a number of plain text commands sent by a web browser to a web server. The basic HTTP commands are shown in the following figure:

| *Command* | *Description* |
|---|---|
| GET | Return the contents of the indicated document. |
| HEAD | Return the header information for the indicated document. |
| POST | Treat the document as a script and send some data to it. |
| PUT | Replace the contents of the document with some data. |
| DELETE | Delete the indicated document. |

**Figure 15** — HTTP commands[16]

119. The HTTP GET command is used to request that the HTTP server return a file to the user's web browser. The GET command includes the name of the requested file. The POST command is used to upload a file to a web server.

##### ii. Encrypted HTTP (HTTPS)

120. An encrypted version of HTTP, referred to as ***HTTPS*** (for "HTTP Secure") was introduced in 1994 by Netscape Communications to support electronic commerce over the Internet. The entire HTTP application layer communication is

[16] Lincoln D. Stein, *How to Set Up and Maintain a World Wide Web Site: The Guide for Information Providers* 49 (1995).

encrypted when using HTTPS. The IP packet and TCP header that HTTPS rides on top of are not encrypted, so an observer can determine that an HTTPS session is running between two nodes identified by the IP addresses in the IP header.

121. It is worth noting that not all encryption used on the Internet is "unbreakable." *See* Schulzrinne Decl. ¶ 42. When properly implemented, modern public standards-based encryption itself is generally considered to be unbreakable. But encryption standards are not enough. The software implementing the encryption standard has to be well designed and bug-free, the systems that make use of the encryption must also be well designed and well implemented, and these systems must be properly and carefully operated for the communications to actually be protected.

122. Not all implementations of HTTPS in use on the Internet today are "unbreakable", and the computers making use of HTTPS are all too frequently compromised because of software bugs or user errors. Once a computer is compromised, it is generally easy to compromise any communications as they are being sent or received by that computer. In addition, some developers decide to create their own encryption protocols and algorithms and most of them turn out to be far from unbreakable.[17] In the cases where the NSA determines that the type of encryption protocol or algorithm being used is weak, it would make sense for the NSA to collect encrypted communications from targeted individuals knowing that, with enough effort, for example, with large amounts of computing power the encryption could be broken. The NSA could also be collecting encrypted communications to subject them to quantum cryptanalysis in the

[17] Joseph Cox, *Why You Don't Roll Your Own Crypto*, VICE: Motherboard (Dec. 10, 2015), https://motherboard.vice.com/en_us/article/wnx8nq/why-you-dont-roll-your-own-crypto.

future. Quantum cryptanalysis, which relies on quantum computers, may make it significantly easier to break certain types of encryption in wide use today. It is not publicly known whether the NSA or any other intelligence agency currently has the capacity to conduct quantum cryptanalysis, but encryption standards bodies have been preparing for a number of years for the possibility that intelligence agencies or malicious actors will. The above factors may help to explain the permissive rules (as discussed in ¶¶ 325-327) for the NSA's collection of encrypted communications under Section 702.

iii. HTTPS Handshake

123. Not all of the HTTP information is hidden when using HTTPS. A single physical web server can be used to support many websites. The web server that I run in my house, for example, supports www.sobco.com, www.sobco.org, www.scottbradner.com, and www.kaybradner.com. Because a single web server may be supporting multiple different websites, a web browser must send the domain name of the website to the web server during the setup phase of an HTTPS session so that the web server knows which website the user wants to access and so that the proper security association can be setup. Since the security association has not yet been set up, the domain name must be sent unencrypted. Thus, HTTPS does not protect the confidentiality of the domain name of the website that is being accessed. For example, an observer would be able to determine that a user had requested a web page from https://en.wikipedia.org, but they would not be able to determine from the HTTPS request that the user had requested the specific web page https://en.wikipedia.org/wiki/Addiction.

iv. IP addresses in HTTP packets

124. There are some cases where the IP addresses in HTTP packets do not accurately identify the original sender of a HTTP packet or its ultimate destination. For example, HTTP proxies are sometimes used in enterprise networks, including hotels, and in some Internet service providers to improve the performance of user's web browsers and to control access to improper websites. HTTP packets sent from all web browsers used by everyone behind an HTTP proxy will have the IP address of the HTTP proxy as the IP Source Address in the header. Likewise, the Destination IP Address in all HTTP packets destined to web browsers that are behind an HTTP proxy will have the IP address of the proxy as their Destination IP Address. There are also cases where there are no proxies or NATs (see below in ¶¶ 173-174) where the IP addresses in the packets identify the sender and receiver of a packet.

**b. Email**

125. As a formal matter, ***electronic mail*** or ***email*** refers to "*a system for sending messages from one individual to another via telecommunications links between computers or terminals using dedicated software*".[18] Email is the third oldest Internet application, behind remote access and file transfer.

[18] *Email*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/email.

i. Email Header Information

126. Individual email messages have a format defined in specifications from the IETF[19]. The start of an email message consists of a series of plain text "headers" that include the names and email addresses of the sender and intended receiver(s) of the message, the date the message was sent, a subject for the message, some information about the path the message took through the Internet which generally includes the IP address of the email server that sent the message, and some information about the format of the body of the message, i.e. the part of the message following the header lines. Very often, an email message will not fit in a single packet. In such cases the header lines will start in the first packet of the communication, but sometimes the header lines will extend into the second packet.

127. An example of some of the entries in an email header are shown in the following figure:

```
From: "Scott O. Bradner" <sob@sobco.com>
Content-Type: text/plain;
        charset=us-ascii
Content-Transfer-Encoding: 7bit
Mime-Version: 1.0 (Mac OS X Mail 11.3 \(3445.6.18\))
Subject: need to reschedule Taveras appt
X-Universally-Unique-Identifier: 78BC10A7-0A77-4C96-96D0-9C394F696E8E
Message-Id: <40D15B68-D405-46CC-A511-24F809988261@sobco.com>
Date: Thu, 5 Apr 2018 09:52:37 -0400
To: "Cheryl F. Chapman" <cfc@sobco.com>
```

**Figure 16** — Sample email header

128. The above is the header portion of an email message from me to my wife. The "From:" header line provides my name and email address as the sender of the email

[19] See, e.g., *Internet Message Format*, Qualcomm Inc., Network Working Group (October 2008), https://www.ietf.org/rfc/rfc5322.txt.

message. The "To:" line shows my wife's name and email address as the destination of the message. The "Subject:" line shows what I said was the subject of the message. The "Date:" line shows the time I sent the message. Finally, the "Message-Id:" line is a unique identifier for this particular message. The body of the message that follows the header lines could be plain text, one or more photos, one or more pieces of video or music, a spreadsheet, a Microsoft Word document, a pdf, or any one of dozens of other things. In addition, the body of an email message may or may not be encrypted.

ii. Email Servers

129. As a general rule, email messages do not go directly from a sender to a receiver. Instead, there could be an email server at the sending end, and there is almost always an email server on the receiving end. Email servers maintain databases of sent and received email messages for each of their users.

130. Email users access their email servers by using a web browser or by using a piece of software called a "mail user agent" on their own computer. With the web browser or mail user agent, an email user can create and send email messages and also read any email he or she might have received.

131. Many large commercial email services, such as Hotmail and Gmail, are accessed via web browsers. Some large commercial email services, for example Microsoft Exchange, are accessible via web browsers but are also accessible via their own special mail user agents. In addition, some computers come with their own generalized mail user agents that can connect to multiple commercial email services. One example of the latter is the Mail program that comes with Apple computers. This is the mail user agent that I use. I use the Apple Mail application to connect to Harvard's Microsoft Exchange server, Google Gmail and to the email server that I run in my house.

132. Mail user agents generally download all new email messages to the user's computer whenever the mail user agent is started. Thus, when an email user turns on their laptop after a few days "off line" a burst of email messages can be transferred to the laptop. Such bursts will often be done over a single communications session between the email server and the mail user agent, resulting in multiple individual email messages in the same communication. Some web mail implementations do the same type of burst fetch of unread email. This behavior may be an example of what the NSA has called a multi-communication transaction (MCT) since the NSA says that an MCT can consist of multiple email messages.[20] (See above at ¶¶ 66-68 and below at ¶¶ 316-320.)

133. There are a number of IETF protocols that define the communications between email servers and between email servers and mail user agents. In addition, there are some proprietary protocols. I will discuss the two most common, standards-based protocols:

a. ***Simple Mail Transfer Protocol*** (***SMTP***): used between email servers and between email servers and some mail user agents

b. ***Internet Message Access Protocol*** (***IMAP***): used between most mail user agents and email servers.

iii. Simple Mail Transfer Protocol (SMTP)

134. The Simple Mail Transfer Protocol (SMTP) is used to transport email messages between email servers and, less frequently, between mail user agents and email servers. The SMTP protocol defines a ***handshake*** that is used to start up a session to transfer an email message. A sample of an SMTP handshake used when a user is sending

[20] Appendix E at 15-16 n.17 (FISC Opinion (Apr. 26, 2017)).

an email message is shown in the following figure, where "S" identifies text sent by the email server and "C" identifies text sent by the email client:

```
S: 220 Beta.GOV Simple Mail Transfer Service Ready
C: HELO Alpha.EDU
S: 250 Beta.GOV

C: MAIL FROM:<Smith@Alpha.EDU>
S: 250 OK

C: RCPT TO:<Jones@Beta.GOV>
S: 250 OK

C: RCPT TO:<Green@Beta.GOV>
S: 550 No such user here

C: RCPT TO:<Brown@Beta.GOV>
S: 250 OK

C: DATA
S: 354 Start mail input; end with <CR><LF>.<CR><LF>
C: ...sends body of mail message...
C: ...continues for as many lines as message contains
C: <CR><LF>.<CR><LF>
S: 250 OK

C: QUIT
S: 221 Beta.GOV Service closing transmission channel
```

**Figure 17** — SMTP startup handshake[21]

135. The SMTP handshake includes the message sender's email address (Smith@Alpha.EDU) and the email address of the intended recipients of the message (Jones@Beta.GOV, Green@Beta.GOV and Brown@Beta.GOV). Even if parts of the body of an email message are encrypted, the SMTP handshake is not, although the entire SMTP exchange could take place within an encrypted connection, in which case the

[21] Comer, *supra* note 3.

SMTP handshake would be encrypted, and any encrypted parts of the email message would be doubly encrypted.

(1) SMTP Metadata

136. The sender's and receiver's email addresses as well as the date and time that the mail was sent and the IP addresses of email servers would all be considered email metadata. This metadata is included in the SMTP startup handshake as well as in the email headers.

(2) IP addresses in email packets

137. The IP addresses in the packets exchanged between email servers identify the email servers but often have no relationship to the actual sender or receiver of an email message. Some mail user agents are configured to use SMTP to send email messages directly to the email server associated with the intended recipient. In such cases the source IP addresses in packets sent to the email server will identify the computer that is running the mail user agent.

iv. Internet Message Access Protocol (IMAP)

138. IMAP defines the formats and meanings of the messages exchanged between a mail user agent and an email server. In general, these messages are used to maintain a copy of the email user's portion of the email server on the user's own computer.

139. As mentioned above in ¶ 132, when a mail user agent connects to an email server using IMAP, all new messages will be downloaded to the user's computer in a batch.

140. In my own case, the mail user agents on my laptops, desktops and smartphone are configured to use IMAP to connect to the email server I run in my house

when sending email. The IP addresses in the packets my email server sends will be the IP address of that server, no matter where in the world I might be. Similarly, packets comprising an email message sent by a Gmail user will include the IP address of the Gmail server in their source address field no matter where the Gmail user is actually located.

**c. Telephone Calls**

141. While it's not part of this case, a number of NSA documents say that the NSA collects telephone calls and that telephone numbers are one type of selector that is used to target Internet transactions, under the upstream collection program. Since almost all international telephone calls are currently transported over the Internet using the IETF-developed Session Initiation Protocol (SIP), it is easy to include them in the upstream program. SIP has HTTP-like headers that are used to specify the source and destination telephone numbers and the IP addresses between which the audio portion of the phone call will flow.

***3. Plain Text in Application Protocol Headers***

142. Many Internet applications, including the applications mentioned above, include "plain text" (i.e., not encrypted and not otherwise encoded) fields in their headers. Such fields can be searched for specific strings such as a name or email address or other string that might indicate that a packet is part of a communication that is of interest, even if portions of the underlying communication are encrypted. These text fields will sometimes be entirely in the first packet of a flow of packets that makes up a communication but often do extend into successive packets.

### *4. Number of Packets in a Communication*

143. As described above in ¶ 49, a particular communication between nodes over the Internet is broken up into packets for transmission. The number of packets in any one communication varies greatly. The sample email message between me and my wife shown above was short enough to be contained within a single packet (although the SMTP handshake that would've preceded the email when sent between email servers would have required an exchange of multiple separate packets), but I sent an email message to a colleague recently that contained two image files. The message was 2.7 million bytes (MB) long so it took at least 1,860 packets to transport that message. I frequently send email messages that are 10 MB or more. It takes thousands of packets to transport each of those messages.

144. I ran a command on the router that interfaces the network in my house to my Internet service provider that asked for statistics on the number of packets in a flow. The results of that command are shown in the following figure:

| Protocol | Total Flows | Flows /Sec | Packets /Flow | Bytes /Pkt | Packets /Sec | Active(Sec) /Flow | Idle(Sec) /Flow |
|---|---|---|---|---|---|---|---|
| TCP-Telnet | 14222087 | 3.3 | 1 | 43 | 4.1 | 1.0 | 15.5 |
| TCP-FTP | 113213 | 0.0 | 2 | 60 | 0.0 | 1.9 | 14.4 |
| TCP-FTPD | 13567 | 0.0 | 1 | 40 | 0.0 | 0.0 | 15.4 |
| TCP-WWW | 2967948 | 0.6 | 81 | 846 | 56.1 | 24.5 | 8.2 |
| TCP-SMTP | 3454819 | 0.8 | 7 | 261 | 5.9 | 2.0 | 5.7 |
| TCP-X | 328461 | 0.0 | 1 | 40 | 0.0 | 0.0 | 15.4 |
| TCP-BGP | 14779 | 0.0 | 1 | 40 | 0.0 | 0.0 | 15.4 |
| TCP-NNTP | 8667 | 0.0 | 1 | 40 | 0.0 | 0.0 | 15.4 |
| TCP-Frag | 174 | 0.0 | 1 | 460 | 0.0 | 0.1 | 15.4 |
| TCP-other | 50802851 | 11.8 | 20 | 432 | 245.9 | 4.5 | 9.1 |
| UDP-DNS | 324539 | 0.0 | 2 | 63 | 0.1 | 0.7 | 15.4 |
| UDP-NTP | 597821 | 0.1 | 1 | 76 | 0.1 | 0.0 | 15.4 |
| UDP-TFTP | 28463 | 0.0 | 1 | 42 | 0.0 | 0.0 | 15.4 |
| UDP-Frag | 36396 | 0.0 | 1 | 540 | 0.0 | 0.0 | 15.5 |
| UDP-other | 68219772 | 15.8 | 1 | 224 | 17.6 | 0.3 | 15.4 |
| ICMP | 1701074 | 0.3 | 5 | 63 | 2.2 | 9.4 | 15.4 |
| IPv6INIP | 14 | 0.0 | 1 | 80 | 0.0 | 0.0 | 15.4 |
| GRE | 57855 | 0.0 | 2111 | 209 | 28.4 | 29.1 | 15.3 |
| IP-other | 451 | 0.0 | 1 | 53 | 0.0 | 0.0 | 15.5 |
| Total: | 142892951 | 33.2 | 10 | 459 | 360.9 | 2.5 | 12.8 |

**Figure 18** — Average flow lengths in my home router

145. The printout shows the statistics since the router was last rebooted a few years ago. The results show that the average length of the email messages that I sent or received over the past few years was 7 packets (TCP-SMTP) and the average length of my web sessions over the same time period was 81 packets (TCP-WWW).

146. I do not think that these statistics are necessarily representative of general Internet traffic, but they do show that much Internet traffic consists of communications comprising multiple packets.

### D. Other Features of the Internet and its Architecture Relevant to this Case

147. In the following section, I will describe other features of the Internet and its architecture that are relevant to this case, including the general structure of the Internet, the role of Internet Service Providers, the way in which networks comprising the Internet connect to one another, the meaning of the "Internet backbone," the undersea fiber optic cables that connect the U.S. to the rest of the world, and the way that packets are routed on the Internet.

#### *1. Internet Architecture*

148. There is no fixed architecture to the Internet. Each customer and service provider is free to design and operate their network or networks in any way they want as long as they are able to transport IP packets along a path from the packet source to the packet destination. Each network operator is also free to interconnect their networks with networks run by other network operators in any way that the two operators agree to, as long as they can properly transport IP packets between the networks.

149. The result is that the Internet structure appears almost random as shown in the following figure from the Opte Internet mapping project:

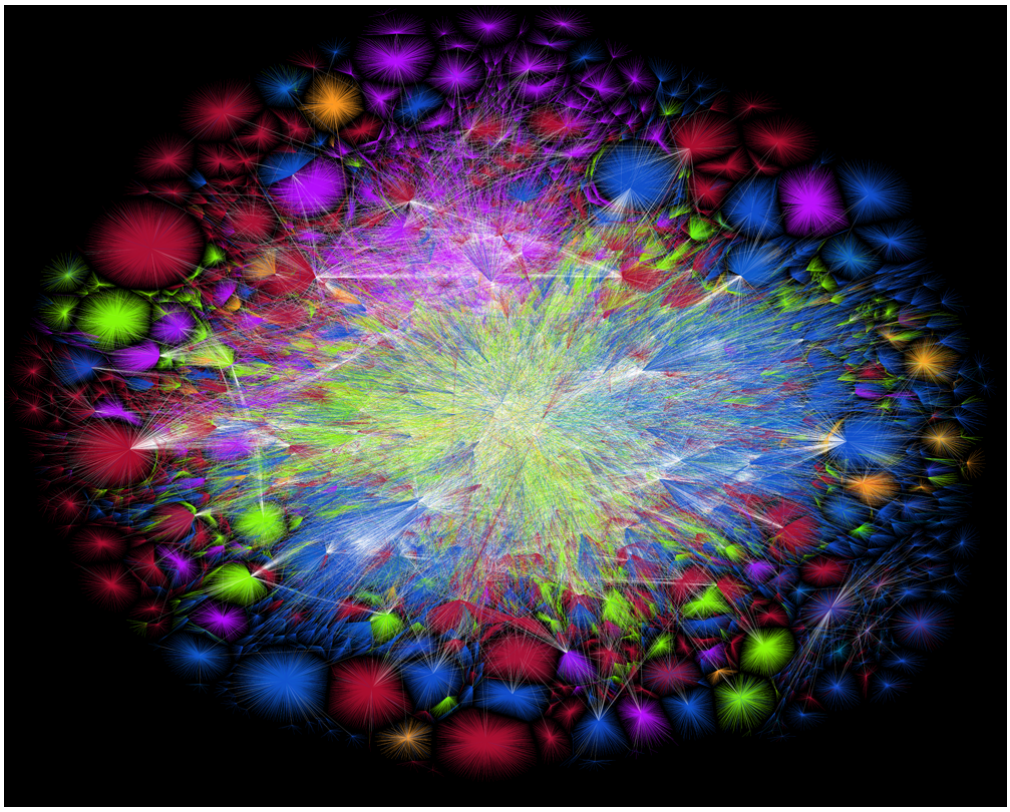


**Figure 19** — The Internet[22]

### *2. Internet Backbone*

150. One of the terms used in this case is "the Internet backbone." Once upon a time, between 1983 and about 1990, it was easy to define the Internet backbone in the U.S. In 1983 it was the ARPANET. The ARPANET was the only nation-wide network that was being used to interconnect other networks, so it was "the Internet backbone." By 1990, the ARPANET had been joined by the NSFNet and the first few commercial ISPs. But there were very few of these ISPs that were nation-wide, so it was reasonable

[22] The Internet 2015, The Opte Project (July 11, 2015), http://www.opte.org/the-internet.

to say that the Internet backbone consisted of the long distance connections in the ARPANET, NSFNet and those ISPs that provided nation-wide service.

151. Since then the growth of ISPs of all sizes and the end of the ARPANET and NSFNet have painted an increasingly more complex picture, to the point that today it is not possible to isolate a single backbone for the U.S. Internet, much less the global Internet. The term "Internet backbone" is one that shows up in the popular press from time to time, but my experience is that experts in the field tend not to use that term. Occasionally, I have seen reference to the "Internet backbones" (plural), referring to the largest ISPs, but more often I've seen references to "ISP backbones", not to an Internet backbone. In an ISP, the backbone is the set of high-speed lines that interconnect routers in different parts of the ISP's geographic footprint.

152. The NSA has provided one interrogatory response and two admissions in regard to their use of the term "Internet backbone":

a. *NSA Defendants respond that to their understanding the Internet backbone is no longer well defined due to the growth of direct peering arrangements, but may be understood as the principal high-speed, ultra-high bandwidth data-transmission lines between the large, strategically interconnected computer networks and core routers that exchange Internet traffic domestically with smaller regional networks, and internationally via terrestrial or undersea circuits.*[23]

b. *NSA Defendants respond that yes, the Internet backbone includes but is not limited to international submarine telecommunications cables that carry Internet communications.*[24]

[23] Appendix D at 18 (NSA Response to Plaintiff's Interrogatory No. 12 (Dec. 22, 2017)).

[24] Appendix H at 6 (NSA Response to Plaintiff's Request for Admission No. 3 (Jan. 8, 2018)).

c. *NSA Defendants respond that yes, the Internet backbone includes but is not limited to high-capacity terrestrial telecommunications cables that carry Internet communications within the United States.*[25]

153. In summary, the government's definition of the Internet backbone includes (1) the high-speed circuits (network links) and routers that are used to interconnect ISPs, (2) the circuits in the undersea cables that connect the U.S. with other countries, and (3) the high speed terrestrial network links (circuits) within the U.S and between the U.S. and other countries. The latter two may be network links between ISPs or within an ISP. I will adopt the government's definition for this report.

154. As stated above in ¶ 70, the Internet is a network of networks. Some of these networks are very small, like the one in my house, and some are very large such as AT&T's IP network, which spans the globe. These networks include customer networks and service provider networks. Each of these millions of networks is under its own management—there is no central manager for the Internet.

### *3. Internet Service Providers (ISPs)*

155. The purpose of service provider networks, known as Internet service providers (ISPs), is to provide "the Internet" to the customer networks that purchase Internet connectivity from the ISP. Each ISP itself consists of multiple interconnected networks. ISPs connect to their customer networks through a link between an IP router in the ISP network and a switch or router in the customer network.

[25] Id. (NSA Response to Plaintiff's Request for Admission No. 4 (Jan. 8, 2018)).

156. According to broadbandnow.com, an Internet site providing information to people looking for ISPs in their area, there are over 2,600 ISPs in the U.S.[26] The ISPs range in size from the big carriers (such as AT&T Wireless and Verizon Wireless, which offer services in all 50 states plus some territories), to the large cable TV companies (which offer ISP service in as many as 40 states), to very small ISPs (such as Surge Communications, which offers Internet services in two just zip codes).

157. For example, Comcast offers its Xfinity Internet service in parts of 40 states. The Xfinity coverage is shown in the following figure:

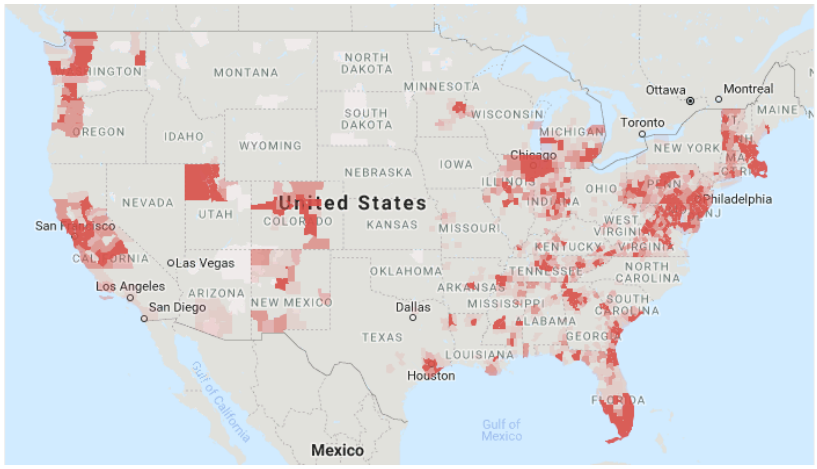



**Figure 20** — Xfinity coverage[27]

[26] *Internet Providers in the U.S.*, Broadband Now, https://broadbandnow.com/All-Providers.

[27] *Xfinity From Comcast Availability Map*, Broadband Now, https://broadbandnow.com/XFINITY (last updated Dec. 1, 2018).

158. A small ISP such as Orca Communications has a still smaller service area, in this case a small part of the southwest coast of Oregon:




**Figure 21** — Orca Communications service area[28]

### a. Address assignments for ISPs

159. Larger ISPs are assigned ranges of IP addresses by one of five Regional Internet Registries (RIRs), each of which is responsible for a part of the globe. The ISPs use the assigned addresses for their own networks, and they subassign some of the addresses to their customers for use in the customer's own networks.

160. Over the last few years a commercial market has developed for the right to use blocks of IP addresses.[29] Individual ISPs or companies can purchase the right to use a block of addresses from someone who currently has that right and then register the

[28] *Orca Communications Availability Map*, Broadband Now, https://broadbandnow.com/ORCA-Communications (last updated Dec. 11, 2018).

[29] Paul McNamara, *MIT Selling 8 Million Coveted IPv4 Addresses; Amazon a Buyer*, Network World (Apr. 21, 2017), https://www.networkworld.com/article/3191503/internet/mit-selling-8-million-coveted-ipv4-addresses-amazon-a-buyer.html.

block with one of the RIRs. The addresses do not have to be used in the same geographic area as they were being used before they were purchased.

#### *4. ISP Interconnection*

161. Because no one ISP connects to all of the customer networks that make up the customer network part of the Internet, ISPs must interconnect with other ISPs to get connectivity to the customer networks they do not directly serve. Each ISP decides on its own how to interconnect with other ISPs to get full Internet connectivity.

162. As a general rule, similarly sized ISPs interconnect with each other with little or no fees exchanged for the interconnection. This type of interconnection is known as ***peering***. Small ISPs must become the customers of larger ISPs in order to be able to interconnect with the larger ISP. The smaller ISP must pay for the interconnection, as any customer must. In general, the interconnections any one ISP maintains are considered proprietary information.

163. ISPs interconnect with other ISPs, either as customers or as peers, through private interconnections and through Internet exchange points.

164. Private interconnections are direct links from a node in one ISP's network to a node in another ISP's network. When large ISPs peer with other large ISPs, they do so at multiple geographically dispersed locations to ensure that traffic between the ISPs can be as distributed as the traffic sources or destinations are, and to ensure reliability through redundancy. For example, AT&T's peering policy requires a minimum of 6 peering points.[30] Large ISPs that peer with multiple other large ISPs are sometimes referred to as ***Tier 1 ISPs***. The ISPs generally considered to be Tier 1 ISPs in the U.S.

[30] *AT&T Global IP Network Peering Policy*, AT&T Business, https://www.corp.att.com/peering.

include AT&T, Verizon, Sprint, Century Link and Level 3. Tier 1 ISPs in Europe include FranceTelecom, Telefonica and Deutsche Telecom.[31]

165. An ***Internet exchange point*** (known as an ***IX*** or an ***IXP***) is a node, usually an Ethernet switch, which has links to nodes in multiple ISPs. Each ISP connected to the exchange point can use the exchange point to interconnect with any other ISP connected to the same exchange point subject to bilateral agreements between the ISPs. The operator of the exchange point need not be a party to any agreement between ISPs to exchange traffic.

166. A single ISP, particularly the large ones, can be connected to multiple Internet exchange points, sometimes in multiple countries or even continents[32]

***5. Customer Networks***

167. Customer networks in the Internet include the small ones such as the one in my house, as well as much larger networks such as the Harvard University's network, Google's internal network and the network at the U.S. Department of Agriculture. Most customer networks themselves consist of many interconnected individual networks.

168. The individual networks that make up a customer network might consist of one or more links, such as physical Ethernet links, interconnected with one or more switches or it might just consist of a single WiFi (wireless) network. The different individual networks that make up a customer network are interconnected with IP routers. For example, I have a physical Ethernet network with multiple Ethernet switches and two

[31] *Who Are the Tier 1 ISPS?*, Dr. Peering International, http://drpeering.net/FAQ/Who-are-the-Tier-1-ISPs.php.

[32] For example, see the list of the exchange points the Australian ISP Telstra peers at: Telstra (International), PeeringDB, https://www.peeringdb.com/net/1459.

WiFi networks in my house. These networks are connected together through an IP router, which I manage.

169. Harvard's network consists of a few hundred separate physical Ethernet networks, each consisting of Ethernet links to individual computers and Ethernet switches to interconnect the Ethernet links. The Harvard network also includes a few dozen WiFi networks. The individual Ethernet networks and the individual WiFi networks are interconnected with many IP routers. Google's internal network spans the globe and consists of an unknown (to me) number of individual networks interconnected through routers.

170. Each individual network in a customer network is assigned its own range of IP addresses to be used by the nodes, such as users' computers attached to that network. Generally, the overall customer network is assigned one or more larger blocks of IP addresses and the individual networks are assigned sub parts of the larger blocks.

**a. Address assignments for customer networks**

171. Most residential or small enterprise customer networks do not have fixed IP addresses on the Internet. Instead they use one or more IP addresses assigned by their ISP that may change from time to time. Larger enterprises can obtain fixed address assignments directly or, for an extra fee, from their ISPs. With some exceptions, networks that are not assigned fixed IP addresses cannot support Internet services such as email servers or web servers.

***6. Customer Network Interconnection***

172. As a general rule with some exceptions, customer networks do not interconnect directly with other customer networks. Instead customer networks connect to ISP networks to get Internet connectivity, including connectivity to other customer

networks. Customers expect to get access to the whole Internet when they purchase Internet service from an ISP.

#### *7. Network Address Translators (NATs)*

173. ***Network address translators*** (***NATs***) are network nodes that sit on the edge of an individual network, a group of networks or even a whole customer network. Their purpose is to translate the IP addresses in the header of an IP packet and the port numbers in the TCP or UDP header such that all of the network nodes on the network appear to have the same IP address. By sharing IP addresses in this way, NATs reduce the demand for the somewhat limited number of IPv4 addresses, and they can hide the internal structure of a network from observers outside of the network, which is seen as a security advantage.

174. But an effect of NATs is that individual computers whose packets pass through a NAT do not have separate IP addresses; they all have the same IP address that was assigned to the NAT, so the communications cannot be distinguished merely by looking at the IP addresses in the packets that make up the conversation.

### E. Routing in the Internet

175. Networks comprise one or more network links interconnected with switches. Networks are connected to other networks through routers.

176. As described above in ¶¶ 71, 84, the network nodes that are used to connect one network to another in the Internet are called routers. This is the case within a customer network, within an ISP network, between a customer network and an ISP network, and between ISPs.

177. For routers to know where to forward packets, they must understand the topology of a relevant part of the network. They gain this understanding by exchanging information with other routers within the name network. The same is true for the routers used to interconnect ISPs—they exchange information so that they can understand the Internet topology well enough to know where to forward packets they receive.

178. Routing protocols define the mechanisms the IP routers use to exchange this topology information. IP routers within a customer network or within an ISP network use a type of routing protocol designed to be used where all the IP routers are run by the same organization such that information from them can be trusted. Such a routing protocol is called an ***Interior Gateway Protocol*** (***IGP***). The two most common IGPs are Open Shortest Path First Routing Protocol (OSPF) and Intermediate System to Intermediate System Routing Protocol (IS-IS).

179. The routing protocol used between ISP networks and other ISP networks or between ISP networks and some of their larger customers is called an ***Exterior Gateway Protocol*** (***EGP***). The only EGP in current use in the Internet is Border Gateway Protocol version 4 (BGP4). ISPs do not generally run a routing protocol between themselves and their customer networks unless the customer has connected their network to multiple ISPs. In such cases, BGP4 is used.

180. Unlike with IGP routing protocols, EGPs operate in an environment where the different routers are operated by different organizations, and an ISP needs to be able to define the level of trust it wants to have in particular information from particular other ISPs or from their customers. Thus, BGP4 has an extensive set of mechanisms to let the operators of routers configure just what information they want to accept from other

routers and what information they want to provide to other routers. The configuration of these mechanisms in a router is done by the router operator. There are no general rules as to what the configuration should be.

### *1. Autonomous System (AS)*

181. A set of routers under common administrative control, such as the routers within a customer network or within an ISP, are assigned an ***Autonomous System number*** for identification. For example, many of the routers at Harvard are assigned AS 11. AS numbers are used by routing protocols as a way to refer to a part of a network or to a whole network such as an ISP.

### *2. Routing an IP Packet*

182. I will now walk through the process by which an IP packet is transported across the Internet, taking as an example my connecting to a web server.

183. In the first step, I type a URL which specifies a particular resource, such as a picture, on a specific website into the window at the top of my web browser, or I click on a link that specifies the same resource. I will use the website for the University of Oxford in England (www.ox.ac.uk) as an example website.

184. For my computer to be able to send a packet containing an HTTP request to www.ox.ac.uk, the computer needs to find out what IP address has been assigned to www.ox.ac.uk. This address is needed so it can be put in the destination IP address field of the packets my computer wants to send to www.ox.ac.uk. Computers use the ***Domain Name System*** (***DNS***) to convert the domain name in the URL into an IP address. At the time of this writing, one of the IP addresses for www.ox.ac.uk was 129.67.242.154.

185. My computer then creates a packet containing the HTTP command my browser wants to execute, likely a GET command, and puts the IP address of www.ox.ac.uk in the destination IP address field in the packet. My computer also puts its own IP address into the source IP address field in the packet. Then, using link-layer addressing, my computer sends the packet to my local router.

186. My local router then looks up the destination IP address in the router's ***routing database*** (also called a ***routing table***). This is the database maintained by the routing protocol. Using the information in the routing database, my local router determines which router the packet needs to go to next on its way toward the web server.

187. In general, my local router's routing table will not have an entry for the specific range of IP addresses that includes the IP address for www.ox.ac.uk. This is because there are many millions of such address ranges and my local router does not have the memory space or processing power to keep track of them all. Instead my local router, after determining that it does not have an appropriate entry in its routing table, uses a ***default route*** configured into the router to identify the ***next-hop router***. Using link-layer addressing, my local router then forwards the packet to that "next-hop router".

188. As a general rule, unless specifically configured otherwise, a router will try to find the "best" next-hop router where the determination of "best" is based on the "cost" of sending a packet through that next-hop router to the destination.

189. In an IGP, cost is generally determined by the number of routers the packet will need to traverse within a customer or ISP network in combination with the speed of the links between the routers.

190. In an EGP, cost is generally based on the number of ISPs (identified by their AS numbers) that the packet will need to traverse across the Internet to reach a destination. I say "generally" because the operator of the router can modify the router's configuration so as to determine the criteria. ISP operators configure the routers they use to connect to other ISPs to filter the routing information they accept from the other ISPs and the routing information they send to those ISPs. ISP operators do this to reject known bad routing information, to prefer next-hop routers in ISPs they have peering contracts with, to prefer some next-hop routers for load balancing reasons, and for a number of other operational reasons. (Dr. Schulzrinne's declaration states that a router may route packets to avoid congested connections. No IGP or EGP routing protocols currently in use on the Internet take "congestion" into account in routing packets. *See* Schulzrinne Decl. ¶ 40. That said, some ISPs do manually reroute traffic to avoid overloaded links.)

191. The next-hop router performs the same type of address lookup process to determine the router that is the next-hop from its point of view.

192. This process continues, hop by hop, until a router recognizes that the address is one on a link directly connected to that router. When a router recognizes this, it uses link-layer addressing to forward the packet to the web server.

193. The decision as to the next-hop router can change at any time based on the most up-to-date information in the routing table in the router, so the next packet in my message to www.ox.ac.uk could be sent to a different next-hop router. I will discuss routing table volatility in the next section.

### *3. Volatility of Routing Information*

194. The Internet today consists of millions of network links and millions of nodes, including switches and IP routers. Changes in state may not occur all that often in each one of these routers and links, but with millions of routers and links, each of which are subject to failures, the overall rate of state change can be significant. Each of these state changes can result in a routing update propagated throughout the Internet. Each of the routers receiving the update updates its own routing, which may produce a change in the next hop a particular packet may be forwarded to and, thus, the links a packet will traverse. Changes in router or link state can result from many things, including local power outages, equipment failures, management induced changes (e.g., turning off a link for debugging or, as mentioned above, rerouting traffic to avoid overloaded links) and physical damage to wires.

195. The following figure shows the rate of changes seen at a particular exchange point in September 2013:

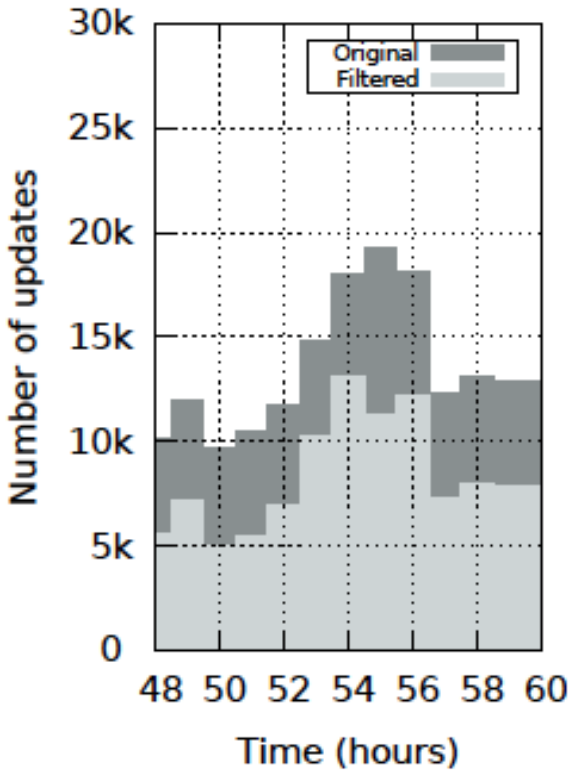



**Figure 22** — BGP updates at an Equinix exchange point in September 2013[33]

196. The figure shows the number of updates seen per hour over a 12-hour period starting September 19, 2013 at midnight GMT. The lighter grey area shows the number of unique updates per hour. For example, during the hour between 1 AM and 2 AM there were about 7,000 updates—a rate of almost two updates per second. Since BGP routing updates are propagated throughout the Internet, the same rate of updates will be seen by BGP routers all over the Internet.

[33] Appendix I at 4 (David Hauweele et al., *What Do Parrots and BGP Routers Have in Common?*, Computer Comm. Rev. (July 2016), https://ccronline.sigcomm.org/wp-content/uploads/2016/07/sigcomm-ccr-paper26.pdf)).

### *4. Asymmetric Data Paths*

197. The packets the web server sends back to my web browser in response to my hypothetical request follow the same process. Each router along the path makes its own determination of the next-hop router. Because of this there is no guarantee that the return packets will follow the same path that the request packets took.

198. I mentioned above in ¶ 164 that when large ISPs interconnect with other large ISPs, they generally do so at multiple geographically distinct places. As a general rule, ISPs configure their routers with special rules for the forwarding of packets that are destined to pass through another ISP. The ISPs generally configure the routers to send such packets to the other ISP through the closest interconnect even if that would not otherwise be the "best" path. Since both ISPs do the same, the paths packets take going in one direction can be very different than the paths packets take coming back. This configuration results in asymmetric paths for packets going in opposite directions between two network nodes. This type of routing is known as "nearest exit routing" or "hot-potato routing"—i.e., the ISP passes the packets off to another ISP as fast as it can.

199. Dr. Schulzrinne's description of routing in ¶¶ 41, 89 is incomplete in his failure to mention the asymmetric routing of communications. He states in ¶ 41, for example, that "*packets traveling between two points on the Internet generally follow the same path for long distances*". This is generally true for packets traveling in a particular direction, unless the ISP decides to change the path as I mention above in ¶ 190. But packets going in one direction between two points commonly take a very different path than packets going in the other direction between those same two points, due to asymmetric routing. You can think of the ISP forwarding rules that result in asymmetric routing as similar to one-way streets, causing the route you take from home to the

restaurant, for example, to be different from the route you take from the restaurant back home.

### F. International Connections

200. The heavily redundant connections between ISPs are reduced somewhat when it comes to intercontinental connections due to the relatively few undersea physical connections. Note that I'm referring to all of the cables connecting the U.S. to other countries as ***undersea*** even though one of them runs under Lake Ontario and would be more properly called an underlake cable. In addition to these undersea fiber cables, the U.S. is interconnected with Canada and Mexico with many ***terrestrial*** fiber cables. There are also some satellite-based interconnections, far fewer than there used to be before so many fiber cables were installed. Satellite-based connections are of far lower capacity than fiber-based ones and, because of the extra distance the signal has to travel up to the satellite and back, have added delays. Thus, satellite-based international communications are generally limited to islands that have not yet been connected with fiber cables, places far away from civilization and expensive satellite telephones. Since the vast majority of international Internet communications is transported over fiber, I will concentrate on that transport mode.

201. There are over 50 undersea fiber optic cables that connect the U.S. to other countries.[34] In addition, there are a number of fiber optic cables connecting the U.S. to Canada and to Mexico. The following figures are from TeleGeography, a well-regarded source of information about the telecommunications industry including, in particular,

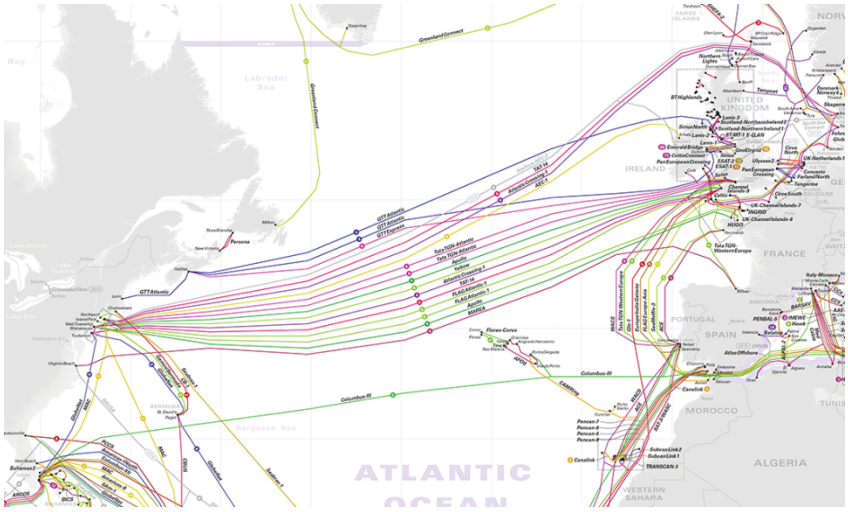
[34] Appendix J (Report on International Submarine Cables Landing in the US, based on information compiled from Telegeography (Jan. 2018)).

maps of undersea cables. The first figure shows the undersea fiber cables connecting the U.S. to other countries as of early 2018:




**Figure 23** — Undersea fiber cables[35]

202. The following figure shows the trans-Atlantic cables:


ATLANTIC OCEAN
UNITED KINGDOM
IRELAND
FRANCE
PORTUGAL
SPAIN
MOROCCO
ALGERIA
WESTERN SAHARA
BELGIUM
Labrador Sea
Bay
Greenland Connect
GTT Atlantic
GTT Express
Hibernia Express
Hibernia Atlantic
Tata TGN-Atlantic
Yellow
AEC-1
AEC-2
Atlantic Crossing-1
Atlantic Crossing-2
Apollo
Marea
Florez-Covo
Columbus III
Globenet
Sahara 1
Pencan 6
Pencan 7
Pencan 8
Pencan 9
Canalink
SubcanLink 2
SubcanLink 1
TRANSCAN-2
Bahamas 2
ARCOS
BICS
MAC
Virginia Beach
Jacksonville
Halifax
Lynn
Charlestown
Tuckerton
Buffalo
Ottawa
Toronto
Crosslake Fibre
Lake Ontario
Lake Erie
Lake Huron
Lake Superior
Lake Michigan
Washington, D.C.
Pacific City
Florence
Bandon
Hillsboro
Hermosa Beach
Redondo Beach
Wamenton
Harbour Pointe
Lynnwood
Tata TGN Pacific
PC-1
Japan U.S.
Los Angeles
Grover Beach
Morro Bay
Point Arena
Manchester
Florida
Yucatan
Belize
Maxcanu
Manzanillo
Mazatlan
Cuba
Havana
Key West
Miami
Naples
Vero Beach
Sargasso Sea
Gulf of Mexico
Greenland
Iceland
Faroe Islands
Scotland
Northern Ireland
Ireland
Wales
England
Isle of Man
Channel Islands
Netherlands
Belgium
Germany
Denmark
Norway
Sweden
Finland
Russia
Estonia
Latvia
Lithuania
Poland
Ukraine
Romania
Bulgaria
Turkey
Greece
Italy
Switzerland
Austria
Hungary
Slovakia
Czech Republic
Slovenia
Croatia
Bosnia and Herzegovina
Serbia
Montenegro
Albania
Macedonia
Kosovo
Moldova
Belarus
Azerbaijan
Georgia
Armenia
Kazakhstan
Uzbekistan
Turkmenistan
Kyrgyzstan
Tajikistan
Afghanistan
Pakistan
India
China
Japan
South Korea
North Korea
Mongolia
Taiwan
Philippines
Vietnam
Laos
Cambodia
Thailand
Myanmar
Malaysia
Singapore
Indonesia
Brunei
Papua New Guinea
Australia
New Zealand
Fiji
Tonga
Samoa
Vanuatu
Solomon Islands
Micronesia
Palau
Guam
Marshall Islands
Kiribati
Nauru
Tuvalu
Cook Islands
French Polynesia
New Caledonia
Hawaii
Alaska
Canada
Mexico
United States
Cuba
Jamaica
Haiti
Dominican Republic
Puerto Rico
Trinidad and Tobago
Barbados
Grenada
Saint Lucia
Saint Vincent and the Grenadines
Antigua and Barbuda
Saint Kitts and Nevis
Dominica
Guadeloupe
Martinique
Aruba
Curaçao
Bonaire
Saint Martin
Saint Barthélemy
Anguilla
Montserrat
British Virgin Islands
United States Virgin Islands
Bermuda
Cayman Islands
Turks and Caicos Islands
Bahamas
Colombia
Venezuela
Guyana
Suriname
French Guiana
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Argentina
Uruguay
Falkland Islands
South Georgia and the South Sandwich Islands
Antarctica
Libya
Egypt
Sudan
South Sudan
Eritrea
Djibouti
Ethiopia
Somalia
Kenya
Uganda
Rwanda
Burundi
Tanzania
Mozambique
Zambia
Malawi
Zimbabwe
Namibia
Botswana
South Africa
Lesotho
Swaziland
Madagascar
Comoros
Mauritius
Seychelles
Réunion
Mayotte
Saint Helena
Ascension Island
Tristan da Cunha
Nigeria
Benin
Togo
Ghana
Ivory Coast
Liberia
Sierra Leone
Guinea
Guinea-Bissau
Gambia
Senegal
Mauritania
Mali
Burkina Faso
Niger
Chad
Cameroon
Equatorial Guinea
Gabon
Republic of the Congo
Democratic Republic of the Congo
Central African Republic
Angola
Namibia
Cape Verde
Canary Islands
Madeira
Azores
Western Sahara
Algeria
Tunisia
Morocco
Portugal
Spain
France
Belgium
Netherlands

203. The following figure shows the trans-Pacific cables:

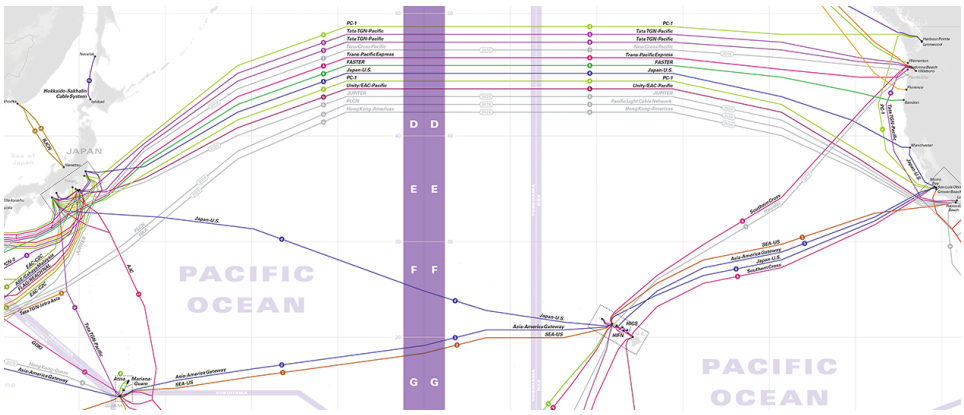
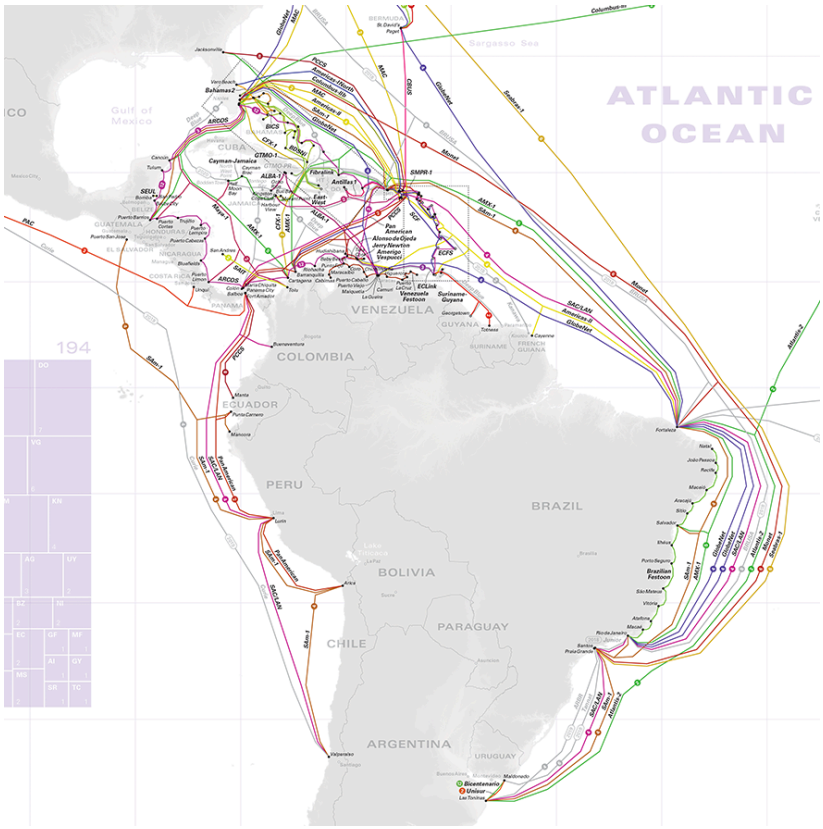



**Figure 25** — Trans-Pacific undersea fiber cables[37]

204. The following figure shows the undersea cables servicing South America and the Caribbean:




[37] Id.

**Figure 26** — Undersea cables between South America, the Caribbean and Europe[38]

205. The following figure shows terrestrial cables between the U.S. and Canada and between the U.S. and Mexico.



**Figure 27** — Terrestrial cables between the U.S. and Canada and between the U.S. and Mexico[39]

### *1. Details of Undersea Fiber-Optic Cables*

206. Each of the undersea cables contains multiple fiber pairs. One fiber in each pair is used to send traffic in one direction, and the second fiber in a pair is used to send traffic in the other direction. Each fiber can support multiple different simultaneous circuits, one on each of a number of colors of light, referred to as ***lambdas***. For example, one of the older transatlantic cables, the TAT-14 cable, has 4 pairs of fibers, each fiber of which supports 40 lambdas, for a total of 160 lambdas in each direction.[40] Each lambda

[38] Id.

[39] *ITU Interactive Transmission Map*, Int'l Tele-Comms Union, https://www.itu.int/itu-d/tnd-map-public (last updated Nov. 2018).

[40] *About the TAT-14 Cable Network*, TAT-14 Cable System, https://www.tat-14.com/tat14.

can support up to 40 gigabits per second (Gbps).[41] The full TAT-14 cables currently support 3.15 terabits per second (Tbps) each. A map of the TAT-14 cables is shown in the following figure:

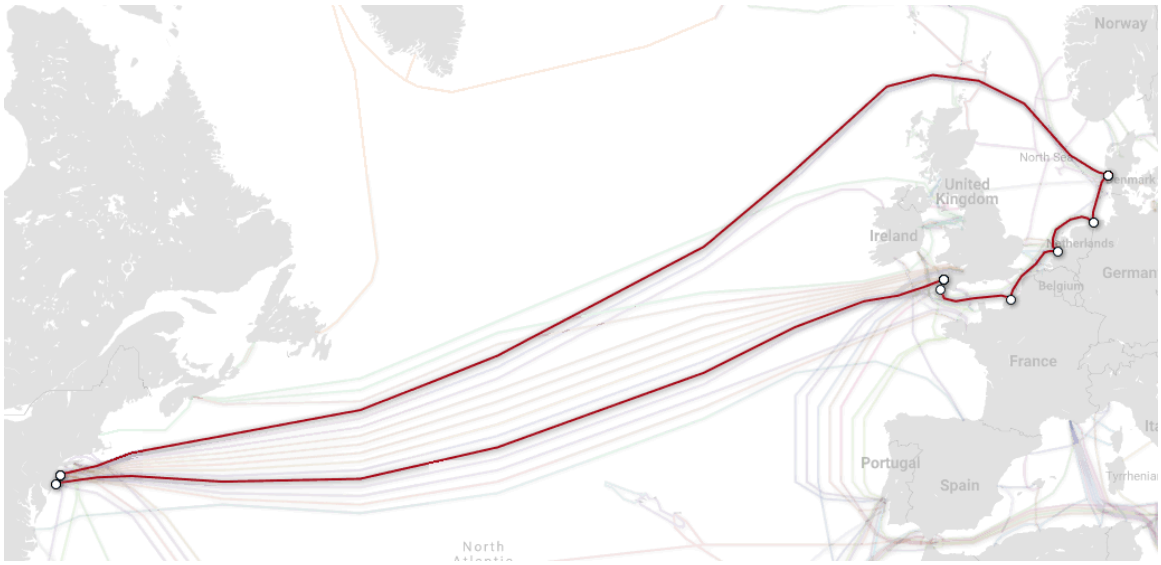



**Figure 28** — TAT-14 cable[42]

207. MAREA, a newer cable, installed by Microsoft, Facebook and Telxius (a global telecommunications infrastructure company) that connects the U.S. to Spain, contains 8 pairs of fibers and can support up to 160 Tbps.[43] A map of the MAREA cable is shown in the figure below:

[41] Gigabits per second (Gbps) is a measure of the speed of data transmission. A gigabit is a billion bits of information, and a bit is the smallest unit of digital information, represented by a one or zero. A terabit is 1,000 gigabits. For comparison, 8 bits make up a *byte*, a single text character is represented by a pattern of bits in a byte. A gigabit is enough data to carry about 30 million 4-character words or about 50 copies of Tolstoy's *War and Peace.*

[42] *Submarine Cable Map: TAT-14*, TeleGeography, https://www.submarinecablemap.com/#/submarine-cable/tat-14 (last updated Dec. 6, 2018).

[43] Deborah Bach, *Microsoft, Facebook and Telxius Complete the Highest-Capacity Subsea Cable to Cross the Atlantic*, Microsoft (Sept. 21, 2017), https://news.microsoft.com/features/microsoft-facebook-telxius-complete-highest-capacity-subsea-cable-cross-atlantic.

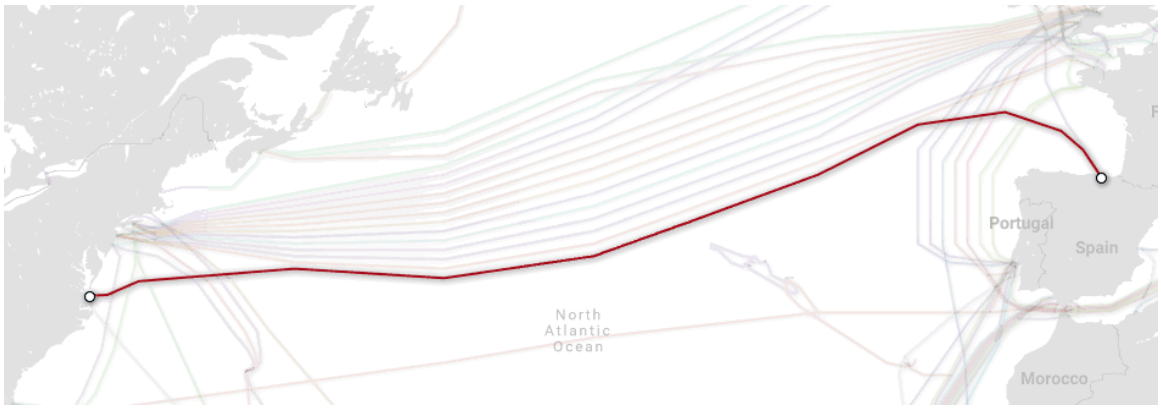



**Figure 29** — MAREA[44]

208. The number of fiber pairs in the undersea cables terminating in the U.S. ranges from 4 to 12 (with BICS being the only cable with 12 pairs, and only 4 cables having 8 pairs).[45]

209. Attached as Appendix J is a list of the international undersea cables that terminate in the U.S.[46] The list was compiled from the information on the TeleGeography website.

210. The above description is consistent with the government's description of the submarine cables:

> *The NSA Defendants respond further that, according to data available from Telegeography, international submarine cables typically contain 2-8 pairs of fiber-optic cables. Each fiber-optic pair is typically capable of carrying between approximately 15 and 120 individual communications circuits on different light wavelengths, depending on age and technology used. As a result, an individual submarine cable may carry between approximately 30 and 960 communications circuits. (Individual circuits*

[44] *Submarine Cable Map: MAREA*, TeleGeography, https://www.submarinecablemap.com/#/submarine-cable/marea (last updated Dec. 6, 2018).

[45] *Submarine Cable Map 2018*, TeleGeography, https://www.submarinecablemap.com.

[46] Appendix J (Report on International Submarine Cables Landing in the US, TeleGeography (Jan. 2018)).

*may be subdivided further to create multiple "virtual circuits" through application of various technologies.) Each wavelength carried on a fiber-optic pair is typically capable of transporting between 10 and 100 gigabits of data per second (10-100 Gbps), meaning that a typical submarine cable can carry between approximately 300 and 96,000 Gbps of data.*[47]

211. Devices at the transmitting end of a fiber use electronics to convert packets into modulated beams of light at specific frequencies (a.k.a., lambdas), and they then use optics to combine multiple lambdas into a single beam of light to send onto the fiber. Devices at the receiving end of a fiber use optics to split the beam of light from the fiber into the individual lambdas, and they then use electronics to reconstitute streams of packets from each of the lambdas.

### *2. Details of Terrestrial Fiber-Optic Cables*

212. Terrestrial fiber-optic cables, ones that cross borders or ones that are a part of an ISP's infrastructure, are much shorter than undersea cables and tend to have far more fibers but, otherwise, operate in the same way that undersea cables do.

### *3. Public Internet Communications on International Fiber-Optic Cables*

213. An individual company can own or lease a whole cable, pairs of fibers within a cable or pairs of lambdas within fibers. In some cases, the cable, fibers or lambdas are owned or leased by ISPs and used as part of the ISP's internal network, as circuits for peering with another ISP or as circuits to Internet exchange points. In the cases where the circuits are connecting to another ISP or to an exchange point, all communications on the circuit would be what I will call in this report ***public Internet***

[47] Appendix H at 4-5 (NSA Response to Plaintiff's Request for Admission No. 1 (Jan. 8, 2018)).

***communications*** or ***public Internet traffic***. That is, communications between Internet users. In the case where the circuit is used as part of the ISP's own network, some of the communications will be to support the ISP operations—to manage their routers for example. These communications would not be considered public Internet communications, while the rest of the traffic on such an internal communications link would be public Internet communications since it would be between Internet users.

214. Not all of the fibers in these cables are used for public Internet communications. Some of the undersea cables, fibers or lambdas are owned or leased by companies for use as part of their own internal networks or for corporate telephone and video communications. Communications on these cables would not be considered public Internet communications. In addition, many cables were built with more fiber than were initially required to allow for future expansion and have not yet been made active, or "lit."

215. Thus, public Internet communications are transported on a subset of the lambdas operating as circuits in a subset of the fibers that these undersea cables are capable of supporting. Since many ISPs consider their internal architecture and the number and location of the other ISPs they peer with to be proprietary, the ISPs and cable operators often do not publicly disclose the specific circuits that are used to transport public Internet communications.

216. Internet sites such as TeleGeography have done a very good job of cataloging the undersea cables that tie together countries around the world, but these sites do not break down which circuits on which fibers on which cables are used for public

Internet traffic and which are used for other purposes such as video distribution or internal corporate networks.

217. Viewing the available information, it is reasonable to infer that the distribution of circuits transporting public Internet communications roughly matches the overall distribution of undersea international cables and terrestrial international cables because the cables, in general, connect population centers where large numbers of Internet users live and work.

#### *4. Undersea Fiber-Optic Cable Landing Locations*

218. There are 47 sites where the international undersea cables that were identified from the TeleGeography information come ashore in the U.S.[48] Some of the cables come ashore in more than one U.S. location. TAT-14, which has branches that come ashore in two towns about 40 miles apart on the New Jersey shore, is an example of such a cable. When an undersea cable comes ashore, it is run to an enclosure where the individual fibers are broken out of the cable. The fibers can terminate in network devices (such as routers) in such an enclosure as shown in ¶ 23 of Dr. Schulzrinne's declaration, or they could be patched through to another cable that connects that enclosure to a location, such as a data center, where the network devices are located. The second option is shown in the following figure from a Virginia Beach planning presentation for the MAREA cable termination. The figure shows a conduit path from an enclosure at the beach where the cable comes ashore to a data center where the network devices are:

[48] See Appendix J for a list of the termination sites.




**Figure 30** — Conduit path for MAREA cable[49]

219. International Internet links can terminate at a variety of different types of physical facilities within the U.S. For example, some terminate at patching stations such as the one in Virginia Beach shown in Figure 31 below, cable landing stations such as the one shown in ¶ 23 of Dr. Schulzrinne's declaration, Internet exchange points, peering points, or ISP points of presence.

[49] Appendix CC (City of Virginia Beach Dep't of Info. Tech., *Next Generation Network and Transoceanic Subsea Cable Updates* (Oct. 4, 2017), https://www.vbgov.com/government/departments/communications-info-tech/Documents/NGN-and-Transoceanic-Subsea-Cables.pdf).



**Figure 31** — Manhole for fiber patching in Virginia Beach[50]

220. As discussed above in ¶¶ 200-201, the vast majority of the U.S. international Internet communications—i.e., communications that start or end in the U.S. where the other end is outside the U.S.—go through the undersea or terrestrial fiber cables shown in the figures above in ¶¶ 201-204.

***5. Terrestrial Fiber-Optic Cable Terminations***

221. International terrestrial fiber-optic cables do not require as distinct terminations as do undersea cables. Many of them are simple ISP interconnects or connections to Internet exchanges and are indistinguishable from any other terrestrial fiber-optic cables.

[50] Id.

### G. Places to Monitor International Public Internet Communications

222. As can be seen in the figures and discussion above, the U.S. termination points of the circuits carried on international undersea cables (see ¶¶ 218-220), as well as the U.S. ends of the international terrestrial cables (see ¶¶ 200, 216, 221) are prime locations to monitor communications between Internet users in the U.S. and Internet users in other countries, because essentially all of the public Internet communications between the U.S. and other countries flow over these circuits.

223. U.S. ends of the circuits carried on the trans-Atlantic and trans-Pacific cables are also attractive places to monitor public Internet communications between some non-U.S. and non-U.S. sites (other than Mexico and Canada). As can be seen from Figure 26, there is only one 2-pair fiber cable connecting South America to Europe and there are no cables connecting South America or the Caribbean with the Far East. Thus, almost all public Internet communications passing between South America, the Caribbean and the rest of the world will pass through the U.S. The same is true, but to a lesser extent, for public Internet communications in circuits in undersea cables between the Far East (China, Japan, Taiwan, and South Korea) and Europe. This means that the U.S. ends of the circuits carried on the trans-Atlantic and trans-Pacific cables are prime locations for monitoring public Internet communications between many non-U.S. locations. Monitoring at those locations also means that any monitoring equipment need only be in U.S. territory. Such monitoring locations would generally not capture communications entirely within a region such as communications between Europeans or such as communications between residents of the Far East.

224. As can be seen in the figures above, the total number of international undersea and terrestrial cables is relatively small, and there are even fewer physical locations where the cables terminate because multiple cables terminate at some of the locations. It is certainly not out of the question that the NSA would have been able to deploy upstream collection devices at all of these sites.

225. As I discuss below in ¶ 291, the FISC has confirmed that the NSA does in fact monitor at least some "*international Internet link[s]*",[51] which are the circuits connecting a network node in the U.S. to a network node in a foreign country. This of course makes sense, given that public Internet traffic on international Internet links will consist almost entirely of communications being sent or received (or both) by a node outside the U.S., which is the traffic that the NSA is authorized to monitor under its Section 702 procedures. It is not relevant to my report or to the conclusions I come to what type of facilities or physical locations at which the NSA is monitoring international Internet links; the relevant point is that the NSA is monitoring at least some international Internet links.

226. NSA representative Rebecca J. Richards, during her deposition, did not specifically say that the NSA monitors at the U.S. ends of the circuits carried on the trans-Atlantic and trans-Pacific cables, but she did say that the NSA did monitor at least one "*Internet backbone circuit*",[52] and she agreed that the international undersea cables can be part of the "*Internet backbone*".[53]

[51] Appendix P at 45 (FISC Opinion (Oct. 3, 2011)).

[52] Appendix K at 122:20-123:5 (Transcript of Deposition of Rebecca J. Richards (Apr. 16, 2018)).

[53] Id. at 79:15-20.

227. In several of its officially disclosed documents, the government has confirmed that it conducts upstream collection on multiple circuits. For example, the PCLOB Report states that upstream collection occurs with the compelled assistance "*of the providers*"—plural—"*that control the telecommunications backbone*".[54] The report also states that the providers facilitating upstream collection must "*assist the government in acquiring communications across these circuits*"—again, plural.[55] That said, it seems very obvious, as the PCLOB Report confirms, that the NSA must be monitoring more than one circuit carried on the international undersea cables. The NSA's thousands of surveillance targets are, presumably, in many parts of the world, and so if the NSA monitored only a single circuit in a single international undersea cable, it could not capture many or most of the communications of those geographically dispersed targets. Moreover, asymmetric routing (as discussed above in ¶¶ 197-199) means that monitoring only a single link could only ever capture those packets in a communication going in one direction, and monitoring only a single link could easily miss all of a target's packets if the routing changed as described above in ¶¶ 194-196.

228. Based on the NSA's description of the capability of undersea fiber cables, cited above at ¶ 210, the international undersea and terrestrial cables that terminate in the U.S. are capable of supporting thousands of individual communications circuits. Some fraction of these circuits are used to transport public Internet communications. It may be that the NSA has deployed enough upstream capture systems to provide full coverage of the international circuits that are used to transport public Internet communications, or the

[54] Appendix F at 40 (PCLOB Report at 35); see also id. at 12 (PCLOB Report at 7).

[55] Id. at 36-37.

NSA may have not done so yet. In any case, I find it hard to believe that the NSA has left many such circuits unmonitored considering the high number of surveillance targets, the variety of circuits that targets' Internet communications may travel into and out of the U.S., the variable routing of Internet communications, the importance the government attributes to the upstream collection program, and the NSA's stated desire to be comprehensive in its collection.[56]

### H. Locating Network Nodes Using IP Addresses

229. The use of regional assignment of IP addresses coupled with companies which have developed databases of the geographic locations of specific IP address ranges mean that determining where on the globe a network node using a particular IP is located has become quite reliable. One example of a use of such lists is a system that needs to restrict access to copyrighted material for licensing reasons. For example, Apple iTunes is only usable in specific countries. One commercial database of U.S. IP address ranges includes more than 66,000 individual entries.[57]

230. Locating where a network node is in the real world using the IP address in packets sent to or from a network node is generally but not always accurate. A NAT (see ¶¶ 173-174) will make a whole network's worth of network nodes appear to be in a single location even if the network nodes were actually located anywhere on a nation-wide or world-wide enterprise network. In addition, network nodes using VPNs or tunnels (see ¶ 91) will appear to be where the VPN or tunnel ends rather than where the node actually is. Thus, an IP address filter which uses a list of "U.S. IP addresses" to include or

[56] Id. at 10, 123, 143.

[57] *Create Country ACL*, Country IP Blocks, https://www.countryipblocks.net/country_selection.php.

exclude communications to be reviewed will likely exclude some communications that should be included or include some communications that should be excluded from or to U.S. Internet nodes because of the use of VPNs and NATs.

## V. NSA'S SECTION 702 COLLECTING OF COMMUNICATIONS

231. The NSA collects copies of communications involving non-U.S. persons under the authority of Section 702 of the Foreign Intelligence Surveillance Act, as amended. As the government has acknowledged, some of the communications also involve U.S. persons.[58] Two of the NSA's collection programs fall under the authorization of Section 702: ***PRISM*** and ***upstream collection***.[59] I will describe both of these programs below.

232. Under these programs the NSA collects, at least, recordings of phone calls and copies of Internet communications, which the NSA refers to as "*transactions*" (see ¶¶ 63-65), as well as metadata about the communications.

233. The NSA stores these copies in multiple NSA systems and data repositories:

> *Communications provided to NSA under Section 702 are processed and retained in multiple NSA systems and data repositories. One data repository, for example, might hold the contents of communications such as the texts of emails and recordings of conversations, while another, may only include metadata, i.e., basic information about the communication,*

[58] Appendix F at 7, 11 (PCLOB Report at 2, 6).

[59] Id. at 12 (PCLOB Report at 7).

*such as the time and duration of a telephone call, or sending and receiving email addresses.*[60]

234. These NSA systems and data repositories are also referred to collectively as "*Section 702 databases*".[61]

235. NSA analysts use search tools to identify copies of communications that are stored in the Section 702 databases and which may be relevant to a particular investigation.

**A. Selectors**

236. Both PRISM collection and upstream collection programs make use of ***selectors*** to identify the communications that are to be collected.

237. The following excerpt describes how selectors are determined:

*Once the NSA analyst has identified a person of foreign intelligence interest who is an appropriate target under one of the FISC-approved Section 702 certifications, that person is considered the target. The NSA analyst attempts to determine how, when, with whom, and where the target communicates. Then the analyst identifies specific communications modes used by the target and obtains a unique identifier associated with the target - for example, a telephone number or an email address. This unique identifier is referred to as a selector. The selector is not a "keyword" or particular term (e.g., "nuclear" or "bomb"), but must be a specific communications identifier (e.g., e-mail address).*[62]

[60] Appendix L at 7 (NSA Director of Civil Liberties & Privacy Office, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* at 6 (Apr. 16, 2014) ("DCLOP Report")).

[61] Appendix F at 132 (PCLOB Report at 128).

[62] Appendix L at 5 (DCLOP Report at 4).

238. The May 2, 2011 letter from a Department of Justice official to Judge Bates of the FISC describes the selectors used in the upstream collection program as including "*electronic communication accounts*", "*electronic communication addresses*" and "*electronic communications identifiers*":

> *As previously described to the Court, in conducting upstream collection using electronic communication accounts/addresses/identifiers (hereinafter "selectors") pursuant to Section 702, NSA acquires Internet communications that are to or from a tasked selector, or which contain a reference to a tasked selector.*[63]

239. The December 8, 2011 DoJ, NSA & DNI joint statement notes that accounts can be tasked:

> *Thus although upstream collection only targets Internet communications that are not between individuals located in the United States and are to, from, or about a tasked account, there is some inevitable incidental collection of wholly domestic communications or communications not to, from, or about a tasked account that could contain U.S. person information.*[64]

240. The Privacy and Civil Liberties Oversight Board (PCLOB) July 2, 2014 report provides additional details on what can be a selector and what cannot:

> *The Section 702 certifications permit non-U.S. persons to be targeted only through the "tasking" of what are called "selectors." A selector must be a specific communications facility that is assessed to be used by the target,*

[63] Appendix M at 1 (FISC Submission (May 2, 2011)); *see also, e.g.*, Appendix N at 4-5 (FISC Submission (Aug. 16, 2011)).

[64] Appendix O at 8 (Joint Statement at 7, *FISA Amendments Act Reauthorization: Hearing Before the H. Permanent Select Comm. on Intelligence* (Dec. 8, 2011)).

> *such as the target's email address or telephone number. Thus, in the terminology of Section 702, people (non-U.S. persons reasonably believed to be located outside the United States) are targeted; selectors (e.g., email addresses, telephone numbers) are tasked. The users of any tasked selector are considered targets—and therefore only selectors used by non-U.S. persons reasonably believed to be located abroad may be tasked. The targeting procedures govern both the targeting and tasking process. Because such terms would not identify specific communications facilities, selectors may not be key words (such as "bomb" or "attack"), or the names of targeted individuals ("Osama Bin Laden"). Under the NSA targeting procedures, if a U.S. person or a person located in the United States is determined to be a user of a selector, that selector may not be tasked to Section 702 acquisition or must be promptly detasked if the selector has already been tasked.*[65]

241. Note that the selector **must be a specific communications facility** such as a telephone number for a telephone facility or an email address for an email facility and cannot be some generic word (e.g., "bomb") or someone's name, since neither of these would be an identifier that was specific to a particular communications facility.

242. Most of the documentation the NSA has publicly released only lists telephone numbers and email addresses as examples of selectors. But some of these documents describe selectors as "*electronic communication accounts/addresses/identifiers*".[66]

[65] Appendix F at 37-38 (PCLOB Report at 32-33).

[66] Appendix M at 1 (FISC Submission (May 2, 2011)).

243. Examples of "*electronic communications accounts*" or "*electronic communications identifiers*" could include Twitter handles, Skype, Snapchat, Snow (a Chinese Snapchat), WhatsApp or Instagram IDs, Wikimedia usernames and similar application-specific identifiers or account names. URLs of target websites or services would also meet the description of "*electronic communications addresses*".

244. In theory, IP addresses could be selectors because they are unique identifiers that qualify as "*electronic communication addresses*". It is worth noting however, that there are many circumstances in which IP addresses do not uniquely identify individual Internet users, which might present difficulties for the NSA in using them as selectors, depending on the circumstances. As the FISC summarized the NSA's explanation:

> *Internet communications are "nearly always transmitted from a sender to a recipient through multiple legs before reaching their final destination." June 1 Submission at 6. For example, an e-mail message sent from the user of [redacted] to the user of [redacted] will at the very least travel from the [redacted] user's own computer, to [redacted], to [redacted] and then to the computer of the [redacted] user. Id. Because the communication's route is made up of multiple legs, the transaction used to transmit the communication across and particular leg of the route need only identify the IP address at either end of that leg in order to properly route the communication. Id. at 7. As a result, for each leg of the route, the transaction header will only contain the IP addresses at either end of that particular leg. Id.*[67]

[67] Appendix P at 34-35 n.33 (FISC Opinion (Oct. 3, 2011)).

245. In other words, packets making up the communication on each of these legs would have the IP addresses of the ends of the individual leg in their source and destination IP address fields. Thus, the IP addresses in the packets of the communications could change multiple times between the source and destination.

246. In addition, the IP addresses in the packets that make up email messages sent or received by a mail server on behalf of any of its users will have the same IP address—the IP address of the server—as their source or destination address, and all packets sent to or from the network nodes behind a NAT or VPN will have the NAT's IP address in the packet's source or destination address fields. (See ¶¶ 173-174.)

247. For these reasons, IP addresses will frequently not be effective selectors for identifying the communications of targets. This, in turn, means that it is more likely that the NSA is reassembling communications in order to determine if they contain selectors.

248. The above sorts of identifiers and others would be uniquely identifying in the way that selectors must be, and so could very well be the type of selectors the NSA uses in conducting upstream collection. The NSA has not publicly disclosed whether it uses them, however, and at least with respect to URLs, the NSA refused during its deposition to say whether it uses them as selectors.[68]

[68] Appendix K at 207:6-208-11 (Richards Depo.)

## VI. PRISM COLLECTION PROGRAM

249. Although this case is about upstream collection, understanding how PRISM collection works may be useful in understanding the distinguishing features of upstream collection. (Note that the NSA now refers to PRISM collection as "*downstream collection*".) The Privacy and Civil Liberties Oversight Board (PCLOB) described the PRISM process as follows:

> *In PRISM collection, the government sends a selector, such as an email address, to a United States-based electronic communications service provider, such as an Internet service provider ("ISP"), and the provider is compelled to give the communications sent to or from that selector to the government. PRISM collection does not include the acquisition of telephone calls. The National Security Agency ("NSA") receives all data collected through PRISM. In addition, the Central Intelligence Agency ("CIA") and the Federal Bureau of Investigation ("FBI") each receive a select portion of PRISM collection.*[69]

## VII. OPINIONS A, B & C: THE NSA'S UPSTREAM COLLECTION PROGRAM INVOLVES COPYING, REASSEMBLING AND REVIEWING INTERNET TRANSACTIONS

250. In the subsections that follow, I explain how the NSA's upstream collection program must work at a technical level, in the monitoring of any particular circuit. As discussed below in ¶¶ 265-329, I conclude that the NSA's upstream collection process must, as a technical matter, involve copying at an absolute minimum the packets constituting the transactions it wishes to review for the presence of selectors. I also conclude that, as a matter of practical necessity, upstream collection involves either:

[69] Appendix F at 12 (PCLOB Report at 7).

a. copying all of the packets flowing on the circuit, so that the packets can be sent to an IP filter to eliminate those that are part of a wholly domestic transaction, if necessary; or

b. copying all of the packets that an IP address filter test determines are not part of a wholly domestic transaction.

251. In either case, at least the packets that are not part of a wholly domestic transaction are copied.

252. **Opinion A:** Thus, it is my opinion that, to conduct upstream collection of international public Internet communications traversing any particular circuit, as this operation has been described by the government, the NSA must be copying at an absolute minimum the packets constituting the transactions it wishes to review for the presence of selectors. Based on other practical necessities I describe below, it is also my opinion that the NSA is almost certainly either (1) copying all packets traversing that circuit or (2) copying all of the packets that an IP address filter test determines are not part of a wholly domestic transaction.

253. As discussed below in ¶¶ 301-309, I also conclude that to determine whether an Internet transaction that passes the NSA's filter contains a selector, the NSA must first reassemble captured packets into transactions.

254. **Opinion B:** Thus, it is my opinion that, in order to review Internet transactions to determine if a selector tasked for collection is present, the NSA must be reassembling the packets of the transactions it intends to review.

255. As discussed below in ¶¶ 310-327, I also conclude that to determine whether an Internet transaction that passes the NSA's filter contains a selector, the NSA must review all of the reassembled copies of Internet transactions by scanning them to determine if the reassembled Internet transactions contain one of more selectors.

256. **Opinion C:** Thus, it is my opinion that the NSA must review the reassembled Internet transactions in order to identify those that include a tasked selector and thus are subject to collection under the upstream collection program.

### A. Upstream Collection Program

257. This case concerns the NSA's upstream collection program, also referred to as ***upstream surveillance***.

258. In the following section I will describe the NSA's upstream collection program as it existed in 2015, when Wikimedia filed its amended complaint. Between 2015 and now, the NSA suspended one part of the program—the part referred to as ***about collection***. As I explain further below, ***about collection*** involved the collection of communications that included a selector in the body of the communication and were therefore "about" a target.

259. In summary, the NSA uses the upstream collection program to collect Internet transactions that contain selectors (see ¶¶ 236-248) and that are from or to a non-U.S. person outside the U.S. The actual collection is done by devices that execute a type of what is known as ***deep packet inspection*** (***DPI***). DPI is a well-known and widely used tool used in enterprise and ISP networks to scan network communications for various purposes, including the detection of security threats. Billions of dollars of DPI equipment are sold annually around the world by many different equipment

manufacturers.[70] For example, since 2008, the Department of Homeland Security has been using successive generations of a DPI system—known as EINSTEIN 2 and EINSTEIN 3 Accelerated—to help protect a number of federal agency networks.[71]

### *1. A Description of NSA's Upstream Collection Program*

260. The government has made a number of statements describing the upstream collection program.

a. The PCLOB described upstream collection as follows:

*upstream collection . . . occurs with the compelled assistance of providers that control the telecommunications 'backbone' over which telephone and Internet communications transit, rather than with the compelled assistance of ISPs or similar companies.*[72]

b. The PCLOB also said that the term "upstream" refers to the fact that the surveillance

*does not occur at the local telephone company or email provider with whom the targeted person interacts . . . but instead occurs 'upstream' in the flow of communications between communication service providers.*[73]

c. In the March 19, 2014 PCLOB hearing, Rajesh De, General Counsel of the NSA, stated

*upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers."*[74] *In a*

[70] See, for example: *Deep Packet Inspection (DPI) Market Research Report, Analysis, Trends, Market Size Estimations and Forecast to 2022*, Reuters (Sept. 12, 2017), https://www.reuters.com/brandfeatures/venture-capital/article?id=16008.

[71] U.S. Dep't of Homeland Security, *EINSTEIN*, https://www.dhs.gov/einstein (last updated May 17, 2018).

[72] Appendix F at 12 (PCLOB Report at 7).

[73] Id. at 40 (PCLOB Report at 35).

> *declaration, Miriam P. stated "Upstream collection, in contrast, involves the compelled assistance (through a Section 702 directive) of certain providers that control the telecommunications backbone over which telephone and Internet-based communications transit. Unlike PRISM, Upstream collection generally involves the acquisition of certain communications as they traverse the telecommunications backbone.*[75]

261. All of these statements differentiate upstream collection from PRISM collection based on where the surveillance takes place and the manner in which the surveillance is conducted. Whereas PRISM collection involves compelling electronic communications service providers to turn over communications of their users, upstream collection involves compelling telecommunications providers to turn over communications that transit their networks. And whereas PRISM collection involves the collection of communications to or from the government's targets, upstream collection involves the collection of communications to, from, or (until April 2017) "about" the government's targets.

262. The government's public statements concerning the locations at which upstream collection is conducted are somewhat inconsistent. The second PCLOB statement above, ¶ 260.b, describes upstream collection as taking place in the "*flow of communications between communication service providers.*" The other statements, ¶ 260.a & c, refer to upstream collection as occurring on the "*Internet backbone*," which, as discussed above in ¶¶ 150-153, the government defines more broadly as including (1) the high-speed circuits (network links) and routers that are used to interconnect ISPs, (2)

---

[74] Appendix Q at 26:6-8 (PCLOB, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014)).

[75] NSA Decl. ¶ 7, *Jewel v. NSA*, No. 4:08-cv-04373 (N.D. Cal. Nov. 7, 2014) (ECF No. 300).

the circuits carried on the undersea cables that connect the U.S. with other countries, and (3) the high speed terrestrial network links (circuits) within the U.S. and between the U.S. and other countries, whether the undersea or terrestrial network links are **between ISPs or within an ISP**.

263. In her deposition, the NSA's representative Rebecca J. Richards agreed that the Internet backbone included connections between ISPs and within ISPs.[76]

264. I will assume for this report that upstream collection may take place on circuits either between ISPs or within an ISP.

### *2. Upstream Collection Process*

265. The process followed for upstream collection was described in the PCLOB report as follows:

> *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." 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–tasked 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 tasked selector. Unless transactions pass both these screens, they are not ingested into government databases. As of 2011, the NSA acquired approximately 26.5 million Internet transactions a year as a result of upstream collection.*[77]

[76] Appendix K at 47:18-22, 52:16- 53:12, 54:20- 55:7 (Richards Depo.).

[77] Appendix F at 41-42 (PCLOB Report at 36-37).

266. The "*government databases*" mentioned in the above extract are the same ones referred to as the "*Section 702 databases.*" (See ¶¶ 233-234.)

267. Upstream collection program-related documents refer to both screening, as the above extract does, and "*scanning*."[78] I will use the term ***reviewing*** in this report for this function.

268. The extract at ¶ 265 describes a 3-stage upstream collection process, but given the manner in which upstream collection must be conducted (as I explain below), it is clearer to describe upstream collection conceptually as having 5 stages.

**a. Stage 1: Copying the Packets**

269. As described in ¶ 38, multiple communications are simultaneously run over each Internet circuit by intermingling packets from different communications on the circuit. This is shown in the following figure:



**Figure 32** — Packets on a circuit

270. The small rectangles in the above figure represent packets flowing from left to right over a circuit. The different colors represent packets from different communications. For this explanation, the circuit is one of the ones that the NSA refers to as an Internet backbone circuit and is operated by an electronic communication service provider, which I will refer to as an ***ISP***.

271. I refer to a ***monitoring system*** in the section below. By that I mean, one or more devices that perform the processing required to implement upstream collection.

[78] See, e.g., Appendix R at 3, 24 (FISC Submission (June 28, 2011)); Appendix S at 6 (NSA Section 702 Minimization Procedures (2014)); Appendix F at 124 (PCLOB Report at 119).

Some of these devices may be ones designed by the NSA specifically for the upstream collection program. The government has acknowledged using "*NSA-designed upstream Internet collection devices*" in the upstream collection process.[79] Some of the devices may be off-the-shelf networking devices. I do not mean to imply any particular arrangement of such devices by using the term "system."

272. As a technical matter, there are only two possible configurations the NSA could be using to accomplish the copying of transactions necessary for upstream collection:

a. Copying all the traffic on a circuit so that the traffic can be passed on to one or more devices that then isolate the Internet transactions of interest. I will refer to this configuration as the ***copy-then-filter*** configuration.

*or*

b. Copying a subset of the traffic on the circuit, for example only the packets that are a part of Internet transactions that are not wholly domestic, and then passing the copied traffic on to one or more devices that then isolate the Internet transactions of interest. I will refer to this configuration as the ***in-line filter*** configuration.

[79] Appendix F at 44 (PCLOB Report at 39).

i. Copy-Then-Filter

273. The copy-then-filter configuration is shown in the following figure:

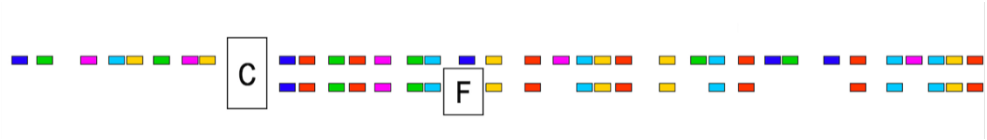



**Figure 33** — Copy-then-filter

274. The box marked "C" in Figure 33 represents a device that copies the traffic. The copying in the copy-then-filter configuration could be done in one of two ways; both ways use devices that are placed into a fiber or a circuit:

a. at the physical layer using a fiber-optic splitter;

*or*

b. at the link layer using a device that makes a copy of all the packets on a circuit.

(1) Fiber-optic splitter

275. A fiber-optic splitter splits the light on a fiber into two parts, each of which is put on its own fiber. Such a splitter could be placed on a fiber carrying traffic from an ISP's terrestrial network into an international cable (Figure 34) or a fiber carrying traffic from an international cable into an ISP's terrestrial network (Figure 35).

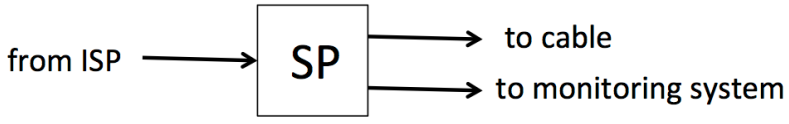



**Figure 34** — Fiber-optic splitter on fiber **into** an international cable

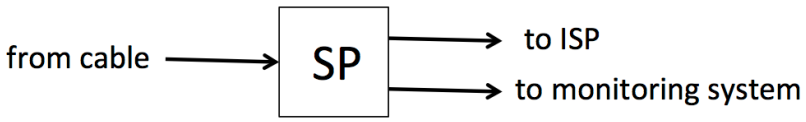



**Figure 35** — Fiber-optic splitter on fiber **from** an international cable

276. For the configuration shown in Figure 34, in which the ISP is sending traffic onto the international cable, one fiber from the splitter goes to the international cable and the other fiber goes to the monitoring system. In the other configuration (Figure 35), where the ISP is receiving traffic from the international cable, one fiber from the splitter carries traffic to the ISP, and the other one goes to the monitoring system.

277. In both cases, as discussed above in ¶ 211, the monitoring system must optically split out the lambdas of interest then reconstitute streams of packets from those lambdas. This process results in two copies of the packets: one copy to the ISP or the international cable and one copy to the monitoring system. Dr. Schulzrinne discusses the use of a fiber-optic splitter in ¶ 55 of his declaration.

(2) Link-Layer Copying

278. A link-layer copying of packets can be done by a separate in-line device or by the ISP's router, using for example the router's mirroring function. Dr. Schulzrinne discusses using a router's mirroring function to copy packets in ¶ 58 of his declaration. The use of either a separate copying device or the mirror function in the ISP's router results in all the packets on the circuit being copied and forwarded to the monitoring system.

(3) Filtering the packets

279. The box marked "F" in Figure 33 represents a filtering function in the monitoring system. This filter function can be used to implement the IP address filter

that accepts only Internet transactions that are not wholly domestic, as described in the above PCLOB extract (see ¶ 265) and described below under Stage 2 (see ¶¶ 290-300). The filter function could also be used to implement more extensive filtering.

ii. In-Line Filter

280. In the in-line filter configuration, all the packets on a circuit being monitored by the NSA are sent through an in-line device configured to copy only those packets that meet a set of criteria. This configuration, which is described in ¶ 57 of Dr. Schulzrinne's declaration, is shown in the following figure:




**Figure 36** — In-line filter

281. The box marked "F" in Figure 34 represents the filter that (a) copies the subset of the packets on the circuit that meet the filter criteria and (b) sends them on for further processing. Dr. Schulzrinne notes in ¶ 60 of his declaration that the mirroring function in many ISP routers can be configured to perform this filtering function by selectively copying packets based, for example, on access control lists that are configured to use the IP addresses or port numbers in packets.

iii. Implementation

282. For a number of reasons explained below, I consider it most likely that the NSA is using the copy-then-filter configuration implemented using fiber-optic splitters or using link-layer copying. I consider it less likely that the NSA is using an in-line filter and very unlikely that the NSA would be using an in-line filter with sensitive or complex filtering criteria such as those described as possibilities by Dr. Schulzrinne.

283. The copy-then-filter configuration is the easiest configuration for both the NSA and the ISP to implement and operate. This configuration requires no or minimal support from the ISP or its personnel and leaves the NSA in full control of the upstream collection process. All the ISP has to do is to hand the NSA copies of all of the packets on a circuit, which is very easy to do using the router mirroring function, or a portion of the light on a fiber, which is very easy to do with a fiber-optic splitter. Thus the ISP is not a party to any proprietary information other than the basic fact that monitoring is being done at a particular location.

284. In contrast, the in-line filter configuration would require either that the ISP agree to place an NSA-operated device into the heart of its network—unlikely because of the potential impact on the ISP's network in the event of an equipment failure or misconfiguration—or that the ISP's personnel have enough knowledge of the filter criteria to configure the ISP's router.

285. Under Section 702, the NSA can compel an ISP to provide assistance to the NSA as part of upstream collection.[80] Thus, the NSA could compel an ISP to configure its routers to provide the in-line filter functionality. But, compelling an ISP to conduct complex in-line filtering on the ISP's routers would require that ISP personnel know what the NSA's filter criteria were. This would not be a real issue if the filter criteria were not sensitive—for example, if the criteria merely excluded packets with U.S. source and destination IP addresses. But if the filter criteria were more selective, as

[80] 50 U.S.C. § 1881a(i)(1)(A) (Attorney General and Director of National Intelligence may direct that providers "*immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition*").

postulated by Dr. Schulzrinne in ¶ 60 of his declaration, then the ISP personnel would have access to sensitive or classified filtering criteria the NSA uses in its upstream collection process, which I believe the NSA would want to minimize to the greatest degree possible.

286. I do know from personal experience that some parts of the U.S. government consider network device configuration details to be secret. When I was involved in the U.S. government Trusted Internet Connections (TIC) Program as a consultant, I was told that the configurations for the EINSTEIN filtering devices were considered secret because they could disclose what the government knew about cyber attackers.

287. Because of the sensitivity of the filter criteria, I consider it most likely that, if the NSA relies on in-line filters operated by an ISP, the filter criteria would not include blacklisting or whitelisting of individual IP addresses or rejection of individual ports such as 443, because if that information were to ever get out it would provide a roadmap for people who wanted to avoid NSA upstream collection. Note that complex filtering could easily be done using the copy-then-filter configuration, which would not require ISP personnel to have access to the NSA's filtering criteria, because the filter itself would be operated by the NSA.

288. Dr. Schulzrinne suggests that the in-line filter configuration is "*desirable from the perspective of reducing the volume of communications that must be processed (electronically reviewed) to identify the communications of interest*," see Schulzrinne Decl. ¶ 57, but he overstates that benefit. Modern deep packet inspection devices individually or operating in parallel, can process or review Internet communications at

the same rate that those communications traverse high-bandwidth Internet links. In addition, adding even a "simple" IP address-based filter to an ISP's router in order to exclude wholly domestic transactions would require adding tens of thousands of lines to the router's configuration and would place potentially significant additional demands on the router's processing power which could affect the performance of the router and create a risk of overloading the router, thereby interfering with the ISP's ability to support its customers' traffic.

289. In my opinion, the copy-then-filter configuration gives the NSA the greatest operational control and confidentiality in carrying out upstream collection with the least risk of interference with the ISP's ordinary network operations. For these reasons, I consider it more likely that a copy-then-filter implementation is used rather than the in-line filtering that Dr. Schulzrinne hypothesizes. But if an in-line filter is used, in my opinion the filter is almost certainly a simple one as discussed in the next section. (See ¶ 298.) In either case, packets are copied, whether before the filter or by the filter.

**b. Stage 2: Filtering**

290. The publicly released documents show that the NSA uses IP address filters to eliminate wholly domestic transactions prior to scanning for selectors, though, as explained below, the documents indicate that the NSA may not filter packets by IP address on certain international Internet circuits it is monitoring. The PCLOB extract in ¶ 265 notes that the "*Internet transactions are first filtered to eliminate potential domestic transactions.*"

291. The publicly released NSA documents reveal, however, that not all Internet transactions are filtered to eliminate wholly domestic communications before

being reviewed for the presence of selectors. For example, the NSA's 2014 targeting procedures says:

> *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 overseas, or [redacted] In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.*[81]

292. The above passage may explain why a wholly domestic "about" transaction could be acquired if the transaction was routed through an international link. Such routing of wholly domestic communications over international circuits does occasionally happen.[82] This situation is described in the following passage from the Foreign Intelligence Surveillance Court's October 3, 2011 opinion describing the operation of the NSA's upstream collection program:

> *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*** *or is routed through a foreign server.*[83]

293. This passage indicates that the NSA does not use IP filtering at least on some of the international circuits it is monitoring. This is unsurprising because, by definition, the packets on international circuits are destined for or come from (or both)

---

[81] Appendix T at 2 (NSA Section 702 Targeting Procedure (2014), at 2).

[82] See, e.g., Shaun Waterman, *Internet Traffic Was Routed Via Chinese Servers*, Wash. Times (Nov. 15, 2010), https://www.washingtontimes.com/news/2010/nov/15/internet-traffic-was-routed-via-chinese-servers.

[83] Appendix P at 45 (FISC Opinion (Oct. 3, 2011)) (emphasis added) (citing the government's June 1, 2011 FISC Submission at 29).

non-U.S. locations and thus cannot have U.S. IP addresses as both source and destination addresses except in the case of a routing abnormality.

294. If the NSA were passing all transactions through an IP filter to eliminate wholly domestic transactions before copying, reassembly and review for selectors, then the NSA would never collect a transaction between U.S. IP addresses. That is because the NSA cannot review transactions for selectors, and therefore potentially collect them, without copying the packets and reassembling them into transactions first. (See ¶¶ 301-0.) Since the NSA admits to collecting wholly domestic "about" transactions from international links, it must not be applying an IP address filter in at least those cases. In addition, since the NSA admits it "*will acquire*" wholly domestic transactions from at least some international links, the NSA must be copying, reassembling and reviewing *all* the transactions on those links—otherwise the NSA would not see the selectors in the wholly domestic transactions and would not be collecting them. This is true for upstream collection of communications "to" and "from" the NSA's targets, not just collection of communications "about" its targets.

295. Where the NSA uses an actual IP address filter, it has further described the filtering mechanism as follows:

> *NSA Defendants respond that to their understanding the term "filtering mechanism," as used in the above-referenced brief when filed, meant, in unclassified terms, the devices utilized in the upstream Internet collection process that were designed to eliminate wholly domestic Internet transactions, and transactions that did not contain at least one tasked selector, before they could be ingested into Government databases. Today the term "filtering mechanism" would mean, in unclassified terms, the devices utilized in the Upstream Internet collection process that are*

*designed to eliminate wholly domestic Internet transactions, and to identify for acquisition Internet transactions to or from persons targeted in accordance with the current NSA targeting procedures.*[84]

296. Most references to the filter function in NSA documents refer to an ***IP filter*** or ***Internet protocol address filter***. An IP filter is a device that can filter Internet packets based on information available in the IP header. The IP header includes a variety of data, but most importantly, it contains the source and destination IP addresses of the packet. (See ¶¶ 96-101.) There are a few places where the NSA refers to its upstream collection filter function as an ***IP address filter***.[85] I believe that the "IP filter" referred to in the other documents is an IP address filter because of these citations and also because the only way that an IP filter could be used to eliminate potential domestic transactions would be to filter based on IP addresses. As discussed above in ¶¶ 229-230, as a general rule, ranges of IP addresses are assigned to ISPs or, through ISPs to their customers in such a way that an individual IP address can be geographically located to a reasonable degree of accuracy. The accuracy is not perfect since blocks of IP addresses are reassigned to different networks in different locations, including in different countries, from time to time. The frequency of these changes has increased significantly in the last few years because of the commercial market for the right to use IPv4 addresses, which I discuss above in ¶ 160. This may be what the NSA is referring to when it says "*[b]ecause NSA's filters will be looking at the best available information*."[86]

[84] Appendix D at 7-8 (NSA Response to Plaintiff's Interrogatory No. 3 (Dec. 22, 2017)).

[85] Appendix U at 24 (FISC Hearing Transcript, *In Re: DNI/AG 702(g) Certification* [*Redacted*] (2008)); Appendix C at 32, 37 (FISC Submission (June 1, 2011)).

[86] See Appendix C at 11 (FISC Submission (June 1, 2011)).

297. Thus, the source and destination IP addresses in each individual packet can be checked to see that both of them are from ranges of IP addresses assigned to a network inside the U.S. Using an IP **address** filter provides the function the NSA described for the IP filter:

> *NSA is required to use other technical means, such as Internet protocol ("IP") filters, to help ensure that at least one end of an acquired Internet transaction is located outside the United States.*[87]

298. Note that even a "simple" filter configured to just reject wholly domestic transactions by using an IP address-based filter is no easy task. There are over 66,000 entries in one of the lists of U.S. address blocks. (See ¶ 229.) Adding and maintaining that many entries to a production router's configuration is a significant task and would have a significant chance of adversely impacting the router's performance.

299. As Dr. Schulzrinne points out in ¶¶ 60-64 of his declaration: In general, such a filter could also be configured to perform other checks such as rejecting any packets transporting protocols that an entity is not interested in, or the reverse, accepting any packets transporting protocols the entity is interested in. The filter could also be configured to reject packets destined to or from particular network addresses an entity might not want to monitor. It should be noted that the more complex the filtering configuration, the more effort is required to keep the filter configurations up to date. As discussed above in ¶¶ 285-289 doing any filtering other than simple U.S. vs. non-U.S. addresses would likely have to be managed by NSA personnel on an NSA operated device or by ISP personnel with security clearances.

[87] Appendix F at 43 (PCLOB Report at 38).

300. To state the obvious, filtering out packets at this stage would eliminate the NSA's ability to collect the Internet communications to which those packets belong, and would thus foreclose its ability under this program to collect and analyze any foreign intelligence information those communications contain.

**c. Stage 3: Reassembling Transactions**

301. The next step is to reassemble the packets that make up individual communications so that they can be reviewed using DPI for the presence of selectors. As computer researchers Shuhui Chen and Yong Tang put it, "*Stream Reassembly is an indispensable function of Deep Packet Inspection*."[88] What Chen and Tang call a "stream" is another name for what the NSA calls "transactions." (See ¶¶ 63-65.)

302. Transaction reassembly is required before the DPI device can review for selectors because: (1) the packets that make up a particular transaction are intermingled with packets from other transactions (see ¶ 38) and must be isolated from the other packets by selecting the packets with the same source and destination address and ports and the same protocol value (the 5-tuple) and adding them to an assembly buffer[89] (see ¶ 113), (2) the packets may also have to be reordered to be in the right sequence (see ¶ 114), and finally, (3) the selectors that the NSA's reviewing devices look for may be split between the packets that make up the transaction.

[88] Appendix V (Shuihui Chen & Yong Tang, *A Stream Reassembly Mechanism Based on DPI*, Inst. of Electrical & Electronics Engineers (2012)).

[89] By ***assembly buffer***, I mean a temporary storage place in the collection device's memory

303. There are DPI designs that can review for keys such as the NSA's selectors without reassembling the streams (transactions),[90] but since the NSA does need the reassembled transactions to be able to store any with selectors in its databases, transaction reassembly is required even if the reviewing process itself does not need to work on reassembled transactions.

304. The reassembly process is shown in the following figure:



**Figure 37** — Reassembling transactions

305. The figure above shows the packets that were passed by the filter being reassembled into Internet transactions. Each transaction comprises all of the packets related to a particular communication (i.e., that have the same 5-tuple) that pass by the monitoring point.

306. The assembly needs to continue until there is an indication that the Internet transaction is complete or there has been some period during which no new packets with a matching 5-tuple have been received.

307. Since the Internet does not guarantee that the order of packets will be maintained during their journey through the network, packets in the buffer may have to be swapped around so that the packets making up the transaction are in the right order. This is required so that any selector that extends across a packet boundary will be made whole for the reviewing process (see below) and be properly recognized.

[90] See, e.g., Appendix W (U.S. Patent No. 8,813,221).

308. Because the paths taken by successive packets as they travel through the network may occasionally change, there is no guarantee that all the packets that make up an Internet transaction will pass by any particular monitoring point. (See ¶ 194.) This will result in some incomplete Internet transactions being assembled. An incomplete Internet transaction might not have a complete selector and thus be missed in the collection process. Conversely, even incomplete Internet transactions may contain complete selectors, and those transactions would thus be collected.

309. Also, because of asymmetric routing paths, the packets that make up the Internet transaction in each direction of the bidirectional exchange of packets that make up most Internet communications (see ¶ 111) will generally not pass through the same monitoring point. (See ¶¶ 197-198.) In those cases where a selector appears in both directions of a communication and where the packets in each direction pass through NSA monitoring points, the upstream collection process will result in both Internet transactions being collected, and they can later be associated during the analysis process. But, it would not be common for some types of selectors, such as a source email address, to be present in both directions of an Internet transaction; normally it would only appear in one direction. The effect of asymmetric routing is one more reason that it is likely the NSA has multiple monitoring points.

### d. Stage 4: Reviewing Transactions

310. The Internet transactions that have been reassembled from packets that passed the NSA's IP address filter then need to be reviewed for the presence of selectors. This stage is shown in the following figure:

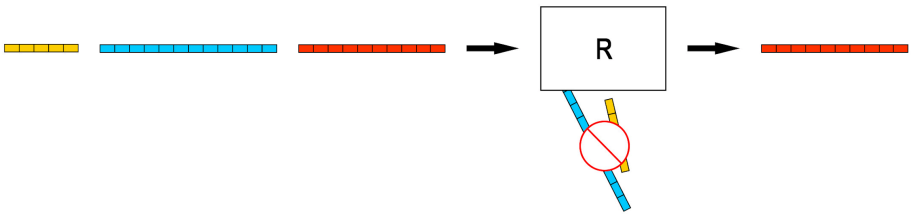



**Figure 38** — Reviewing transactions for selectors

311. The above figure shows a series of reassembled transactions being sent to a reviewing device (the box marked "R") and only the transactions containing selectors exiting the device. The remaining transactions are discarded.

312. As discussed above in ¶¶ 236-240, the selectors the NSA uses in the upstream collection program include "*electronic communication accounts/addresses/identifiers*".[91] The examples provided in the NSA documents are account identifiers, telephone numbers and email addresses. These are carried in the application layer in Internet communications. (See ¶ 60.)

313. For example, email addresses are carried in the SMTP handshake (see ¶¶ 134-137), in email headers (see ¶¶ 126-128), in IMAP (see ¶¶ 138-140), and in HTTP/S (see ¶¶ 117-123) when HTTP is the user's interface to an email server (see ¶¶ 129-133). In all of these cases, the email addresses are carried in the application layer of an Internet communication. Email addresses are also sometimes carried in the body of

[91] Appendix M at 1 (FISC Submission (May 2, 2011)).

Internet communications, which is also in the application layer, such as the body of email messages or in the contents of web pages. Telephone numbers in voice over IP are carried in the SIP headers (see ¶ 141), which are also in the application layer. Thus, the NSA must be reviewing the application layer of Internet communications if it is looking for these types of selectors within the communications.

314. In her deposition, Rebecca J. Richards acknowledged that the NSA, at least in 2015, did review the application layer of Internet communications.[92] Following an order from her counsel, she refused to answer the same question about upstream collection today because she said that the answer would be classified.[93] It is strange that the NSA considers classified the answer to the question of whether upstream collection today involves reviewing the application layer of communications. There is no question that it must involve that sort of reviewing, because the email addresses and other user identifiers in Internet communications are transported in the application layer. The NSA has acknowledged using "*NSA-designed upstream Internet collection devices*" in the collection process.[94] The NSA has also acknowledged reviewing web traffic:

> *Results were reviewed for three randomly selected days in April, averaged to produce an estimated figure of collection of [redacted] for the month of April. This figure was then compared to the total take of Section 702 upstream collection of web activity for the month. From this sample NSA estimates that approximately 9% of the monthly Section 702 upstream collection of [redacted].*[95]

[92] Appendix K at 263:11-18 (Richards Depo.).

[93] Appendix K at 266:4-13 (Richards Depo.).

[94] Appendix F at 44 (PCLOB Report at 39).

[95] Appendix C at 30 (FISC Submission (June 1, 2011)).

315. ***Web communications*** are the communications carried by HTTP or HTTPS. (See ¶¶ 117-123.) Thus, since the NSA was comparing the amount of collection of a particular redacted type of communication against the amount of collection of "web activity" to get a percentage, they must have been comparing the amount of web (HTTP/S) collection.

i. "multiple communications transaction (MCT)" collection

316. The PCLOB Report described MCT collection as follows:

> *An MCT is an Internet "transaction" that contains more than one discrete communication within it. If one of the communications within an MCT is to, from, or "about" a tasked selector, and if one end of the transaction is foreign, the NSA will acquire the entire MCT through upstream collection, including other discrete communications within the MCT that do not contain the selector.*[96]

317. An example of this type of MCT is the burst of email messages downloaded to a mail user agent when a user reconnects to a mail server after being disconnected for a while. (See ¶ 132.) Under the upstream collection program, the NSA would collect an MCT comprised of multiple email messages if any of the email messages in the burst is from a target outside the U.S. to someone inside the U.S. It might be that only one of the email messages is from the target and ten more are from sources within the U.S., but the entire MCT would be collected.

318. In order to discover that an MCT includes an email message that is from a target, the NSA must be reviewing the entire transaction. This is because each email

[96] Appendix F at 12 (PCLOB Report at 7).

within a burst of email messages has its own header information (e.g., "To:" and "From:" addresses). (See ¶¶ 126-128.)

319. MCT collection is controversial because it can involve the capture of wholly domestic communications, which is generally not authorized under upstream collection. It can also involve the capture of international communications that are not to, from, or about a targeted selector, which again is not generally authorized under upstream collection. But the NSA says that it does not have the technology to separate out the collectable from the non-collectable communications in MCTs.[97]

320. In its April 2017 Order, the FISA Court restricted the NSA to collecting MCTs only "*when the target is a party to the entire MCT*." For example, when the target identified by the selector is in the "To" field of each of the email messages in the MCT.[98]

ii. "about" collection

321. Until April 2017, the upstream collection program collected transactions where selectors appeared **anywhere** in a transaction, not just in the sender or receiver fields of the transaction. For example, upstream collection would collect an email if it contained a selector inside the email message's "body" text. The NSA's "about" collection shows that the NSA was scanning the entirety of each of the reassembled transactions for selectors, likely with the same DPI device that was used to review for other selectors, not just the application headers. (See the discussion above about MCTs.) Prior to April 2017, this scanning led to the ingestion of Internet transactions that were

[97] Appendix F at 45 (PCLOB Report at 40).

[98] Appendix E at 26 (FISC Opinion (Apr. 26, 2017)).

"about" a target in addition to transactions sent by or addressed to a target. The PCLOB Report described "about" collection as follows:

> *An "about" communication is one in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not necessarily a participant in the communication. Rather than being "to" or "from" the selector that has been tasked, the communication may contain the selector in the body of the communication, and thus be "about" the selector.*[99]

322. This procedure was controversial because it involved the warrantless reviewing of the contents of Americans' communications and because it involved the collection of many wholly domestic communications where both the sender and receiver of the message were within the U.S. After an extensive review, apparently prompted by the findings of the Foreign Intelligence Surveillance Court that the NSA had not complied with certain procedures related to the upstream collection program, the NSA decided to stop the "about" collection and destroy most of the transactions that had been collected under the "about" collection process.[100]

323. The NSA has not said that it stopped reviewing the entire contents of transactions when it stopped the "about" collection. As mentioned above in ¶¶ 258-259, about collection likely used the same DPI devices that were used to look for communications *to* or *from* a selector, which the NSA still needs to do. "About" collection merely involved retaining transactions with selectors located in parts of a transaction other than in the application headers.

[99] Appendix F at 12 (PCLOB Report at 7).

[100] Appendix X (NSA Press Releases (Apr. 28, 2017)).

324. The recent extension of Section 702 permits the NSA to resume "about" collection under the upstream collection program if it gives proper notice before doing so.[101]

iii. Collection of Encrypted Internet Transactions

325. Under Section 702, the NSA is authorized to collect encrypted Internet transactions and to retain them for an extended period so they can attempt to decrypt them[102]. An HTTPS transaction is an example of an encrypted Internet transaction. In theory, the NSA could configure its IP filters to reject HTTPS traffic by rejecting packets with a destination or source TCP port of 443 but, during her deposition, Rebecca J. Richards followed her lawyer's order to not say if the NSA had done so.[103]

326. In fact, there are obvious reasons that the NSA would seek to collect traffic on port 443 even though it is encrypted.

a. The NSA may, currently or in the future, be able to decrypt important encrypted messages. It is this possibility that justifies the NSA's retention of encrypted communications longer than it is permitted to keep unencrypted communications.[104]

b. For example, the NSA could have compromised the end systems generating or receiving the HTTPS traffic and thus have obtained the keys to permit the transaction to be decrypted. (See ¶ 121.)

---

[101] FISA Amendments Act Reauthorization Act of 2017, Pub. L. No. 115-118, § 103(b).

[102] *See e.g.*, Appendix F at 65, 68 (PCLOB Report at 60, 63); Appendix S at 10 (NSA Section 702 Minimization Procedures (2014)).

[103] Appendix K at 280:13-281:11 (Richards Depo.).

[104] See e.g., Appendix F at 65, 68 (PCLOB Report at 60, 63); Appendix S at 10 (NSA Section 702 Minimization Procedures (2014)).

c. Even if the NSA is not able to decrypt all HTTPS traffic, there is nonetheless useful information that can be obtained from HTTPS transactions including the IP addresses of the Internet user and of the web server. In addition, as discussed in ¶ 123, the domain name of the web server (e.g., www.government.ru) is disclosed in the setup phase of an HTTPS session. In short, even if encrypted, HTTPS communications can reveal who a target is communicating with or which Internet domains he or she is visiting.

d. In addition, as noted in ¶ 109, port numbers are not always a perfect indicator of what application protocol is being used because port numbers can be changed as long as both ends of a communication agree on what port numbers to use. Because of this it is not uncommon for applications to use port 443, the port number assigned for HTTPS, for other uses just to bypass security filters blocking packets using unknown or unwanted ports. Ignoring HTTPS traffic would thus entail ignoring many other types of communications that also use port 443.

e. Finally, HTTPS is one of the most common application-layer protocols used to transmit Internet communications around the world today. Ignoring HTTPS traffic would create a large and needless blind spot.

327. For at least the above reasons, it is very likely that the NSA is reviewing HTTPS transactions whose constituent packets meet the origin or destination criteria for review under upstream collection.

328. Many of the above reasons for collection of HTTPS communications also apply to collecting other forms of encrypted communications, such as communications in

VPNs. For at least these reasons, the NSA would have an incentive to collect encrypted communications of all types.

**e. Stage 5: Ingesting Transactions**

329. The Internet transactions that pass the reviewing stage are then ingested into the NSA's Section 702 databases. (See ¶¶ 231-235.) The following figure shows this stage:

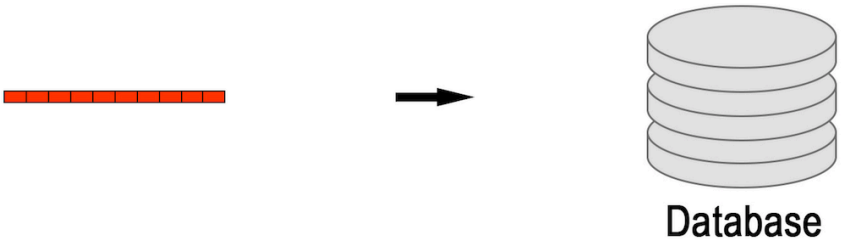



**Figure 39** — Ingesting transactions that contain one or more selectors

330. The above figure shows an Internet transaction, in which the reviewing mechanism found one or more selectors, being ingested into the NSA's Section 702 database.

***3. Upstream Collection Monitor Placement***

331. The NSA has admitted that the upstream collection program collects information from the Internet backbone, and that the Internet backbone consists of high-speed network links between and within ISPs, including terrestrial and undersea fiber cables. (See ¶¶ 150-153.)

332. Since the upstream collection program is limited to collecting Internet transactions where at least one end is outside of the U.S., the logical places to locate upstream collection systems would be at the U.S. end of circuits carried on the undersea and other fiber cables that go between the U.S. and other countries. The FISC, citing the

government's submissions, has confirmed that at least some of the upstream collection program occurs at these points. It has described upstream collection of transactions routed through "*an international Internet link being monitored by the NSA*."[105] As discussed above in ¶¶ 222-223, these locations are also logical places for the NSA to collect communications where both ends are outside the U.S. This non-U.S. collection is feasible because so much of the world's Internet traffic flows through the U.S. (See ¶¶ 222-228.)

333. The NSA has not provided any public information on what percent of the total international public Internet capacity is covered by the upstream collection program, but the government has repeatedly stated that the intention of the upstream collection program is "*to comprehensively acquire communications that are sent to or from its targets*"[106] as long as the communications are not wholly domestic.[107] The NSA refers to the Internet communications it acquires through upstream collection as "*transactions*." (See ¶¶ 63-65.) In order to comprehensively acquire its targets' transactions, the NSA must be comprehensively reviewing Internet transactions to see if they are transactions to or from NSA targets, since the NSA cannot know in advance which of the many transactions on the Internet could be to or from one of the NSA's targets. In order to comprehensively review Internet transactions, the NSA must be comprehensively monitoring the places on the Internet where the non-wholly domestic transactions to or from its targets will transit. If the NSA is not comprehensive in where it does

[105] Appendix P at 45 (FISC Opinion (Oct. 3, 2011)).

[106] Appendix F at 15, 128 (PCLOB Report at 10, 123); see also id. at 148 (PCLOB Report at 143).

[107] Appendix F at 148 (PCLOB Report at 143) ("*[T]he NSA takes additional measures, including the use of IP filters, to try to avoid collecting wholly domestic communications.*").

monitoring, then it cannot be comprehensive in its collection of the transactions to or from its targets. The places where non-wholly domestic transactions to or from its targets will transit include the U.S. ends of the Internet backbone circuits transporting transactions between the U.S. and other countries. (See ¶¶ 200-211.)

334. The NSA has disclosed that it has over 120,000 Section 702 targets, all of them located abroad.[108] The paths that transactions will take between those targets and correspondents in the U.S. are controlled by Internet routing protocols. (See ¶¶ 175-180.) Because of this, in general, the packets that make up these Internet transactions will take the shortest path between the sender and receiver. Using the shortest path will mean that the packets sent by a target located outside the U.S. to a site within the U.S. will generally traverse the topologically closest international link that supports public Internet traffic between the sender's location and the U.S. With thousands of targets in different places around the globe, a wide distribution of international circuits will be used by Internet transactions sent and received by the NSA's targets. In addition, people, including the NSA's targets, move around from time to time, and such movement may change which international circuits their communications use. Thus, the number, distribution and movement of the NSA's targets means that the NSA needs to monitor communications carried by most, if not all, such circuits carried on international cables if it wants to ensure that it captures the communications of those targets.

335. Moreover, regardless of which circuits it monitors, the NSA must also be comprehensive in its monitoring of each circuit. That is, if the NSA's goal is to comprehensively obtain its targets' communications, then it must comprehensively copy,

[108] Appendix Y at 14 (ODNI Statistical Transparency Report for 2017 (Apr. 2018)).

reassemble and review all transactions that could conceivably be to or from a target that transit the circuits being monitored. Since all transactions transiting the monitoring points other than the ones that are wholly domestic could be to or from a target, the NSA must be copying, reassembling and reviewing all, or essentially all, international transactions that transit the circuits being monitored.

## VIII. OPINION D: WIKIMEDIA COMMUNICATIONS ARE TRANSPORTED ON ALL INTERNATIONAL CIRCUITS ORIGINATING OR TERMINATING IN THE UNITED STATES.

336. Wikimedia operates servers in multiple countries to optimize the user experience in different regions of the world. This case concerns the international traffic to and from Wikimedia's U.S.-based servers or users, including the communications between Wikimedia's users outside the U.S. and Wikimedia's U.S.-based servers, the traffic between Wikimedia's non-U.S. servers and its U.S-based users, and the international communications of Wikimedia's staff originating in or terminating in the U.S.

337. Comparing the geographic distribution of international undersea and terrestrial cables, which are used to carry public Internet traffic (which I discussed above in ¶¶ 200-204), with the geographic distribution of countries from which users access Wikimedia's U.S.-based servers (which I discuss below in ¶¶ 341-350) makes it clear that communications to and from Wikimedia's U.S.-based servers are carried on all of the circuits transporting public Internet traffic in the cables connecting the U.S. to other countries.

338. **Opinion D:** Thus, it is my opinion that it is virtually certain that Wikimedia's international communications traverse every circuit carrying public Internet traffic on every international cable connecting the U.S. to other countries.

### A. Wikimedia

339. Wikimedia Foundation is a non-profit organization based in San Francisco, California, that operates twelve free-knowledge projects on the internet, including Wikipedia, Wiktionary, Wikinews, Wikibooks, and Wikisource. Wikipedia is one of the top ten most-visited websites in the world.[109] Wikimedia describes its mission as 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.

340. This case involves Wikimedia's international Internet communications, described more fully below.

#### *1. Wikimedia Websites*

341. People all over the world make use of Wikimedia websites. Most users access the websites in order to get information about some topic. For example, Wikipedia is an online free encyclopedia, Wiktionary is an online dictionary, Wikinews is an online news site, Wikibooks is an online repository with open-content textbooks, and Wikisource is an online free library. All of these sites, and seven more, are capable of supporting people around the world in their native languages. For example, as of January 2018, Wikimedia projects supported web pages in 288 languages.[110]

342. In addition, many people around the world volunteer as content producers and editors for Wikimedia services.

---

[109] *The Top 500 Sites on the Web*, Alexa, https://www.alexa.com/topsites.
[110] Appendix Z at 29 (Wikimedia Responses to Defendants' Interrogatories (Jan. 11, 2018)).

### *2. Wikimedia International Communications*

343. Wikimedia operates servers in multiple countries to optimize the user experience in different regions of the world.

344. For purposes of my analysis below, I focus on Wikimedia's web activity, but my conclusions apply to Wikimedia's communications in total. This case concerns three categories of Wikimedia's international communications:

a. Wikimedia's international communications with its community members, which consist principally of the traffic between Wikimedia's users outside the U.S. and its U.S.-based servers, as well as traffic between Wikimedia's U.S.-based users and its Amsterdam-based servers;

b. communications log information sent from Wikimedia's Amsterdam-based servers to its U.S.-based servers[111]; and

c. international communications of Wikimedia's staff that originate in or terminate in the U.S.

345. Wikimedia has maintained servers in the U.S. in the following locations: Ashburn, Virginia; Carrollton, Texas; Chicago, Illinois; Dallas, Texas; San Francisco, California; and Tampa, Florida.[112]

346. For the six-month period between August 1, 2017 and January 31, 2018, Wikimedia engaged in approximately 760 billion international communications.[113] To put the volume of Wikimedia's Internet traffic in comparative perspective, it operates one

[111] According to Wikimedia's discovery responses, "*Every time Wikimedia receives an HTTP/S request from a person accessing a Wikimedia Project webpage, it creates a corresponding log entry*." Appendix AA at 19 (Wikimedia's Second Amended Responses to Defendants' Interrogatories (Apr. 17, 2018)).

[112] Appendix Z at 26-27 (Wikimedia Responses to Defendants' Interrogatories (Jan. 11, 2018)).

[113] Appendix BB Ex. 1 (Wikimedia Response to ODNI Interrogatory No. 19 (Apr. 6, 2018)).

of the top ten most-visited websites in the world, alongside Google.com, Youtube.com, Facebook.com, and Baidu.com.[114]

347. Not only is the volume of Wikimedia's communications immense, but its millions of users are widely dispersed around the globe. For example, Internet users in every country accessed Wikimedia's U.S.-based servers between August 1, 2017 and January 31, 2018. During that time period, Internet users outside the U.S. made over 380 billion web requests to Wikimedia's servers inside the U.S., and Wikimedia's servers sent over 380 billion responses to those requests. See Appendix BB[115] and the map below:

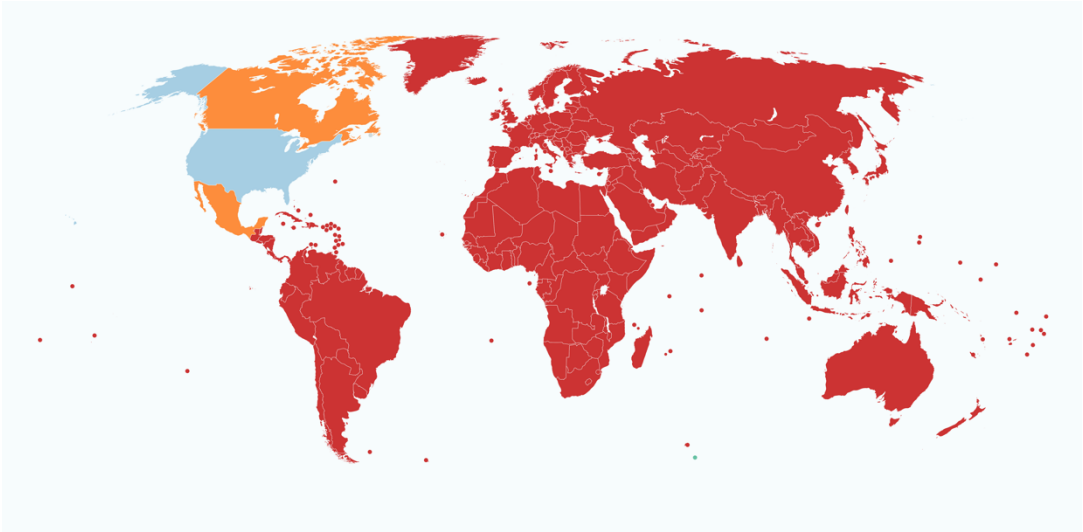


**Figure 40** — Countries from which Wikimedia's U.S. servers received web requests

348. Wikimedia's U.S.-based servers receive web requests via circuits in undersea cables from all the countries colored in red. The websites also receive web requests via terrestrial as well as undersea and under-lake circuits from Canada and Mexico, shown in orange. In summary, Wikimedia U.S.-based servers receive web

[114] *The Top 500 Sites on the Web*, Alexa, https://www.alexa.com/topsites.

[115] Appendix BB (Wikimedia Response to ODNI Interrogatory No. 19 (Apr. 6, 2018)).

requests from all of the world's inhabited continents and islands. Thus, Wikimedia users are very widespread. To provide some context, Wikimedia's U.S.-based servers receive hundreds of billions of requests annually and provide at least as many responses. Even with a large number of international circuits, there are very many Wikimedia communications on each circuit. For example, even if there are thousands of international circuits, there would still be hundreds of millions of Wikimedia communications on the average circuit.

349. The paths that Internet communications take between Wikimedia users outside the U.S. and Wikimedia servers in the U.S. are controlled by Internet routing protocols. (See ¶¶ 175-180.) Because of this, in general, the packets that make up these Internet communications will take the shortest path between the sender and receiver. Using the shortest path will mean that the packets sent by a user located outside the U.S. to a server within the U.S. will generally traverse the topologically closest international circuit that supports public Internet traffic between the user's location and the U.S. With Wikimedia users located in all of the world's inhabited continents and islands, the widest possible distribution of international circuits will be used by Internet communications sent and received by the Wikimedia users.

350. Thus, it is my opinion that it is virtually certain that Wikimedia's international communications traverse every circuit carrying public Internet traffic on every international cable connecting the U.S. to other countries, including the "international Internet links" monitored by the NSA.

### *3. Protocol Support on Wikimedia Websites*

351. Wikimedia websites support both HTTP and HTTPS. Within Wikimedia's foreign-to-U.S. HTTP and HTTPS communications, the percentage of communications that use HTTPS had been growing and is now about 97.7% overall.[116] But there are a number of countries where the percentage is much lower. For example, 38% of Iranian communications with Wikimedia's U.S.-based servers use HTTP, as do 28% of Irish communications, 24% of Chinese communications, 19% of Dutch communications, and 16% of Finnish communications (all with Wikimedia's U.S.-based servers).[117] To provide context, Wikimedia's U.S.-based servers received over 8 billion HTTP requests from foreign users in the six months between August 1, 2017 and January 31, 2018.[118]

352. As discussed above in ¶¶ 122, 326, even encrypted Internet transactions can still reveal important information or can be saved for later attempts at decryption. In other words, just because a communication is encrypted does not mean that the NSA will not copy, scan or collect it.

## IX. OPINION E: THE NSA HAS COPIED, REASSEMBLED AND REVIEWED WIKIMEDIA COMMUNICATIONS

353. Based on my conclusions above in Opinions A–D, as well as the other features of upstream surveillance I've discussed, I conclude that: Even if the NSA were monitoring only a single circuit under upstream collection, it would be copying and

[116] Appendix AA (Wikimedia's Second Amended Responses to Defendants' Interrogatories (Apr. 17, 2018)).

[117] Id.

[118] Appendix BB, Exhibit 1

reviewing at least some of Wikimedia's communications. Moreover, while it is unnecessary to my conclusion here, the government's officially released documents indicate that the NSA is monitoring multiple circuits, which only increases my confidence that the NSA is copying and reviewing Wikimedia's communications. In fact, for the reasons discussed above in ¶¶ 332-333, the NSA is very likely to be monitoring a large number of international circuits, given that it would need to monitor **most, if not all,** such circuits to accomplish its stated (and unsurprising) goal of reliably and comprehensively collecting the communications of its targets.[119]

354. Moreover, the NSA's need to monitor most, if not all, communications carried by international circuits in order to comprehensively acquire its targets' communications makes it highly likely that the NSA is copying and reviewing some of Wikimedia's communications in each of its categories of international communications. (See ¶ 343.)

355. The NSA's monitoring of many circuits would only increase the volume of Wikimedia communications that the government is intercepting, copying and reviewing in the course of its upstream collection program.

356. **Opinion E:** Thus, it is my opinion that it is virtually certain that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications.

[119] Appendix F at 15, 128, 148 (PCLOB Report at 10, 123, 143)

## X. DR. SCHULZRINNE'S DECLARATION

357. The government submitted a declaration by Dr. Henning Schulzrinne in support of its motion for summary judgment. Dr. Schulzrinne is a computer scientist at Columbia University. I have known him for many years having first met at the IETF. The government appears to have asked Dr. Schulzrinne to address a different question than Wikimedia's counsel asked me to address. Wikimedia's counsel asked me to address the likelihood that the NSA has, in the course of upstream collection, copied, reassembled or reviewed at least some of Wikimedia's communications. Dr. Schulzrinne's declaration does not address that question. He does not state any opinion about the likelihood that the NSA has copied, reassembled or reviewed Wikimedia's communications.

358. Nor does Dr. Schulzrinne mention many of the critical features of upstream collection on which I base my conclusion that it is a virtual certainty that the NSA has copied, reassembled or reviewed at least some of Wikimedia's communications.

359. For example, he does not address the number of targets of Section 702 surveillance that the government has acknowledged (over 120,000 as of April 2018); he does not acknowledge the NSA's stated goal of "*comprehensively acquir[ing] communications that are sent to or from its targets*";[120] he does not discuss the asymmetric routing of communications on the Internet; he does not mention the special permission the NSA has under Section 702 to collect and analyze encrypted communications; he does not acknowledge that useful information can be obtained from

[120] Appendix F at 15 (PCLOB Report at 10).

the scanning of encrypted Internet communications even if their content cannot be decrypted; and he does not acknowledge that the NSA has publicly conceded that it monitors "*web activity*."

360. In his declaration, Dr. Schulzrinne makes one point about how surveillance can be performed on the Internet, and one about how the NSA could avoid Wikimedia traffic.

361. In regards to the mechanisms of surveillance, Dr. Schulzrinne describes (as I also describe) that there are two configurations of equipment with which the NSA could be obtaining copies of the Internet communications it will review for selectors. Dr. Schulzrinne states that the second configuration (what I call an ***in-line filter***, see ¶¶ 279-281) "*would be desirable*."[121] I disagree with his conclusion. (See ¶¶ 288, 363-365.)

362. Second, Dr. Schulzrinne speculates that the NSA could, as a technical matter, filter out some types of communications so that its surveillance equipment would not copy, reassemble or review any of Wikimedia's communications. Dr. Schulzrinne's explanation is not entirely accurate as a technical matter, and it is simply implausible as a practical matter given everything that is known about upstream collection. (See ¶ 367.)

### A. Surveillance Configurations

363. Dr. Schulzrinne describes the same two surveillance configurations as I do. I referred to them as the ***copy-then-filter*** and the ***in-line filter*** configurations. (See ¶¶ 269-289.) Dr. Schulzrinne says that the in-line filter configuration would be desirable as compared to the copy-then-filter configuration because it would reduce the volume of communications that would need to be scanned. As I mentioned above in ¶ 288, I do not

[121] Schulzrinne Decl. ¶ 57.

think that reducing the volume of communications is all that important because modern DPI equipment can, either singularly or in parallel, keep up with the traffic in the type of channels the NSA is dealing with. To the extent that such an in-line filter would permit cheaper DPI equipment to be used, it might be desirable, but there are other important countervailing factors, as described below.

364. Dr. Schulzrinne describes the filtering being done using the mirror function in the ISP's existing routers. If that were the case, it would avoid the need for extra network equipment (the fiber-optic splitter) that would be required in the copy-then-filter configuration. But, as I discuss above in ¶ 287, if the filter function is implemented using the mirror function in the ISP's router, the filter functions would likely have to be limited to some non-secret set of filters such as the list of IP address ranges that are located in the U.S. Otherwise the ISP technician who configures the router, the router itself and the backup systems used to manage the router would be dealing with secret information (the filter criteria), which, if it were to be compromised, would give a roadmap on how to avoid NSA collection. The copy-then-filter configuration has the advantage that the filter device could be entirely under the control of the NSA and thus avoid the risk of the ISP personnel having access to potentially secret filter configurations.

365. In the copy-then-filter configuration, all Wikimedia traffic that transits a channel that the NSA is monitoring will be copied. In the in-line filter case, unless the filter was set to filter with a higher degree of selectiveness than checking to see if the IP addresses are in the U.S. or not then all international Wikimedia traffic that transits a

channel that the NSA is monitoring will be copied. In both cases all international Wikimedia traffic would be copied.

**B. Selectively Filtering Internet Traffic**

366. Dr. Schulzrinne spends considerable time discussing the possibility that the NSA could use selective filtering to avoid Wikimedia traffic. He describes using the traffic mirror function present in some ISP routers to blacklist or whitelist IP addresses or protocols.[122] While such filtering is technically possible, there are a number of reasons to conclude that Dr. Schulzrinne's hypotheticals are implausible and, accordingly, that it is implausible that the NSA is engaging in such filtering.

a. As discussed above in ¶¶ 285-289, having the mirror function in the ISP router do advanced selective filtering would mean that the configuration of the mirror function would include secret information, complicating the protection of such information.

b. Adding any protocol specific blocklist, for example not including any packets with port 443 (HTTPS) or protocol 50 (IP Sec) in reassembly and review, would create a blind spot that would provide a path by which an NSA target could communicate without the communications being detected. Sophisticated targets could easily probe to find any such blind spots and exploit them.

c. As discussed in ¶ 288, there is no particular reason to think that selective filtering is needed to reduce the load on the DPI devices. In any case, while the total number of Wikimedia's mostly text-based communications is immense, the total amount of those communications in bytes is minuscule as

[122] Id. ¶¶ 63-71.

compared to YouTube's video-based traffic. If filtering traffic for performance reasons were desirable, the NSA would get much more result from filtering YouTube than from filtering Wikimedia.

d. Dr. Schulzrinne mentions using ***whitelists*** (lists of addresses the NSA is interested in) rather than ***blacklists*** (lists of addresses the NSA wants to ignore).[123] As a practical matter, whitelists are almost useless for the type of collection program the NSA is running. Whitelisting requires knowing in advance all of the IP addresses that might be used by each of the NSA's targets as well as assuming that those targets are not moving around and thereby changing their IP addresses. This is not remotely possible. (See ¶¶ 137, 140, 173-174, 229-230, 244-247, 334.)

e. Dr. Schulzrinne suggests selectively filtering applications, for example by using the port number in the transport header.[124] As I discuss in ¶ 109, the use of a particular port number does not mean that a particular application is being used. Port numbers are only advisory in that pairs of Internet devices can decide what application they want to run on a port—for example, running email using port 80 to avoid firewalls. If the NSA were blacklisting traffic using specific ports, it would provide another path that NSA targets could use to avoid collection.

[123] Id. ¶¶ 65-66.

[124] Id. ¶¶ 70-71.

f. One example application Dr. Schulzrinne suggests could be blacklisted is the world wide web (ports 80 and 443).[125] Doing so would leave a very large hole in the NSA's collection ability. The hole would include web email, web chat, web-based editors which have been used to send hidden messages, ISIS videos and the like. In addition, the NSA acknowledges collecting web traffic.[126] (See ¶¶ 314-315.)

g. Dr. Schulzrinne specifically suggests blacklisting HTTPS (port 443). As mentioned just above, the fact that a communication uses port 443 does not mean that the communication is actually HTTPS or even that the communication is encrypted. In addition, as I discuss above in ¶ 326, there are many obvious reasons to believe the NSA is acquiring HTTPS communications, including the fact that the NSA is expressly authorized to collect encrypted Internet communications, and that one can learn a lot from an encrypted HTTPS session, including the IP addresses of the user and server and the domain name of the server.

h. Even if the NSA were blacklisting HTTPS, it would still be virtually certain that the NSA would still be copying, reassembling and reviewing Wikimedia HTTP communications considering the number and distribution of those communications. (See ¶ 351.)

[125] Id. ¶ 79.

[126] Appendix C at 30 (FISC Submission (June 1, 2011)).

### C. Selectively Filtering Wikimedia IP addresses

367. Dr. Schulzrinne posits that the NSA could "blacklist" Wikimedia's IP addresses and suggests that if the NSA did so, "*NSA would receive no access to Wikimedia HTTP or HTTPS communications (or, for that matter, Wikimedia communications of any kind)*" (Schulzrinne Decl. ¶ 81). As I show below, that claim is technologically inaccurate and entirely implausible. Dr. Schulzrinne concedes that he has no evidence to support the possibility that the NSA made such a decision, and he does not offer his view on the **likelihood** that the NSA would make such a decision; he merely claims that it is technically possible.[127]

a) In my opinion it is basically inconceivable that the NSA would have decided to blacklist Wikimedia IP addresses. Given that there are millions of websites on the public Internet, the idea that the NSA would have gone through them to decide which to monitor and which not to, in addition to being an incredibly resource-intensive task, is just totally unbelievable. Any such blacklist would purposefully create blind spots in the upstream collection program that could be exploited by NSA targets to bypass surveillance. Including Wikimedia IP addresses in any such blacklist would deliberately limit the possible collection of information on the use of Wikimedia resources by NSA targets, a potentially valuable source of information about the online research and reading of its targets. Viewed in total, taking into account the total lack of any evidence supporting the possibility that the NSA took such action, the idea that the NSA made a deliberate decision to avoid Wikimedia communications seems entirely implausible.

[127] Schulzrinne Decl. ¶ 77

b) It is also technologically incorrect that blocking Wikimedia's IP addresses would block all Wikimedia traffic. Even if NSA blacklisted Wikimedia's IP addresses, Wikimedia's communications would still be copied, reassembled and reviewed by the NSA in at least several circumstances:

(1) MCTs that contain Wikimedia communications, where the enclosing communication is not to or from Wikimedia, but one or more of the embedded communications are to or from Wikimedia.

(2) In the case where a person located outside the U.S. is using an email service located inside the U.S. to send email to Wikimedia. The first "leg" of the journey the email takes from the user's mail agent to the email server would be subject to copying, reassembly and review because the transaction carrying the email message is not wholly domestic. The same is true in reverse: email from Wikimedia to such a person outside the U.S. would not be seen as wholly domestic in the leg between the email service and the user's mail agent. In both of the above cases, the email transaction transiting the international circuit would not have any Wikimedia IP addresses in the IP headers of the packets such that they could be discarded by an IP address-based blacklist.

(3) The traffic between a VPN service in the U.S. and a user located outside the U.S. would not have Wikimedia IP addresses in the traffic even if the user were accessing a Wikimedia site.

c) In any case, the NSA's descriptions of its IP address filtering all state that the goal is to filter out "*wholly domestic communications*,"[128] and these descriptions do not contain any mention of any other goals for the filtering.

**D. U.K. Surveillance Disclosures and Court Proceedings**

368. The U.K.'s signals intelligence agency, Government Communications Headquarters (GCHQ), is charged with performing the functional equivalent of upstream collection in the U.K.[129] GCHQ's public disclosures reinforce my conclusion that, for various technical and practical reasons, the NSA copies the entire stream of communications on a circuit it is monitoring. The GCHQ has explained in court filings that, for "*technical reasons*" and "*as a matter of practical necessity*," it needs to intercept the entire stream of communications on a circuit (which GCHQ refers to as a "*bearer*") when engaging in its equivalent of upstream collection:

> *As explained in detail in the Observations, the s.8(4) Regime operates in this way as a matter of practical necessity. For technical reasons, it is necessary to intercept the entire contents of a bearer, in order to extract even a single specific communication for examination from the bearer: Observations, §§1.31-1.34.*[130]
>
> *Subjects of interest are very likely to use a variety of different means of communication, and to change those means frequently. Moreover, electronic communications do not traverse the internet by routes that can*

[128] Appendix D at 7-8 (NSA Response to Plaintiff's Interrogatory No. 3 (Dec. 22, 2017)); Appendix F at 46, 125, 148 (PCLOB Report at 41, 120, 143); Appendix H at 7-8 (NSA Response to Plaintiff's Request for Admission No. 6 (Jan. 8, 2018)).

[129] Appendix DD ¶ 12 (*Case of Big Brother Watch & Others v. United Kingdom*, Eur. Ct. H.R., ¶ 12 (2018), http://hudoc.echr.coe.int/eng?i=001-186048).

[130] Appendix EE ¶¶ 7-8 (Further Observations of the Government of the United Kingdom ¶¶ 7-8, *10 Human Rights Organizations v. United Kingdom*, Eur. Ct. H.R. (Dec. 16, 2016), https://privacyinternational.org/sites/default/files/2018-02/2016.12.16%20Government%27s%20further%20obs.pdf).

> *necessarily be predicted. Communications will not take the geographically shortest route between sender and recipient, but the route that is most efficient, as determined by factors such as the cost of transmission, and the volume of traffic passing over particular parts of the internet at particular times of day. So in order to obtain even a small proportion of the communications of known targets overseas, it is necessary for the Services to intercept a selection of bearers, and to scan the contents of all those bearers for the wanted communications.*[131]

369. In its ruling, the European Court of Human Rights repeated this description of how the U.K.'s Internet surveillance program operates.[132] In spite of the fact that the GCHQ may not be operating under the same requirement to exclude wholly domestic U.K. traffic from its collection program, GCHQ's practice—and the reasons it has publicly described—reinforce my conclusions that the NSA relies on the copy-then-filter configuration to conduct the upstream collection program and that it does not selectively filter traffic prior to copying it as Dr. Schulzrinne hypothesizes it could.

370. But even if Dr. Schulzrinne's hypothesis that the NSA is filtering certain traffic before copying the remainder were to be true, for the reasons I set forth above, it is virtually certain that the NSA has, in the course of the upstream collection program, copied, reassembled and reviewed at least some of Wikimedia's communications. This, also for the reasons I set forth above, is also true in the highly improbable scenario that

[131] Appendix FF ¶¶ 1.29-1.31, 4.5-4.6 (Observations of the Government of the United Kingdom, ¶¶ 1.29-1.31, 4.5-4.6, *10 Human Rights Organizations v. United Kingdom*, Eur. Ct. H.R. (Apr. 16, 2016), https://privacyinternational.org/sites/default/files/2018-02/United%20Kingdom%E2%80%99s%20Observations%20on%20the%20Merits.pdf).

[132] Appendix DD ¶ 284 (*Case of Big Brother Watch & Others v. United Kingdom*, Eur. Ct. H.R., ¶ 284 (2018)).

Dr. Schulzrinne hypothesizes that the NSA has been purposefully blacklisting Wikimedia IP addresses from the upstream collection program.

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

Date: 12/18/18

Scott Bradner

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

WIKIMEDIA FOUNDATION,

*Plaintiff*,

v.

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

*Defendants*.

No. 1:15-cv-00662-TSE

**DECLARATION OF SCOTT BRADNER**
**APPENDIX LIST**

Curriculum vitae .....A

List of documents provided by Plaintiff's counsel .....B

FISC Submission (June 1, 2011) .....C

NSA Responses to Plaintiff's Interrogatories (Dec. 22, 2017).....D

FISC Opinion (Apr. 26, 2017) .....E

Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (July 2, 2014).....F

Paul Baran, RAND Corp., *On Distributed Communications Networks* (Sept. 1962).....G

NSA Responses to Plaintiff's Requests for Admission (Jan. 8, 2018) .....H

David Hauweele et al., *What Do Parrots and BGP Routers Have in Common?*, Computer Comm. Rev. (July 2016) .....I

Report on International Submarine Cables Landing in the US, TeleGeography (Jan. 2018).....J

Transcript of Deposition of Rebecca J. Richards (Apr. 16, 2018).....K

NSA Director of Civil Liberties & Privacy Office, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (Apr. 16, 2014).....L

FISC Submission (May 2, 2011) .....M

FISC Submission (Aug. 16, 2011).....N

Joint Statement, *FISA Amendments Act Reauthorization: Hearing Before the H. Permanent Select Comm. on Intelligence* (Dec. 8, 2011) .....O

FISC Opinion (Oct. 3, 2011).....P

Privacy & Civil Liberties Oversight Board, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014).....Q

FISC Submission (June 28, 2011) .....R

NSA Section 702 Minimization Procedures (2014) .....S

NSA Section 702 Targeting Procedures (2014).....T

FISC Hearing Transcript, *In Re: DNI/AG 702(g) Certification* [*Redacted*] (2008).....U

Shuihui Chen & Yong Tang, *A Stream Reassembly Mechanism Based on DPI*, Inst. of Electrical & Electronics Engineers (2012) .....V

U.S. Patent No. 8,813,221.....W

NSA Press Releases (Apr. 28, 2017) .....X

ODNI Statistical Transparency Report for 2017 (Apr. 2018).....Y

Wikimedia Responses to Defendants' Interrogatories (Jan. 11, 2018).....Z

Wikimedia Second Amended Responses to Defendants' Interrogatories (Apr. 17, 2018).....AA

Wikimedia Amended Response to ODNI Interrogatory No. 19 (Apr. 6, 2018).....BB

City of Virginia Beach Dep't of Info. Tech., *Next Generation Network and Transoceanic Subsea Cable Updates* (Oct. 4, 2017) .....CC

*Case of Big Brother Watch & Others v. United Kingdom*, Eur. Ct. H.R. (2018) .....DD

Further Observations of the Government of the United Kingdom, *10 Human Rights Organizations v. United Kingdom*, Eur. Ct. H.R. (Dec. 16, 2016) .....EE

Observations of the Government of the United Kingdom, *10 Human Rights Organizations v. United Kingdom*, Eur. Ct. H.R. (Apr. 16, 2016) .....FF

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

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

**DECLARATION OF SCOTT BRADNER**
**APPENDIX LIST**

Curriculum vitae .....A

List of documents provided by Plaintiff's counsel .....B

FISC Submission (June 1, 2011) .....C

NSA Responses to Plaintiff's Interrogatories (Dec. 22, 2017).....D

FISC Opinion (Apr. 26, 2017) .....E

Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* (July 2, 2014).....F

Paul Baran, RAND Corp., *On Distributed Communications Networks* (Sept. 1962).....G

NSA Responses to Plaintiff's Requests for Admission (Jan. 8, 2018) .....H

David Hauweele et al., *What Do Parrots and BGP Routers Have in Common?*, Computer Comm. Rev. (July 2016) .....I

Report on International Submarine Cables Landing in the US, TeleGeography (Jan. 2018).....J

Transcript of Deposition of Rebecca J. Richards (Apr. 16, 2018).....K

NSA Director of Civil Liberties & Privacy Office, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (Apr. 16, 2014).....L

FISC Submission (May 2, 2011) .....M

FISC Submission (Aug. 16, 2011).....N

Joint Statement, *FISA Amendments Act Reauthorization: Hearing Before the H. Permanent Select Comm. on Intelligence* (Dec. 8, 2011) .....O

FISC Opinion (Oct. 3, 2011).....P

Privacy & Civil Liberties Oversight Board, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014).....Q

FISC Submission (June 28, 2011) .....R

NSA Section 702 Minimization Procedures (2014) .....S

NSA Section 702 Targeting Procedures (2014).....T

FISC Hearing Transcript, *In Re: DNI/AG 702(g) Certification* [*Redacted*] (2008).....U

Shuihui Chen & Yong Tang, *A Stream Reassembly Mechanism Based on DPI*, Inst. of Electrical & Electronics Engineers (2012) .....V

U.S. Patent No. 8,813,221.....W

NSA Press Releases (Apr. 28, 2017) .....X

ODNI Statistical Transparency Report for 2017 (Apr. 2018).....Y

Wikimedia Responses to Defendants' Interrogatories (Jan. 11, 2018).....Z

Wikimedia Second Amended Responses to Defendants' Interrogatories (Apr. 17, 2018).....AA

Wikimedia Amended Response to ODNI Interrogatory No. 19 (Apr. 6, 2018).....BB

City of Virginia Beach Dep't of Info. Tech., *Next Generation Network and Transoceanic Subsea Cable Updates* (Oct. 4, 2017) .....CC

*Case of Big Brother Watch & Others v. United Kingdom*, Eur. Ct. H.R. (2018) .....DD

Further Observations of the Government of the United Kingdom, *10 Human Rights Organizations v. United Kingdom*, Eur. Ct. H.R. (Dec. 16, 2016) .....EE

Observations of the Government of the United Kingdom, *10 Human Rights Organizations v. United Kingdom*, Eur. Ct. H.R. (Apr. 16, 2016) .....FF

DECLARATION OF SCOTT BRADNER

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

# Appendix A

# SCOTT BRADNER

## WORK EXPERIENCE

- Senior Technology Consultant, Office of the CTO, Harvard University, Cambridge, MA, 2012 to 2016. Exploring, developing and upgrading technology at Harvard, monitoring changing technology trends and exploring their potential for use at Harvard. Last focus was on implementing cloud-based identity and access management applications.
- University Technology Security Officer, Office of the CTO, Harvard University, Cambridge, MA, 2011 to 2012.
- University Technology Security Officer, Office of the CIO, Harvard University, Cambridge, MA, 2008 to 2011. Developed and maintained university IT security policies, assessed compliance with such policies, provided advice on IT security issues.
- University Technology Security Officer, Office of the Assistant Provost for Information Systems, Harvard University, Cambridge, MA, 2004 to 2008. Developed and maintained university IT security policies, assessed compliance with such policies, provided advice on IT security issues.
- Senior Technical Consultant, Office of the Assistant Provost for Information Systems, Harvard University, Cambridge, MA, 1996 to 2008. Assist Assistant Provost in ascertaining the implications of advanced technology on the University, served as a liaison to various University groups dealing with technology issues.
- Senior Technical Consultant, Office for Information Technology (OIT), Harvard University, Cambridge, MA, 1989 to 1996. Design data networks, install and operate production gateways, served as OIT liaison to external organizations, oversee installation of fiber infrastructure, develop network based applications, develop recommendations on security and privacy, document existing Harvard network and network support organization.
- Founded and managed the Harvard Network Device Test Lab, 1988 to 1999.
- Senior Technical Consultant, Psychology Department, Harvard University, Cambridge, MA, 1975 to 1990. Managed computer facility consisting of UNIX computers, PCs and Macintosh computers, developed phototypesetting facility, designed and installed first Harvard campus data network and designed the Longwood Medical Area Network.

- Computer Programmer, Psychology Department, Harvard University, Cambridge, MA, 1966 to 1975. Co-developed real-time operating system and designed special hardware to support real-time research experiments.
- Computer Programmer, Information International Incorporated, Cambridge, MA, 1964 to 1965. Worked on film scanning systems.
- Lab technician, Children's Hospital Cancer Institute, Boston, MA, 1964.

## TEACHING

- Instructor, Harvard University Extension School, from 1995 to the present. Teaching classes in *Technology, Security, Privacy, and the Realities of the Cyber World*. Previously taught *Advanced Topics in Data Networking Protocols and Network Architecture* and *Security, Privacy, and Usability*, also at the Harvard University Extension School
- Tutorial Instructor, Networld + Interop, from 1990 to 2001. (Now known as Interop.) Taught classes in multiprotocol enterprise and Internet service provider data networking.
- Tutorial Instructor, IBM Corporation, from 1990 to 1995. Taught classes in advanced TCP/IP data networking.
- Senior Preceptor, Harvard University, 1982 to 1990. Taught classes in the use of computers in psychology and supervised special projects in computer and networking electronics and in computer programming.

## CONSULTING

- Consultant on network design, management and security to educational institutions, Federal agencies, international telecommunications enterprises and commercial organizations ranging from Fortune 500 companies to small businesses, 1989 to present. Served as an Expert Witness in a number of legal cases including the Communications Decency Act challenge in the U.S. Federal court.

## PATENTS

- US Patent 4,799,262 - *Speech Recognition* (with Joel A. Feldman and William F. Ganong, III) 1989

## AWARDS

- The Jonathan B. Postel Service Award from the Internet Society
- The Petra T. Shattuck Excellence in Teaching Award from the Harvard University Extension School

## ORGANIZATIONS

### Internet Engineering Task Force (IETF)

- Consultant to IAOC and IETF Trust (2016 to present)
- Member, IETF Administrative Oversight Committee (IAOC) of the IETF Administrative Activity (IASA) (2012 to 2016)
- Co-Chair, Operations and Management Area Working Group (opsawg), (2007 to 2016)
- Co-Chair, Authority-to-Citizen Alert Working Group (atoca), (2010 to 2012)
- Co-Chair, Congestion and Pre-Congestion Notification Working Group (pcn), (2007 to 2012)
- Co-Chair, Internet Emergency Preparedness Working Group (ieprep), (2002 to 2007).
- Liaison between IETF and ITU-T, (1995 to 2009).
- Chair, New IETF Standards Track Discussion Working Group (newtrk), (2004 to 2006).
- Member, IETF Internet Engineering Steering Group (1993 to 2003).
- Co-Director, Sub-IP Area (2001 to 2003).
- Co-Chair, Transport Area Working Group (tsvwg), (1999 to 2003).
- Co-Director, Transport Area (1997 to 2003).
- Co-Director, IPng Area (1993 to 1996).
- Co-Director, Operational Requirements Area (1993 to 1997).
- Chair, Benchmarking Methodology Working Group (bmwg), (1990 to 1993).
- Edited or co-edited many IETF process and IPR documents (RFC 2026, RFC 2028, RFC 2418, RFC 2436, RFC 2438, RFC 2690, RFC 2691, RFC 3113, RFC 3131, RFC 3233, RFC 3356, RFC 3427, RFC 3667, RFC 3668, RFC 3978, RFC 3979, RFC 4053, RFC 4748, RFC 4775, RFC 5378, RFC 6756, RFC 7127, and RFC 7691).
- Maintained and presented IETF newcomers tutorial (2003-2016) (IETF meeting: 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, and 95).
- Editor of most cited RFC (RFC 2119).

## Internet Society (ISOC)

- Secretary of the Board (2003 to 2016)
- Vice President for Standards, (1995 to 2003).
- Trustee, (1993 to 1999).

## The American Registry for Internet Numbers (ARIN)

- Vice Chair of the Board (2011 to 2012)
- Treasurer (2009 to 2010)
- Secretary of the Board (1997 to 2009)
- Trustee, (1997 to 2012)

## IEEE Internet Computing

- Editorial Board, (1999 to 2008).

## Wiley Computer Publishing

- Wiley Network Council, (1997 to 2000). Technical editing for a number of books including: Internet Performance Survival Guide, by G. Huston; Converged Networks and Systems, by I. Faynberg; Network Services Investment Guide: Maximizing ROI in Uncertain Times, by M. Gaynor; Network Routing Basics: Understanding IP Routing in Cisco Systems, by J. Macfarlane; The NAT Handbook: Implementing and Managing Network Address Translation, by B. Dutcher; and WAN Survival Guide: Strategies for VPNs and Multiservice Networks, by H. Berkowitz

## Corporation for Regional and Enterprise Networking, Inc. (CoREN)

- Co-chair, Joint MCI-CoREN Technical Committee (1994 to 1995)

## New England Academic and Research Network (NEARnet)

- Co-founder
- Member, Steering Committee (1989 to 1995)
- Chair, Technical Committee (1989 to 1995)

## Longwood Medical Area Network

- Chair, Technical Committee (1991 to 1995)

## Technical Advisory Boards

- I have been on over two dozen technical advisory boards over the years.

**Member, ACM, IEEE, ISOC**

## SELECTED PUBLICATIONS

### Columns

- *Net Insider*, Network World, 1992 to 2013
- *View from the USA*, Nikkei Communications, 1997 to 1999

### Papers and Articles

- Gaynor, M., L. Lenert, K. D. Wilson and S. Bradner, Why common carrier and network neutrality principles apply to the Nationwide Health Information Network (NWHIN), Journal of American Medical Informatics Association, 2013
- Gaynor, M, F. Yu, C. Andrus, S. Bradner and J. Rawn, A General Framework for Interoperability with Applications to Healthcare, Health Policy and Technology, January 2013
- Bellovin, S., S. Bradner, W. Diffie, S. Landau, and J. Rexford., As Simple as Possible - But Not More So, Communications of the ACM, August 2011
- Bellovin, S., S. Bradner, W. Diffie, S. Landau, and J. Rexford, Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure, Harvard Law School National Security Journal, May 2011
- Gaynor, M., A. Pearce, S. Bradner, and Ken Post, Open Infrastructure for a Nationwide Emergency Services Network, International Journal of Information Systems for Crisis Response Management (IJISCRAM), 2009
- Gaynor, M., and S. Bradner, Statistical Framework to Value Network Neutrality, Media Law & Policy, New York Law School, March 2008
- Gaynor, M. and S. Bradner, Valuing Network Neutrality, Broadband Properties, December 2007
- claffy, kc, S. Meinrath and S. Bradner, The (un)Economic Internet?, IEEE Internet Computing, May/June 2007
- Bradner, S., The End of End-to-End Security, IEEE Security & Privacy, March/April 2006
- Goodell, G., M. Roussopoulos and S. Bradner, A Directory Service for Perspective Access Networks, Harvard University Computer Science Group Technical Report TR-06-06, 2006
- Goodell, G., S. Bradner and M. Roussopoulos, Building a Coreless Internet without Ripping out the Core, Hotnets05, November 2005

- Bradner, S. and C. Metz, Guest Editor's Introduction: The Continuing Road toward Internet Media, IEEE Internet Computing, July-August, 2005
- Bradner, S., Internet governance - a train on many tracks, ARIN newsletter, December 2004
- Gaynor, M., S. Bradner A Real Options Metric to Evaluate Network, Protocol, and Service Architecture, Computer Communication Review (CCR), October 2004
- McKnight, L., J. Howison, and S. Bradner, Wireless Grids: Distributed Resource Sharing by Mobile, Nomadic, and Fixed Devices, IEEE Internet Computing, July-August 2004
- Goodell, G., S. Bradner and M. Roussopoulos, Blossom: A Decentralized Approach to Overcoming Systemic Internet Fragmentation, Harvard University Computer Science Group Technical Report TR-25-04, 2004
- Kung, H.T., C-M. Cheng, K-S Tan, and S. Bradner, Design and Analysis of an IP-Layer Anonymizing Infrastructure, Proceedings of the third DARPA Information Survivability Conference and Exposition (DISCEX 3), April 2003
- Bradner, S., Are Global Internet-Related Standards Possible?, International Journal of IT Standards and Standardization Research, Jan-Mar 2003
- King, K. and S. Bradner, Internet Emergency Preparedness in the IETF, Applications and the Internet Workshops, Jan 2003
- Kung, H.T., S. Bradner, and K. S. Tan, An IP-layer Anonymizing Infrastructure, MILCOM 2002, Anaheim, CA, October 2002
- Bradner, S., Internet Telephony -- Progress Along the Road, IEEE Internet Computing, May/Jun 2002
- Gaynor, M. and S. Bradner, The Real Options Approach to Standardization, Proceedings of Hawaii International Conference on Systems Science, Jan 2001
- Gaynor, M., S. Bradner, M Iansiti, and HT Kung, The Real Options Approach to Standards for Building Network-based Services, Proceeding of IEEE Conference on Standardization and Innovation in Information Technology, Oct 2001
- Gaynor, M. and S. Bradner, Using Real Options to Value Modularity in Standards, Journal of Knowledge Technology & Policy (Special issue on IT standards)
- Bradner, S., Virtual networking: reflections on the status of ATM, Journal of High Speed Networks, Volume 6, Number 3, 1997

- Bradner, S., The Bradner Report: The yet untold story and barking dogs, Network Computing, Aug 15, 1997
- Bradner, S., The Bradner Report, Network Computing, July 15, 1996
- Bradner, S., The Bradner Report 1995, Network Computing May 15, 1995
- Bradner, S., The Bradner Bridge Report, Network Computing, October 1, 1994
- Bradner, S., The Exclusive Bradner Report, Network Computing, September 1, 1994
- Bradner, S. and D. Greenfield, Building the Highway, PC Magazine, March 30, 1993
- Bradner, S., Rooting out the Best Routers, SunExpert Magazine, October 1992
- Bradner, S., Bridges or Routers: What Matters?, 3TECH The 3Com Technical Journal, Winter 1992
- Bradner, S., Ethernet Bridges and Routers: Faster Than Fast Enough, Data Communications, February 1992
- Bradner, S., Testing Multiprotocol Routers: How Fast is Fast Enough?, Data Communications, February 1991

## Books

- Bradner, S., *Forward* in *The Complete April Fools' Day RFCs*, compiled by T. Limoncelli and P. Salus, Peer-to-Peer Communications, 2007, ISBN 13: 978-1-57398-042-5
- Bradner, S., *Forward* in *TCP/IP for Dummies* by C. Leiden and M. Wilensky, Wiley Publishing, 2003, ISBN 0-7645-1760-0
- National Research Council, *The Digital Dilemma*, The National Academies Press, 2000, ISBN: 978-0-309-06499-6
- Bradner, S., *Current Trends in the IETF and Voice over IP*, chapter in *Carrier IP Telephony 2000*, The International Engineering Consortium, 2000, ISBN 0-933-21775-7
- Bradner, S., *The Internet Engineering Task Force*, a chapter in *Open Sources: Voices from the Open Source Revolution,* edited by C. DiBona, S. Ockman & M. Stone, O' Reilly, 1999, ISBN 1-56592-582-3
- Mitchell, D., S. Bradner and K Claffy, *In Whose Domain?: Name service in Adolescence*, section in *Coordinating the Internet*, MIT Press, 1997, ISBN 0-262-11230-2
- Bradner, S., and A. Mankin (Eds.), *IPng, Internet Protocol Next Generation*, Addison-Wesley 1996, ISBN 0-201-63395-7

- Bradner, S., *A Practical Perspective on Routers*, a chapter in *The Internet System Handbook*, Edited by D. Lynch & M. Rose, Addison-Wesley, 1993, ISBN-0-201-56741-5

## IETF RFCs and Internet Drafts

- Bradner, S. and J. Contreras, Eds., *Intellectual Property Rights in IETF Technology*, RFC 8179, May 2017
- Bradner, S. Ed., *Updating the Term Dates of IETF Administrative Oversight Committee (IAOC) Members*, RFC 7691, November 2015 ID00, ID01, ID02, ID03, ID04
- Kolkman, O., S. Bradner and S. Turner, *Characterization of Proposed Standards*, RFC 7127, January 2014
- Bradner, S., K. Dubray, J. McQuaid, and A. Morton, *Applicability Statement for RFC 2544: Use on Production Networks Considered Harmful*, RFC 6815, November 2012
- Trowbridge, S., Ed., E. Lear, Ed., G. Fishman, Ed., S. Bradner, Ed., *Internet Engineering Task Force and International Telecommunication Union - Telecommunication Standardization Sector Collaboration Guidelines*, RFC 6756, September 2012
- Bradner, S, L. Conroy & K. Fujiwara, *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)*, RFC 6116, March 2011 ID00, ID01, ID02, ID03, ID04, ID05, ID06, ID07, ID08, ID09
- Klensin, J. and S. Bradner, *Restoring Proposed Standard to Its Intended Use*, IETF Internet Draft, January 2011
- Arkko, J. and S. Bradner, *IANA Allocation Guidelines for the IPv6 Routing Header*, RFC 5871, May 2010
- Bradner, S. and J. Contreras, Eds., *Rights Contributors Provide to the IETF Trust*, RFC 5378, November 2008, ID00 ID01 ID02 ID03 ID04 ID05 ID06 ID07 ID08 ID09
- Falk, A. and S. Bradner, *Naming Rights in IETF Protocols*, RFC 5241, 1-April-2008
- Arkko, J. and S. Bradner, *IANA Allocation Guidelines for the Protocol Field*, RFC 5237, February 2008
- Bradner, S., B. Carpenter (Ed.), and T. Narten, *Procedures for Protocol Extensions and Variations*, RFC 4775, December 2006
- Bradner, S. Ed., *RFC 3978 Update to Recognize the IETF Trust*, RFC 4748, October 2006, ID00 ID01 ID02 ID03

- Bradner, S., *Obtaining Additional Permissions from Contributors*, Internet Draft, July 2005
- Trowbridge, S., S. Bradner and F. Baker, *Procedures for Handling Liaison Statements to and from the IETF*, RFC 4053, April 2005
- Bradner, S., *IETF Rights in Contributions*, RFC 3979, March 2005, ID00
- Bradner, S., *Intellectual Property Rights in IETF Technology*, RFC 3978, March 2005
- Bradner, S. Ed., *Extracting RFCs*, Internet Draft, February 2005, ID01
- Bradner, S., *Indication of Trademarks in IETF Documents*, January 2005, Internet Draft
- Bradner, S., *Sample ISD for the IETF Standards Process*, Internet Draft, October 2004
- Bradner, S., *Omniscience Protocol Requirements*, RFC 3751, 1-April-2004
- Bradner, S., *Intellectual Property Rights in IETF Technology*, RFC 3668, February 2004
- Bradner, S., *IETF Rights in Contributions*, RFC 3667, February 2004, ID00 ID01 ID02 ID03 ID04 ID05 ID06 ID07 ID08
- Bradner, S., *Ideas for changes to the IETF document approval process*, Internet Draft, July 2003
- Bradner, S., *An Idea for an Alternate IETF Standards Track*, Internet Draft, July 2003 ID01
- Mankin, A., S. Bradner, R. Mahy, D. Willis, J. Ott, and B. Rosen, *Change Process for the Session Initiation Protocol (SIP)*, RFC 3427, December 2002, ID00 ID01 ID02 ID03
- Fishman, G., and S. Bradner, *Internet Engineering Task Force and International Telecommunication Union - Telecommunications Standardization Sector Collaboration Guidelines*, RFC 3356, August 2002, ID00 ID01ID02
- Bradner, S. Ed. *Intellectual Property Rights in IETF Technology*, Internet Draft, June 2002 (published as RFC 3668) ID01
- Bradner, S. Ed., *IETF Rights in Submissions*, Internet Draft (published as RFC 3667), ID01
- Hoffman, P., and S. Bradner, *Defining the IETF*, RFC 3233, February 2002
- Bradner, S., P. Calhoun, H. Cuschieri, S. Dennett, G. Flynn, M. Lipford, and M. McPheters, *3GPP2-IETF Standardization Collaboration*, RFC 3131, June 2001 ID00
- Bradner, S. and HT Kung, *Requirements for an Anonymizing Packet Forwarder*, Internet Draft, November 2001
- Kung, HT & S. Bradner, *A Framework for an Anonymizing Packet Forwarder*, Internet Draft, November 2001

- Bradner, S. and A. Mankin, *Report of the Next Steps in Signaling BOF*, Internet Draft, July 2001
- Rosenbrock, K., R. Sanmugam, S. Bradner, J. Klensin, *3GPP-IETF Standardization Collaboration*, RFC 3113, June 2001, ID00 ID01
- Gaynor, M. and S. Bradner, *Firewall Enhancement Protocol (FEP)*, RFC 3093, 1-April-2001
- Bradner, S., A. Mankin and J. Schiller, A Framework for Purpose Built Keys (PBK), Internet Draft, February 2001, ID01, ID02, ID03 ID04, ID05
- Bradner, S., A. Mankin and V. Paxson *Advancement of metrics specifications on the IETF Standards Track*, Internet Draft, February 2000, ID01 ID02 ID03
- Bradner, S. and V. Paxson, *IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers*, RFC 2780, March 2000 ID00 ID01 ID02 ID03 ID04
- Bradner, S., *A Memorandum of Understanding for an ICANN Protocol Support Organization*, RFC 2691, September 1999, ID01
- Bradner, S., *A Proposal for an MOU-Based ICANN Protocol Support Organization*, RFC 2690, September 1999, ID00
- Bradner, S., *OSI connectionless transport services on top of UDP Applicability Statement for Historic Status*, RFC 2556, March 1999 ID00 ID01
- Bradner, S., *The Roman Standards Process -- Revision III*, RFC 2551, 1-April-1999
- Bradner, S., and J. McQuaid (Eds.), *Methodology for testing network interconnection devices*, RFC 2544, March 1999
- Bradner, S., *Bylaws for a Protocol Support Organization*, Internet Draft, September 1998, ID01 ID02 ID03
- O'Dell, M., H. Alvestrand, B. Wijnen, and S. Bradner, *Advancement of MIB specifications on the IETF Standards Track*, RFC 2438, October 1998, ID00 ID01
- Bradner, S. *Secret Handshakes: How to get RFCs published in the IETF*, Internet Draft, October 1998 ID01 ID02 ID03
- Brett, R., S. Bradner, and G. Parsons, *Collaboration between ISOC/IETF and ITU-T*, RFC 2436, October 1998
- Bradner, S. (Ed), *IETF Working Group Guidelines and Procedures*, RFC 2418, September 1998, ID00 ID01 ID02 ID03
- Mankin, A., A. Romanow, S. Bradner, V. Paxson, *IETF Criteria for Evaluating Reliable Multicast Transport and Application Protocols*, RFC 2357, June 1998
- Mankin, A., F. Baker, B. Braden, S. Bradner, M. O'Dell, A. Romanow, A. Weinrib, L. Zhang, *Resource ReSerVation Protocol (RSVP) -- Version 1 Applicability Statement Some Guidelines on Deployment*, RFC 2208, September 1997

- Bradner, S. Ed., *Internet Protocol Multicast Problem Statement*, Internet Draft, September 1997
- Bradner, S. Ed., *Internet Protocol Quality of Service Problem Statement*, Internet Draft, September 1997
- Elz, R., R. Bush, S. Bradner and M., Patton, *Selection and Operation of Secondary DNS Servers*, RFC 2182, July 1997
- Bradner, S, *Key words for use in RFCs to Indicate Requirement Levels*, RFC 2119, March 1997 ID00 ID01 ID02
- Bradner, S., *Source directed access control on the Internet.*, RFC 2057, November 1996 ID00 ID01
- R. Hovey and S. Bradner, *The Organizations Involved in the IETF Standards Process*, RFC 2028, October 1996, ID00 ID01 ID02
- Bradner, S. (Ed.), *Internet Standards process - revision 3*, RFC 2026, October 1996, ID00 ID01 ID02 ID03 ID04 ID05 ID06
- Bradner, S., and J. McQuaid (Eds.), *Methodology for testing network interconnection devices*, RFC 1944, May 1996, ID00 ID01 ID02
- Halpern, J. and S. Bradner, *RIPv1 Applicability Statement for Historic Status*, RFC 1923, March 1996
- Bradner, S. and A. Mankin, *The recommendation for the IP next generation protocol*, RFC 1752, January 1995, ID00
- Bradner, S. and A. Mankin, *IP: Next Generation (IPng) White Paper Solicitation*, RFC 1550, December 1993
- Bradner, S. (Ed.), *Benchmarking terminology for network interconnection devices*, RFC 1242, July 1991

### *Talks* (some of the talks I've done over the years)

- Internet Governance: A perpetual "threat"- Harvard Kennedy School, Cambridge MA - 2017-08-02
- The Internet: The anti-network, Harvard College, Cambridge MA 2016-11-07
- IANA, Important but not for what they do, NANOG, Dallas TX, 2016-10-17
- sob@harvard 2/14/66 – 7/1/16, Harvard ABCD, 2015-12-11
- Internet Engineering Task Force (IETF), Harvard Kennedy School, Cambridge MA - 2015-11-18
- Changing Concepts of Anonymity, Confidentiality, and Privacy in SBER, (with Dean Gallant), PRIM&R, Boston MA – 2015-11-12
- "It" will be called "The Internet" but … - NANOG on the Road, Cambridge MA - 2015-04-21
- Internet Governance: A perpetual "threat"- Harvard Kennedy School, Cambridge MA - 2015-01-15

- Random Wanderings – Harvard ABCD, Cambridge MA - 2014-12-12
- Mobile Devices in Research: Growing tool, new issues?, PRIM&R, 2014-12-6
- Governance in a Cyber World - Harvard Kennedy School, Cambridge MA - 2014-07-29
- Internet-101 - Harvard Kennedy School, Cambridge MA - 2014-01-14
- This and That, Harvard ABCD, 2013-12-13
- The Internet, once not, but now, of this world? - Harvard Kennedy School, Cambridge MA - 2013-10-16
- That, This and the Other Thing, Harvard ABCD, Cambridge MA -2013-05-05
- 5 Levels Seems Right, Harvard, 2012-12-03
- Unimaginable but True: the regulatory status of the Internet - Harvard Kennedy School, Cambridge MA - 2012-09-12
- Flowing Down from Layer 9 (say goodbye to the Internet?) - Harvard ABCD, Cambridge MA - 2011-12-09
- Protecting Research Data - PRIM&R - 2011-12-01
- Protecting Research Data - Boston College, Boston MA - 2011-10-17
- Witness to the Evolution: IP from has-been to is-all to ?? - IPTCOMM - 2011-08-01
- Data Security also FISMA - Research Compliance Conference - 2011-06-13
- Technical Issues in Data Security - PRIM&R - 2011-04-29
- Internet-101, Internet Law Forum - 2011-04-08
- Change & Opportunity II, Harvard ABCD – 2010-12-03
- The Internet: Its Past, Present, and Possible Futures - ISOC-NE - 2010-10-20
- Challenges of Research Data Security - EDUCAUSE Security 2010-04-14
- Privacy is not a Spectator Sport - Grand Valley State University, Allendale MI - 2010-02-25
- Change & Opportunity – Harvard ABCD – 2009-12-11
- Research Data Protection Policy at Harvard - PRIM&R - 2009-11-15
- Google Knows: Should you care? – Harvard – 2009-03-11
- New Year, New Rules (No Money) – Harvard ABCD – 2008-12-12
- The Past, Present and Future of the Internet - Boston Network Users Group - 2008-12-02
- Technology Security - Mandatory and Unachievable (but Approachable) - MIT - 2008-11-5
- How is the Internet Different? Is "good enough" good enough? - VON Mexico, Mexico City - 2008-02-28
- Work Mutterings Other Mutterings – Harvard ABCD – 2007-11-02
- The Implications of the Unmet Last Goal for the Internet Protocols - Boston Network Users Group - 2007-01-02

- Security & Privacy Rules & Pre Rules – Harvard ABCD – 2006-07-07
- Where is Controversy? - Alcatel - 2006-11-1
- Will the Internet be permitted to grow up? - Wainhouse Research - 2006-07-20
- Internet II: Looking forward from 10 years ago - Joint Techs - 2006-07-17
- Network Neutrality: Federal Non-Legislation - Cornell, Ithaca NY - 2006-06-28
- Owing the Desktop: Is .edu like .com – Cornell, Ithaca NY - 2006-06-28
- Internet Governance: Not Just Dealing with a Uniqueness Requirement - MIT, Cambridge MA - 2006-05-02
- Not Your Father's Internet, and that Hurts - CENIC, Oakland CA - 2006-04-15
- Internet Concepts, History, Regulations & Governance - Harvard Business School, Boston MA - 2006-04-03
- Security Related Musings - Boston University, Boson MA - 2006-03-01
- The Myth of network Neutrality - EDUCAUSE streaming radio - 2006-02-15
- Where-to-Where (was End-to-End) - Cisco, San Jose CA - 2005-12-07
- Electronic Data Security: Designing a Good Data Protection Plan - Human Research Protection Program (HRPP), Boston MA - 2005-12-06
- This Internet Thing - CS50 - Harvard University, Cambridge MA - 2005-10-22
- Where-to-Where (was End-to-End) - Greater Boston Chapter / ACM - October 20 2005
- NGN: Replacement or Evolution? - FCC, Washington DC - 2005-09-12
- Will the Internet be reliably bad enough to preserve PPVPNs? - MPLSCON, New York, NY - 2005-05-17
- Wireless Grids: The current hype or the next Internet? - TTI Vanguard, Chicago IL - 2005-04-12
- IP nets: from the origins to a possible NGN future - Cisco, San Jose CA - 2005-01-11
- Witness to the Evolution - Cisco Networkers, New Orleans LA - 2004-07-15
- How to Kill Worms and Viruses with Policy Pontifications, NANOG, Miami FL - 2004-02-10
- A Short History of the Internet - NANOG, Miami FL - 2004-02-09
- The Internet Engineering Task Force (IETF) Stuff - Harvard Berkman Center, Cambridge MA - 2003-07-29
- IETF - Global Standards Collaboration 8, Ottawa, Canada - 2003-05-28
- The Internet: Imagination, Innovation or Imitation - USTA - 2003-05-20
- Will the future Internet look like what we have today? - Orange Country IEEE, Irvine CA - 2003-05-20

- Will there be an Internet in 5 years? - Syracuse University, Syracuse NY - 2003-05-08
- Locating the IETF: GIS related work at the IETF - OGC - 2003-02-13
- The Sub-IP Area and Optical Networking at the IETF - GRID Forum, Amsterdam - 2002-09-25
- Internet Architectural Philosophy and the New Business Reality - GRID Forum, Amsterdam - 2002-09-24
- Are technology standards too important to leave to those that know what they are doing? - Public Design Workshop - 2002-09-14
- The IETF: A Decentralized Voluntary Standards Process - SES, Washington DC - 2002-08-13
- The Internet and Optical Networking at the IETF - COIN 2002 - 2002-07-22
- The Future of the Net - Wireless 2002, Calgary AB - 2002-07-08
- Can the e2e RG be real-world useful? - IRTF e2e RG meeting - 2002-05-15
- An IETF Insider View - TranSwitch - 2002-04-15
- The Internet: Philosophy & Technology - Boston University, Boston MA - 2002-02-04
- IETF Stuff, USVP, Mountain View CA, 2002-01-15
- Once there was a network and it was not the one we needed, but the one we built hurts or how the Internet is not the phone network and why that matters to users, service providers, cops and society - MIT, Cambridge MA - 2002-01-10
- The Future of the Net - CINA - 2001-09-15
- Impact of enum and IP telephony - Taiwan - 2001-08-21
- Standards-Setting and United States Competitiveness, Hearing, US. House of Representatives, Committee on Science, Subcommittee on Environment, Technology, and Standards, Washington DC - 2001-06-28
- The future of the nets or will it be The Net? - New England telecommunications Association - 2001-01-17
- Convergence in Telecom Networks: Is there A future? - Lucerne - 2000-11-13
- Convergence Efforts in the IETF - SPIE, Boston MA - 2000-11-08
- Current IETF Efforts and Technology Trends - Lucent - 2000-08-18
- Internet of the Future: Convergence Nirvana? - Broad Band Year, San Jose CA - 2000-06-28
- Internet Engineering Task Force: Standards & ideas for the Internet - G8 meeting, Paris - 2000-05-16
- Internet Engineering Task Force - IPR Summit, London - 2000-04-11

- Next Generation Internet: Where will it stop? - Ericsson, Stockholm - 2000-01-31
- The IETF and the Future of the Internet - ISOC SE, Stockholm - 2000-01-31
- Voice-Over-IP Standards and Interoperability Update IETF - NCF Chicago IL - 1999-10-27
- Does reality matter?: QoS & ISPs – GTE, Burlington MA - 1999-09-15
- WAN Quality of Service - Information Technology Business Forum, Seattle WA - 1999-07-21
- Emerging Trends for the Millennium: Communications Technology - NACAS- 1999-06-26
- The Internet's Impact on Government Programs and Services - Kentucky GIS - 1999-05-03
- Convergence and the IETF - Signaling Futures '99, Tucson AZ - 1999-03-30
- The IETF: Standards and non-Standards - IEEE, Austin TX - 1999-03-08
- Internet Governance: Where are we Now? - Harvard JFK School, Cambridge MA- 1999-02-24
- Technical and Political Issues With Alternatives to Undersea Cables - Nortel - 1998-04-21
- Internet QoS: A definable goal?, Nortel, 1998-04-21
- Real QoS versus a Few Traffic Classes - Next Generation Networks, Washington DC - 1998-11-04
- Internet 2, NGI, and the Real World – Harvard, Cambridge MA - 1998-04-15
- Reality and the Internet of the Future Programs - IEEE - 1998-04-09
- Measuring the Impact of the Integrated Infrastructure for Voice Video and Data on Traditional Telephone Service Administration - IIR, Washington DC - 1998-04-20
- Institutionalizing the IANA Functions To Deliver a Stable and Accessible Global Internet for Mission Critical Business Traffic and Transactions - Reengineering the Internet - London - 1998-01-28
- The problems in trying to create a QoS Internet, ISOC-IL, 1998-01
- Technical and political issues with alternatives to undersea cables, ISOC-IL, 1998-01
- Technology Trends and the IETF - Bellcore - 1997-11-24
- Managing the Bandwidth Explosion - SaskTel, Saskatoon SK - 1997-09-23
- Next Generation Routers - Third Workshop on Real-time and Media Systems (RAMS'97), Taiwan - 1997-08
- Next Generation Routers Overview - Interop - 1997
- Trends and Issues in the next Generation Internet Protocols - Harvard ABCD, Cambridge MA- 1997-07-11

- Reality and the "next generation" projects: NGI, Internet 2 and the real world - U Texas, Austin TX - 1997-04-30
- The future of the Internet - GTE - 1997-04-14
- Internet II Status – IEPG, Memphis TN - 1997-04-06
- IVD at Citicorp - Citicorp, New York City NY - 1997-01-14
- Current Status, Problems and Future Directions of ATM Technology - High Speed Nets - 1996-11
- Under Construction: The Network of the Future - Federal Deposit Insurance Corporation - 1996-11
- Internet II: Introduction – Chicago IL - 1996-10-01
- In whose domain: name service in adolescence (with Don Mitchell & K Claffy) - Harvard JFK School, Cambridge MA - 1996-09-08
- Working Group Workshop – IETF, Los Angeles CA - 1996-03
- Will there be an Internet in the Year 2000? - ATM year, San Jose CA - 1996-05
- The Future of IP - 1996-05-18
- IP Next Generation (IPng), Reseau Interordinateurs Scientifique Quebecois (RISQ) '95, Montreal QU, 1995-01-17
- The new Internet, Reseau Interordinateurs Scientifique Quebecois (RISQ) '95, Montreal QU, 1995-01-17
- Did we miss the fork in the road? - Information Superhighway Summit, San Jose CA - 1994-09-27
- Tunneling - SHARE 83, Boston MA - 1994-08-09
- Internet Engineering Task Force - SHARE 83, Boston MA - 1994-08
- The TCP/IP Protocols - SHARE 83, Boston MA - 1994-08
- Router Tests V.6 - Interop, San Francisco CA - 1993-08-25
- Performance of Routers, Enterprise Networks, Boulder CO - June 15, 1993
- Concept of Routing in a Heterogeneous Network, SHARE 80, San Francisco CA - 1993-04-03
- Routing in IP, SHARE 80, San Francisco CA - 1993-04-03
- Router & Bridge Performance, SHARE 80, San Francisco CA - 1993-04-03
- Network Security, SHARE 80, San Francisco CA - 1993-04-02
- Connecting to the Internet, SHARE 80, San Francisco CA - 1993-04-01
- The AppleTalk & IPX Protocols, SHARE 80, San Francisco CA - 1993-04-01
- Jargon Busting - An Introduction to the Technology of Data Networks, ACM SIGUCCS User Services Conference XX, 1992-11-08
- Kerberos, A User and Service Authentication System, SHARE 79, Atlanta GA, 1992-08-20
- Router & Bridge Performance, SHARE 79, Atlanta GA, 1992-08-19

- Unix Security, SHARE 78, Anaheim CA - 1992-04-04
- Routers versus Bridges, SHARE 78, Anaheim CA - 1992-04-03
- Routers and Bridges Performance, SHARE 78, Anaheim CA - 1992-04-03
- Router Tests V.5 - Interop, Washington DC - 1992-05-20
- NEARnet & NSFnet (& MERIT) (& ANS) - IETF, San Diego CA - 1992-04-14
- Enterprise-wide Network Design - Networks and Imaging Symposium and Exhibition - 1992-02-19
- Router Tests V.4 - Interop, San Jose CA - 1991-10-09
- A Technical Non-IBM View of networking - IBM, Raleigh NC - 1990-11-28
- Traffic Patterns in an X Window Environment - Interop, San Jose CA - 1990-10-11
- Router Tests V.3 – Interop, San Jose CA - 1990-10
- Application of Bridges and Routers - CANET - 1990-06-14
- Worms, Viruses, etc: Things That Go Bump on the Net - SHARE 73, Orlando FL, 1989-08
- Unknown Mailer Error 101, or Why It's So Hard to See You - USENIX, Salt Lake City UT - 1984-06-15
- MLE (Multi-Lingual Editor) - USENIX - 1984-01-18

Last updated: August 19, 2017

# LIST OF CASES

## Patent litigation in which I was announced as an expert.

*Sprint v. Time Warner Cable*: USDC Kansas, Case No. 2:11-cv-2686 Kansas, expert for TWC, Jan 2017 to March 2017: Winston & Strawn

*OpenTV v. Apple*: USDC Northern California Case No. 5:15-cv-02008-EJD, 2016 WL 344845; expert for Apple, June 2015 to Aug 4 2016, declaration: O'Melveny & Meyers (N.D. Cal., dismissed by stipulated order Aug. 4, 2016)

*Sprint v Cable One et al*: USDC Kansas, Case Nos. 11-2684-JWL, 11-2685-JWL & 11-2686-JWL: expert for Comcast, October 2014 to December 2017, expert report: Winston & Strawn

*Sprint v Comcast*: Case No. l:12-cv-01013-RGA (D. Del.): expert for Comcast: June 2014 to Jan 2015, expert reports, deposition: Winston & Strawn

*Sprint v Big River Telecom*: USDC Kansas, Case No. 08-cv-02046-JWL-DJW: expert for Big River Telecom: July 2009 to Sept 2009, expert report: Kirkland & Ellis, (D. Kan., dismissed with prejudice by joint stipulation pursuant to F. R. Civ. P. 41(a)(1)(A)(ii) Sep. 30, 2009)

*VoxPath v Verizon*: USDC E. TX, Grayson Case No. 4:08-cv-127-RA: expert for Verizon: Dec 2008 to mid 2013: Winston & Strawn (case dismissed with prejudice)

*Level3 v. Limelight*: USDC E. VA C.A. 2:07CV589 (RGD-FBS): expert for Level 3: Jan 2008 to Jan 2009: expert report, deposition, testified at trial: Winston & Strawn

*Verizon v. Vonage*: USDC E. VA. CF 1:06CV682 (CMH/BRP): expert for Vonage: Aug 2006 to spring 2007: expert report, deposition: Steptoe & Johnson

*Fenner Investments v. Juniper Networks*: USDC E. TX. C.A. 2:05CV0: expert for Nortel: April 2006 to mid 2006, expert report: Finnegan, Henderson, Farabow, Garrett & Dunner

*Nortel Networks v. Foundry Networks*: USDC MA C.A. No. 01-10442DPW: expert for Foundry: October 2002 to October 2004, expert report, deposition: Orrick, Herrington & Sutcliffe

*Red River Fiber-Optics Company v. Level 3 Communications*: USDC E. TX, Marshall C.A. No. 2-01CV208-TJW: expert for Level 3: October 2002 thru July 2003: expert report, deposition: Merchant Gould

*MuniAuction v. Thomson Corporation*: expert for Thomson: USDC W. PA C. A. No. 01-1003: June 2002 to Oct 2006: expert report, deposition, testified at trial: Wilmer Cutler Pickering Hale and Dorr

*Storage Technology Corporation vs. Cisco Systems*: USDC N. CA, San Francisco C.A No. C00-1176 (SI): expert for Storage Technology: December 2000 to June 2005: expert report, deposition, testified at trial: Brooks & Kushman

*DataRace vs. Lucent Technologies*: expert for Data Race, (Texas): No. CIV.A. SA98CA746PMA: November 1997 to September 1999: expert report, deposition, testified at Markman: McCamish & Socks

In addition, there are a number of cases where I have not yet been announced, that concluded before I was announced or where I served as a consultant.

## Inter Parties Reviews in which I provided a declaration.

*NFL Enterprises LLC. v. OpenTV Inc.*, Inter Parties Review, U.S. Patent No. 6,233,736, Case number IPR2017-02092, Expert for NFL, Aug 2017 to July 2018, declaration: Vinson & Elkins LLP, withdrawn

*Apple v. OpenTV Inc.*, Inter Parties Review, U.S. Patent No. 6,233,736, Case number IPR2016-00992, Expert for Apple, Dec 2015 to Aug 2016, declaration: O'Melveny & Meyers, withdrawn

*Sony Mobile Communications Inc. v. SSH Communications Security Oyj*, Inter Parties Review, U.S. Patent No. 8,544,079, Case number IPR2015-01869, June 2015 to March 2016, Expert for Sony, declaration: Turner Boyd

*Sony Mobile Communications Inc. v. SSH Communications Security Oyj*, Inter Parties Review, U.S. Patent No. 9,071,578, Case number IPR2016-01180, March 2016 to December 2016, Expert for Sony, declaration: Turner Boyd

## Other cases in which I provided a declaration or expert report.

*SNMP Research, Inc., et al v Nortel Networks Inc., et al*, Chapter 11 09-10138 (KG), Adv. Proc. No. 11-53454 (KG), expert report, 1 Sept 2016 to November 2017.

*Nathan Florence et al v. Mark Shurtleff et al*, USDC UTAH Central Division, Case Civil No. 2:05CV00485 DB, expert for Nathan Florence et al, declaration, May to December 2011: SNR Denton US

*American Booksellers Foundation for Free Expression et al v. Daniel S. Sullivan as Attorney General of the State of Alaska*, USDC Alaska, Case No. 3:10-cv-00193-RRB, expert for the American Booksellers Foundation for Free Expression, declaration, August 2010: SNR Denton US

American Booksellers Foundation for Free Expression et al v. Martha Coakley as Attorney General of the State of the Commonwealth of Massachusetts et al, USDC Massachusetts, Civil Action No.: 1:10-cv-11165, expert for the American Booksellers Foundation for Free Expression, declaration, July 2010: SNR Denton US

*ACLU v. Reno/American Library Association v. U.S. Department of Justice*, Expert for American Library Association, March 1996 to August 1996, declaration, deposition, testified at Federal Court hearing 1996-03-21, 1996-03-22, Jenner & Block

Last updated: September 16, 2018

DECLARATION OF SCOTT BRADNER

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

# Appendix B

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

WIKIMEDIA FOUNDATION,

*Plaintiff*,

v.

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

*Defendants*.

No. 1:15-cv-00662-TSE

**DECLARATION OF SCOTT BRADNER**
**LIST OF DOCUMENTS PROVIDED BY PLAINTIFF'S COUNSEL**

**A. Documents Included in the Appendix to the Bradner Declaration**

1. Appendices C, D–F, H, K, L–U, X–Z, AA, BB, DD–FF

**B. Defendants' Discovery Responses**

2. Defendant DOJ's Objections and Responses to Plaintiff's First Set of Interrogatories, dated January 2, 2018

3. Defendant DOJ's Objections and Responses to Plaintiff's First and Second Sets of Requests for Admission, dated January 8, 2018

4. Defendant DOJ's Objections and Responses to Plaintiff's First and Second Sets of Requests for Production, dated January 8, 2018

5. Defendant DOJ's January 2018 Production, Bates Numbers DOJ000001-000235 (DOJ Attachments A-C)

6. Defendant NSA's Objections to Plaintiff's Second Set of Interrogatories, dated March 22, 2018

7. Defendant NSA's Objections to Plaintiff's Third Set of Requests for Admission, dated March 22, 2018

8. Defendant NSA's Objections and Responses to Plaintiff's First and Second Sets of Requests for Production, dated January 8, 2018

9. Defendant NSA's January 2018 Production, Bates Numbers NSA-WIKI00000-00297

10. Defendant ODNI's Objections and Responses to Plaintiff's First Set of Interrogatories, dated December 22, 2017

11. Defendant ODNI's Objections and Responses to Plaintiff's First and Second Sets of Requests for Admission, dated January 8, 2018

12. Defendant ODNI's Revised Objections and Responses to Plaintiff's First and Second Sets of Requests for Production, dated February 5, 2018

**C. Wikimedia's Discovery Responses**

13. Plaintiff Wikimedia Foundation's Responses and Objections to DOJ's First Set of Requests for Production, dated January 26, 2018

14. Plaintiff Wikimedia Foundation's Responses and Objections to NSA's First Set of Requests for Production, dated January 11, 2018

15. Plaintiff Wikimedia Foundation's Responses and Objections to ODNI's Second Set of Interrogatories, dated January 26, 2018

**D. Documents Publicly Released by Defendants in *ACLU v. NSA*, 16-cv-8936-RMB (S.D.N.Y.)**

16. Bates Numbers ACLU 16-CV-8936 (RMB) 00001-000011: FISC Submission, "2015 Summary of Notable Section 702 Requirements" (July 15, 2015)

17. Bates Numbers ACLU 16-CV-8936 (RMB) 000012-000015: FISC Opinion and Order, *In Re Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act* (Aug. 11, 2014)

18. Bates Numbers ACLU 16-CV-8936 (RMB) 000016-000025: FISC Submission, "Government's Response to the Court's Order of July 7, 2015" (July 14, 2015)

19. Bates Numbers ACLU 16-CV-8936 (RMB) 000026-000036: FISC Order, "Order Appointing an Amicus Curiae" (Aug. 13, 2015)

20. Bates Numbers ACLU 16-CV-8936 (RMB) 000037-000038: FISC Submission, "Notice Concerning the Court's Order of August 13, 2015, Appointing an Amicus Curiae" (Aug. 18, 2015)

21. Bates Numbers ACLU 16-CV-8936 (RMB) 000039-000042: FISC Order, "Briefing Order" (Sept. 16, 2015)

22. Bates Numbers ACLU 16-CV-8936 (RMB) 000043-000048: Letter from FBI to FISC Attaching "Annual Report Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act" (Oct. 20, 2014)

23. Bates Numbers ACLU 16-CV-8936 (RMB) 000049-000082: FISC Submission, "Brief of Amicus Curiae" (Oct. 16, 2015)

24. Bates Numbers ACLU 16-CV-8936 (RMB) 000083-000121: FISC Submission, Government's Response to the Court's Briefing Order of September 16, 2015 (Oct. 16, 2015)

25. Bates Numbers ACLU 16-CV-8936 (RMB) 000122-000169: Transcript of FISC Proceedings Held Before the Honorable Thomas F. Hogan (Oct. 20, 2015)

26. Bates Numbers ACLU 16-CV-8936 (RMB) 000170-000177: FISC Submission, "Government's Ex Parte Submission of Attorney General Guidelines" (Aug. 19, 2008)

27. Bates Number ACLU 16-CV-8936 (RMB) 000178: NSA External Oversight Process Description: "Emergency USP Content Queries within FAA 702 PRISM and Telephony Content Collection"

28. Bates Numbers ACLU 16-CV-8936 (RMB) 000179-000183: NSA External Oversight Process Description: "USP Queries within FAA 702 PRISM and Telephone Content Collection"

29. Bates Numbers ACLU 16-CV-8936 (RMB) 000184-000185: DOJ National Security Division Memorandum from Stuart J. Evans, Deputy Assistant Attorney General for Intelligence, to Litigation Section, Office of Intelligence, Re: "Restriction Regarding the Use of FISA Section 702 Information in Criminal Proceedings Against United States Persons"

30. Bates Numbers ACLU 16-CV-8936 (RMB) 000186-000187: NSA External Oversight Process Description: "USP Queries of Communications Metadata Derived from FAA 702 [*Redacted*] and Telephony Collection"

31. Bates Numbers ACLU 16-CV-8936 (RMB) 000188-000190: "USP Query Guidance for Personnel with Access to Unminimized FISA Section 702 Data"

32. Bates Numbers ACLU 16-CV-8936 (RMB) 000191-000221: FISC Submission, "Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications," *In RE DNI/AG 702(g) Certifications* [*Redacted*] (filed Sept. 26, 2016)

33. Bates Numbers ACLU 16-CV-8936 (RMB) 000222-000233: Redacted FISC Submission

34. Bates Numbers ACLU 16-CV-8936 (RMB) 000234-000239: FISC Submission, "Certification of the Director of National Intelligence and the

Attorney General Pursuant to Subsection 702(g) of the Foreign Intelligence Surveillance Act of 1978, As Amended," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed Sept. 26, 2016)

35. Bates Numbers ACLU 16-CV-8936 (RMB) 000240-000244: FISC Submission, "Affidavit of Admiral Michael S. Rogers, United States Navy, Director, National Security Agency," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed Sept. 26, 2016)

36. Bates Numbers ACLU 16-CV-8936 (RMB) 000245-000247: FISC Submission, "Affidavit of James B. Comey, Director, Federal Bureau of Investigation," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed Sept. 26, 2016)

37. Bates Numbers ACLU 16-CV-8936 (RMB) 000248-000250: FISC Submission, "Affidavit of the Director of the Central Intelligence Agency," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed Sept. 26, 2016)

38. Bates Numbers ACLU 16-CV-8936 (RMB) 000251-000253: FISC Submission, "Affidavit of the Director of the National Counterterrorism Center," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed Sept. 26, 2016)

39. Bates Numbers ACLU 16-CV-8936 (RMB) 000254-000263: FISC Submission, "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" (filed Sept. 26, 2016)

40. Bates Numbers ACLU 16-CV-8936 (RMB) 000264-000280: FISC Submission, "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" (filed Sept. 26, 2016)

41. Bates Numbers ACLU 16-CV-8936 (RMB) 000281-000285: FISC Submission, "Procedures Used by the Federal Bureau of Investigation 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" (filed Sept. 26, 2016)

42. Bates Numbers ACLU 16-CV-8936 (RMB) 000286-000328: FISC Submission, "Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (signed Sept. 21, 2016)

43. Bates Numbers ACLU 16-CV-8936 (RMB) 000329-000339: FISC Submission, "Minimization Procedures Used by the Central Intelligence Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (filed Sept. 26, 2016)

44. Bates Numbers ACLU 16-CV-8936 (RMB) 000340-000343: Redacted FISC Filing, "Exhibit F"

45. Bates Numbers ACLU 16-CV-8936 (RMB) 000344-000358: FISC Submission, "Minimization Procedures Used by the National Counterterrorism Center in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (filed Sept. 26, 2016)

46. Bates Numbers ACLU 16-CV-8936 (RMB) 000359-000364: FISC Order, *In RE DNI/AG 702(g) Certifications* [*Redacted*] (Oct. 26, 2016)

47. Bates Numbers ACLU 16-CV-8936 (RMB) 000365-000373: FISC Submission, "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" (signed July 24, 2014)

48. Bates Numbers ACLU 16-CV-8936 (RMB) 000374-000419: Transcript of FISC Proceedings Before the Honorable Mary A. McLaughlin, *In RE DNI/AG 702(g) Certification* [*Redacted*] (2008)

49. Bates Numbers ACLU 16-CV-8936 (RMB) 000420-000434: FISC Submission, "Government's Reply to [Redacted] to Petition" (2014)

50. Bates Numbers ACLU 16-CV-8936 (RMB) 000435-000471: Transcript of FISC Proceedings Before the Honorable Thomas F. Hogan (Aug. 4, 2014)

51. Bates Numbers ACLU 16-CV-8936 (RMB) 000472-000509: FISC Submission, "Verified Report in Response to Order," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed July 18, 2014)

52. Bates Numbers ACLU 16-CV-8936 (RMB) 000510-000548: FISC Opinion (2014)

53. Bates Numbers ACLU 16-CV-8936 (RMB) 000549-000579: FISC Opinion (Apr. 7, 2009)

54. Bates Numbers ACLU 16-CV-8936 (RMB) 000580-000671: FISC Submission, "Quarterly Report to the Foreign Intelligence Surveillance Court

Concerning Compliance Matters Under Section 702 of the Foreign Intelligence Surveillance Act" (Mar. 2015)

55. Bates Numbers ACLU 16-CV-8936 (RMB) 000672-000752: FISC Submission, "Quarterly Report to the Foreign Intelligence Surveillance Court Concerning Compliance Matters Under Section 702 of the Foreign Intelligence Surveillance Act" (Mar. 2014)

56. Bates Numbers ACLU 16-CV-8936 (RMB) 000753-000776: Letter from DOJ National Security Division to FISC Enclosing Memorandum Re: "Discussion with the Foreign Intelligence Surveillance Court on 24 July 2012 Regarding the Waiver Provisions of NSA's Minimization Procedures Governing Data Acquired Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended" (Aug. 28, 2012)

57. Bates Numbers ACLU 16-CV-8936 (RMB) 000792-000841: FISC Submission, "Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications" (filed July 15, 2015)

58. Bates Numbers ACLU 16-CV-8936 (RMB) 000842-000847: FISC Submission, "Certification of the Director of National Intelligence and the Attorney General Pursuant to Subsection 702(g) of the Foreign Intelligence Surveillance Act of 1978, As Amended," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed July 15, 2015)

59. Bates Numbers ACLU 16-CV-8936 (RMB) 000848-000851: FISC Submission, "Affidavit of Admiral Michael S. Rogers, United States Navy, Director, National Security Agency," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed July 15, 2015)

60. Bates Numbers ACLU 16-CV-8936 (RMB) 000852-000854: FISC Submission, "Affidavit of James B. Comey, Director, Federal Bureau of Investigation," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed July 15, 2015)

61. Bates Numbers ACLU 16-CV-8936 (RMB) 000855-000857: FISC Submission, "Affidavit of the Director of the Central Intelligence Agency," *In RE DNI/AG 702(g) Certification* [*Redacted*] (filed July 15, 2015)

62. Bates Numbers ACLU 16-CV-8936 (RMB) 000858-000862: FISC Submission, "Procedures Used by the Federal Bureau of Investigation 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" (filed July 28, 2014)

63. Bates Numbers ACLU 16-CV-8936 (RMB) 000863-000866: Redacted FISC Filing, "Exhibit F"

64. Bates Numbers ACLU 16-CV-8936 (RMB) 000867-000898: FISC Submission, "Government's Verified Response to the Court's Order Dated October 14, 2015" (filed Oct. 21, 2015)

65. Bates Numbers ACLU 16-CV-8936 (RMB) 000899-000910: FISC Submission, "Verified Response to the Court's Order Dated November 6, 2015" (signed Dec. 18, 2015)

66. Bates Numbers ACLU 16-CV-8936 (RMB) 000911-001000: NSA Analysis & Production, "Draft FAA 702 Guidance"

67. Bates Numbers ACLU 16-CV-8936 (RMB) 001001-001049: "FAA 702 Adjudication Checklist"

68. Bates Numbers ACLU 16-CV-8936 (RMB) 001050-001096: "OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL," at 36-82

69. Bates Numbers ACLU 16-CV-8936 (RMB) 001097-001100: "OVSC1203: FISA Amendments Act (FAA) Section 702 Transcript 20160818 FINAL," at 83-86

70. Bates Numbers ACLU 16-CV-8936 (RMB) 001101-001150: NSA Presentations, "FAA 702 Metrics Update" (Dec. 2013-Feb. 2016)

71. Bates Numbers ACLU 16-CV-8936 (RMB) 001151-001189: NSA Presentations, "FAA 702 Metrics Update" (Mar.-Aug. 2016)

72. Bates Numbers ACLU 16-CV-8936 (RMB) 001190-001228: NSA Presentations, "FAA 702 Metrics Update" (Aug.-Dec. 2016)

73. Bates Numbers ACLU 16-CV-8936 (RMB) 001229-001230: NSA Presentations, "FAA 702 Metrics Update" (Dec. 2016)

74. Bates Numbers ACLU 16-CV-8936 (RMB) 001231-001235: NSA, "Report of Annual Review Pursuant to Section 702(I) of the Foreign Intelligence Surveillance Act for Period 9/1/2012 Through 8/31/2013"

75. Bates Numbers ACLU 16-CV-8936 (RMB) 001236-001240: "National Security Agency Response to Congressionally Direction Action: Report of Annual Review Pursuant to Section 702(I) of the Foreign Intelligence Surveillance Act for Period 9/1/2013 Through 8/31/2014"

76. Bates Numbers ACLU 16-CV-8936 (RMB) 001241-001244: "National Security Agency Response to Congressionally Direction Action: Report of

Annual Review Pursuant to Section 702(I) of the Foreign Intelligence Surveillance Act for Period 9/1/2014 Through 8/31/2015"

77. Bates Numbers ACLU 16-CV-8936 (RMB) 001245-001247: "National Security Agency Response to Congressionally Direction Action: Report of Annual Review Pursuant to Section 702(I) of the Foreign Intelligence Surveillance Act for Period 9/1/2015 Through 8/31/2016"

78. Bates Numbers ACLU 702 FOIA 09 15 2017 release 000001-000057: "Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence" (Feb. 2016)

79. Bates Numbers ACLU 702 FOIA 09 15 2017 release 000058-000066: ODNI, "Annual Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2015" (Apr. 30, 2016)

**E. Documents Publicly Released by Defendants in *EFF v. DOJ*, 16-cv-02041 (N.D. Cal.)**, http://icontherecord.tumblr.com/post/161824569523/additional-release-of-fisa-section-702-documents

80. Document 1: FISC Opinion (2008)

81. Document 2: FISC Opinion (2010)

82. Document 3: FISC Opinion and Order (Aug. 30, 2013)

83. Document 4: FISC Opinion and Order (2010)

84. Document 5: FISC Opinion and Order (2009)

85. Document 6: FISC Opinion (2014)

86. Document 7: FISC Opinion and Order (2012)

87. Document 8: FISC Order (Oct. 29, 2013)

88. Document 9: FISC Order Re: DNI/AG 702(g) [Redacted] (2010)

89. Document 10: FISC Order (2009)

90. Document 11: FISC Opinion and Order (2009)

91. Document 12: FISC Opinion on Motion for Disclosure of Prior Decisions (2014)

92. Document 13: FISC Opinion (2010)

93. Document 14: FISC Opinion and Order (Apr. 7, 2009)

94. Document 15: FISC Opinion and Order (Dec. 13, 2013)

95. Document 16: FISC Briefing Order (2010)

96. Document 17: FISC Briefing Order (Oct. 13, 2011)

97. Document 18: FISC Order (Oct. 29, 2013)

**F. Documents Publicly Released by Defendants in *N.Y. Times v. DOJ*, 16-cv-07020 (S.D.N.Y.)**

98. Bates Numbers NYT v. DOJ, 16 CIV 7020_000041-000049: First Tranche (4 documents totaling 11 pages), *available at:* https://www.documentcloud.org/documents/3867003-Savage-NYT-FOIA-2011-FISC-MCT-Files.html

99. Bates Numbers NYT v. DOJ, 16 CIV 7020_000050-000237: Second Tranche (11 documents totaling 175 pages), *available at:* https://www.documentcloud.org/documents/3986047-Savage-NYT-FOIA-NSA-MCT-Bates-Case-Files.html

100. Bates Numbers NYT v. DOJ, 16 CIV 7020_000411-000585: Third Tranche (12 documents totaling 190 pages), *available at:* https://www.documentcloud.org/documents/4064819-Savage-NYT-FOIA-2011-Bates-MCT-third-tranche.html

**G. Other Documents Publicly Released by Defendants**

101. FISC Opinion and Order Concerning "Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications" (filed Nov. 6, 2015)

102. FISC Submission, "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" (filed July 15, 2015)

103. FISC Opinion and Order Concerning "Government's Ex Parte Submission of Reauthorization Certifications and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certifications and Amended Certifications" (Sept. 20, 2012)

DECLARATION OF SCOTT BRADNER

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

# Appendix C

This document was also filed as ECF No. 168-27 and can be found in this Joint Appendix at JA2890.

DECLARATION OF SCOTT BRADNER

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

# Appendix D

This document was also filed as ECF No. 168-22 and can be found in this Joint Appendix at JA2721.

DECLARATION OF SCOTT BRADNER

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

# Appendix E

This document was also filed as ECF No. 168-25 and can be found in this Joint Appendix at JA2790.

DECLARATION OF SCOTT BRADNER

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

# Appendix F

This document was also filed as ECF No. 168-19 and can be found in this Joint Appendix at JA2434.

DECLARATION OF SCOTT BRADNER

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

# Appendix G

# ON DISTRIBUTED COMMUNICATIONS NETWORKS

Paul Baran

September 1962

P-2626

# ON DISTRIBUTED COMMUNICATIONS NETWORKS

Paul Baran*

The RAND Corporation, Santa Monica, California

## INTRODUCTION

The previous paper** described how redundancy of coding can be used to build efficient digital data links out of transmission links of variable and often less than presently useful quality. An arbitrarily low over-all error rate can be purchased with a modest redundancy of coding and clever terminal equipment. But even links with low error rates can have less than perfect reliability.

We should like to extend the remarks of the previous paper and address ourselves to the problem of building

---

*Any views expressed in this paper are those of the author. They should not be interpreted as reflecting the views of The RAND Corporation or the official opinion or policy of any of its governmental or private research sponsors. Papers are reproduced by The RAND Corporation as a courtesy to members of its staff.

This paper was prepared for presentation at the First Congress of the Information Systems Sciences, sponsored by The MITRE Corporation and the USAF Electronic Systems Division, November, 1962.

The writer is indebted to John Bower for his suggestions that switching in any store-and-forward system can be described by a model of a postmaster at a blackboard. Programming assistance provided by Sharla Boehm, John Derr, and Joseph Smith is gratefully acknowledged.

**A prior paper was presented by Paul Rosen and Irwin Lebow of MIT Lincoln Laboratories, discussing redundancy of coding on a single link, "Low Error Efficient Digitial Communications Links," First Congress on the Information Systems Sciences, McGraw-Hill, New York, 1962.

digital communication networks using links with less than perfect reliability. We shall again trade in the currency of redundancy, but instead of redundancy of coding we shall make use of redundancy of connectivity.

This thing called redundancy is a powerful tool. But the systems planner must choose that form of redundancy so that the form of the "noise" or interference appears to be somewhat statistically independent for each redundant element added. If this goal is completely met, there can be an exponential payoff for a linear increase of added elements. As an example, we shall consider in some detail the synthesis of a system where the form of the disturbance or "noise" is the simultaneous destruction of many geographically separated installations. The system in particular is to be a very high-speed digital data transmission network composed of unreliable links, but which exhibits any arbitrarily desired level of system reliability or survivability.

## DEFINITION OF SURVIVABILITY

This communications network shall be composed of several hundred stations which must intercommunicate with one another. Survivability as herein defined is the percentage of stations surviving a physical attack and remaining in electrical connection with the largest single group of surviving stations. This criterion is a measure of the ability of the surviving stations to operate together as a coherent entity after attack.

## TYPES OF NETWORKS

Although one can draw a wide variety of networks, they all factor into two components: centralized (or star) and distributed (or grid or mesh). (Types (a) and (c) in Fig. 1)

The centralized network is basically vulnerable. Destruction of the central node destroys intercommunication between the end stations. In practice, a mixture of star and mesh components is used to form communications networks. For example, type (b) in Fig. 1 shows a hierarchial structure to a set of stars connected in the form of a larger star with an additional link forming a loop. Such a network is sometimes called a "decentralized" network, because complete reliance upon a single point is not always required. But, as destruction of a small number of nodes in a decentralized network can destroy communications, we shall turn to consider the properties, problems, and hopes of building communications networks that are as "distributed" as possible. The unstandardized terms centralized, decentralized, and distributed are often and conveniently used as relative adjectives when referring to real-world networks.

## DEFINITION OF REDUNDANCY LEVEL

Figure 2 defines the term "redundancy level," which is used in this paper as a measure of connectivity. A minimum span network, one formed with the smallest number

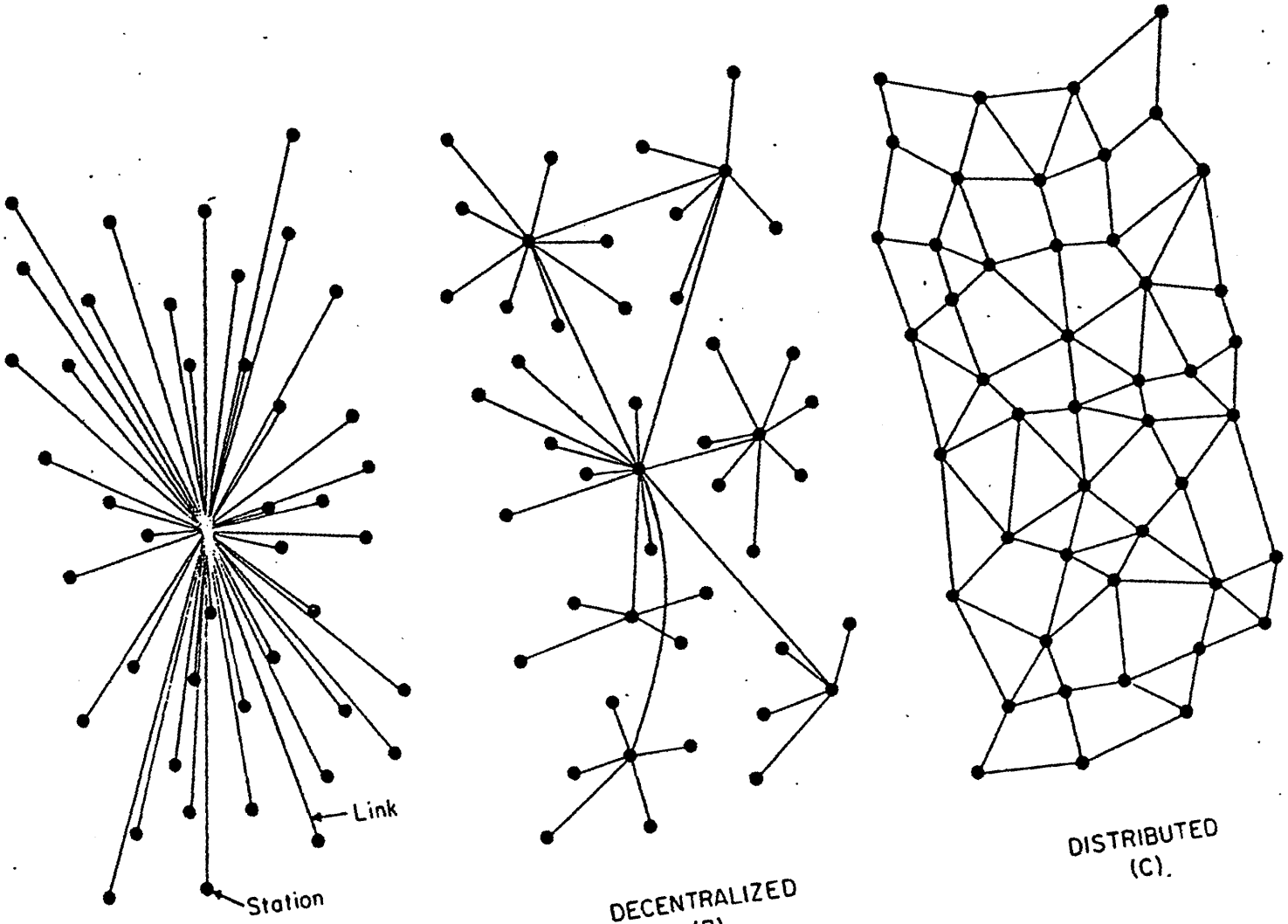



FIG. 1 — Centralized, Decentralized and Distributed Networks

of links possible, is chosen as a reference point, and is called "a network of redundancy level one." If two times as many links are used in a gridded network than in a minimum span network, the network is said to have a redundancy level of two. Figure 2 defines connectivity of 1, 1½, 2, 3, 4, 6, and 8. Redundancy level is equivalent to link-to-node ratio in an infinite size arrays of stations.

ASSUMPTION OF PERFECT SWITCHING

Each node and link in the array of Fig. 2 has the capacity and the switching flexibility to allow transmission between any ith station and any jth station, provided a path can be drawn from the ith to the jth station.

Starting with a network composed of an array of stations connected as in Fig. 3, an assigned percentage of nodes and links are destroyed. If, after this operation, it is still possible to draw a line to connect the ith station to the jth station, the ith and jth stations are said to be connected.

RATIONALE FOR DESTRUCTION PATTERNS

Figure 4 indicates network performance as a function of the probability of destruction for each separate node. If the expected "noise" was destruction caused by conventional hardware failure, the failures would be randomly distributed through the network. But, if the disturbance

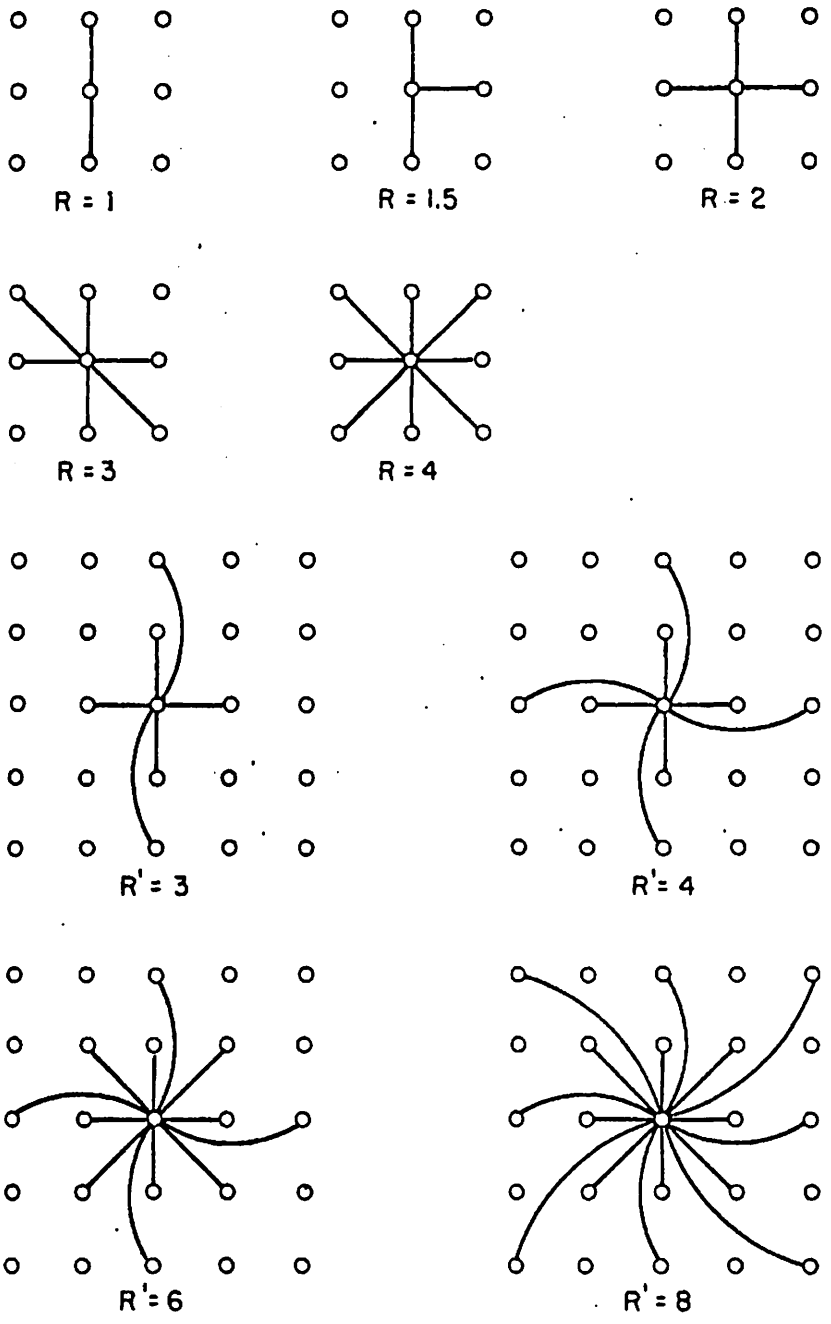



FIG. 2 – Definition of Redundancy Level

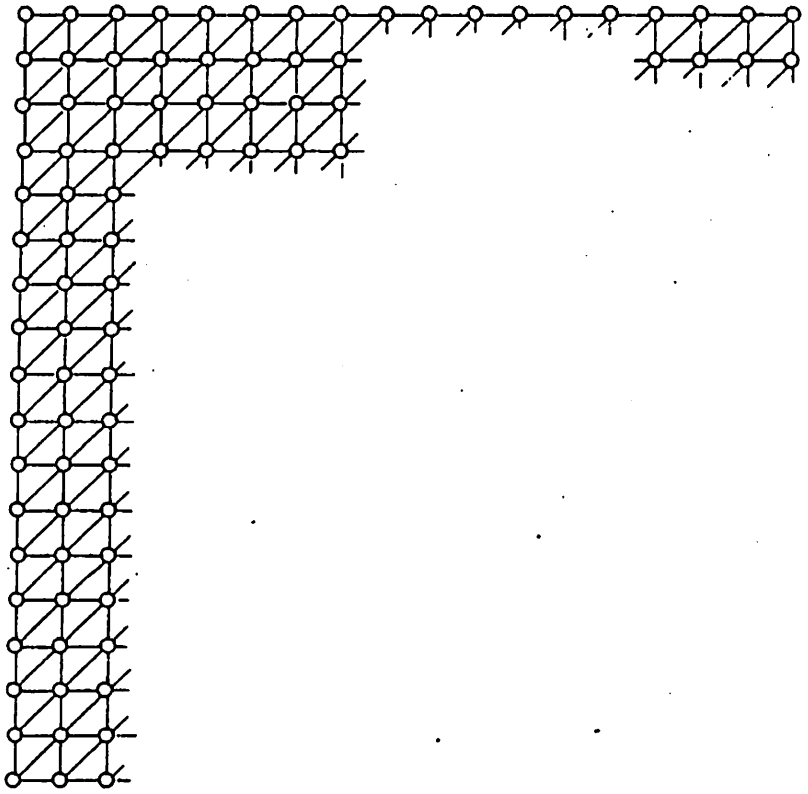


FIG. 3 — An Array of Stations

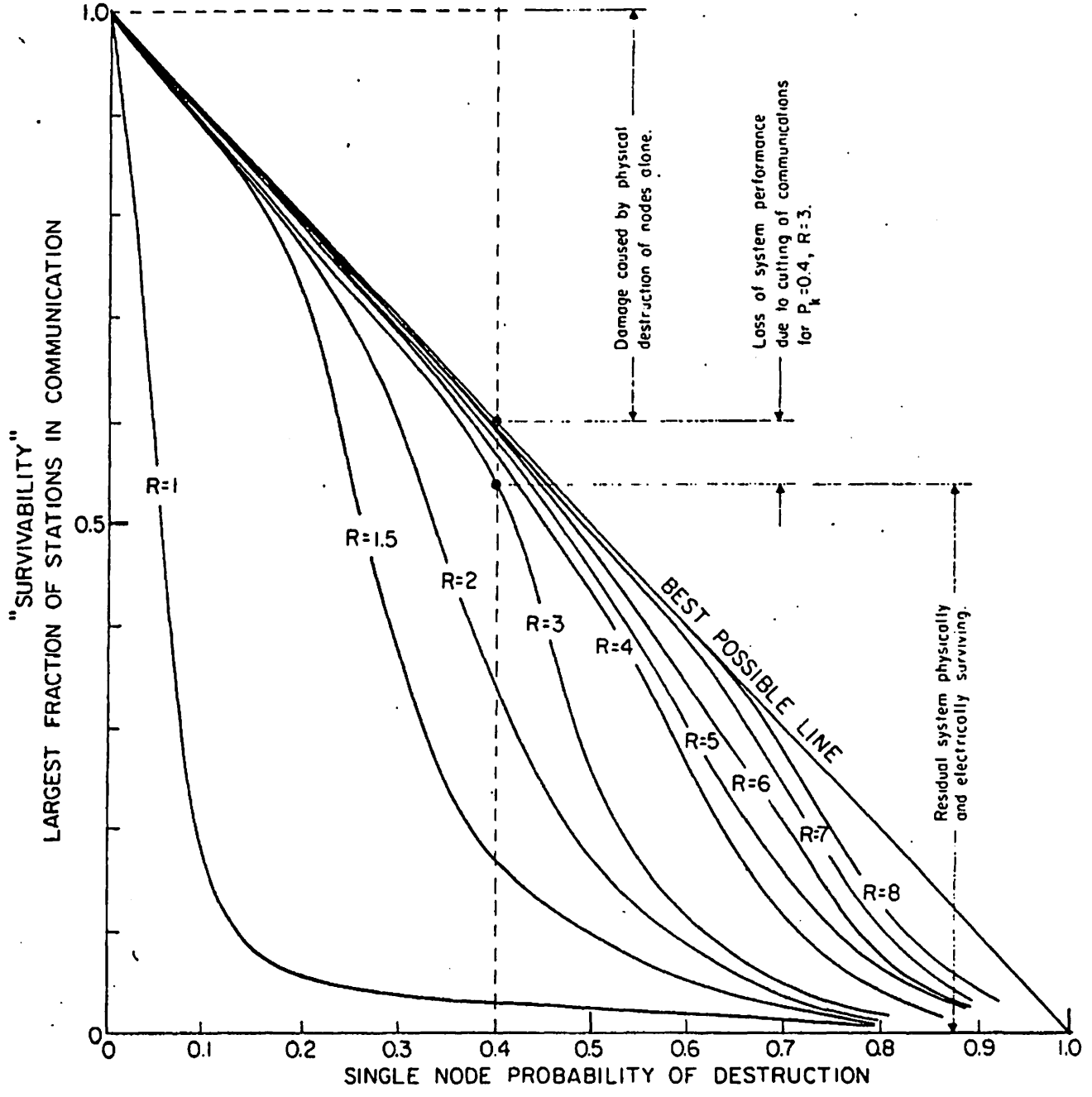



FIG. 4 — Perfect Switching in a Distributed Network — Sensitivity to Node Destruction, 100% of Links Operative.

were caused by enemy attack there are two possible "worst cases" to be considered.

To bisect a 32-link width network requires direction of 288 weapons each with a probability of kill, $p_k = 0.5$, or 160 with a $p_k = 0.7$, to produce over an 0.9 probability of successfully bisecting the network. If hidden alternative command is allowed, then the largest single group would still have an expected value of almost 50 percent of the initial stations surviving intact. If this raid misjudges complete availability of weapons, or complete knowledge of all links in the cross section, or the effects of the weapons against each and every link, the raid fails. The high risk of such raids against highly parallel structures causes examination of alternative attack policies. Consider the following uniform raid example. Assume that 2,000 weapons are deployed against a 1000-station network. The stations are so spaced that destruction of two stations with a single weapon is unlikely. Divide the 2,000 weapons into two equal 1,000 weapon salvos. Assume any probability of destruction of a single node from a single weapon less than 1.0; for example, 0.5. Each weapon on the first salvo has a 0.5 probability of destroying its target. But, each weapon of the second salvo has only a 0.25 probability, since one-half the targets have already been destroyed. Thus, the uniform attack is felt to represent a worst-case configuration.

MONTE CARLO SIMULATION

Such worst-case attacks have been directed against an 18x18-array network model of 324 nodes with varying probability of kill and redundancy level, with results shown in Fig. 4. The probability of kill was varied from zero to unity along the abscissa while the ordinate marks survivability. The criterion of survivability used is the percentage of stations not physically destroyed and remaining in communications with the largest single group of surviving stations. The curves of Fig. 4 demonstrate survivability as function of attack level for networks of varying degrees of redundancy. The line labeled "best possible line" marks the upper bound of loss due to the physical failure component alone. For example, if a network underwent an attack of 0.5 probability destruction of each of its nodes, then only 50 per cent of its nodes would be expected to survive--regardless of how perfect its communications. We are primarily interested in the additional system degradation caused by failure of communications. Two key points are to be noticed in the curves of Fig. 4. First, extremely survivable networks can be built using a moderately low redundancy of connectivity level. Redundancy levels on the order of only three permit withstanding extremely heavy level attacks with negligible additional loss to communications. Secondly, the survivability curves have sharp break-points.

A network of this type will withstand an increasing attack level until a certain point is reached, beyond which the network rapidly deteriorates. Thus, the optimum degree of redundancy can be chosen as a function of the expected level of attack. Further redundancy buys little. The redundancy level required to survive even very heavy attacks is not great--on the order of only three or four times that of the minimum span network.

SIMULATION RESULTS--LINK FAILURE ONLY

In the previous example we have examined network performance as a function of the destruction of the nodes (which are better targets than links). We shall now reexamine the same network, but using unreliable links. In particular, we want to know how unreliable the links may be without further degrading the performance of the network.

Figure 5 shows the results for the case of perfect nodes; only the links fail. There is little system degradation caused even using extremely unreliable links--on the order of 50 percent down-time--assuming all nodes are working.

COMBINATION LINK AND NODE FAILURES

The worst case is the composite effect of failures of both the links and the nodes. Figure 6 shows the effect of link failure upon a network having 40 percent of its nodes destroyed. It appears that what would today be regarded as an unreliable link can be used in a distributed

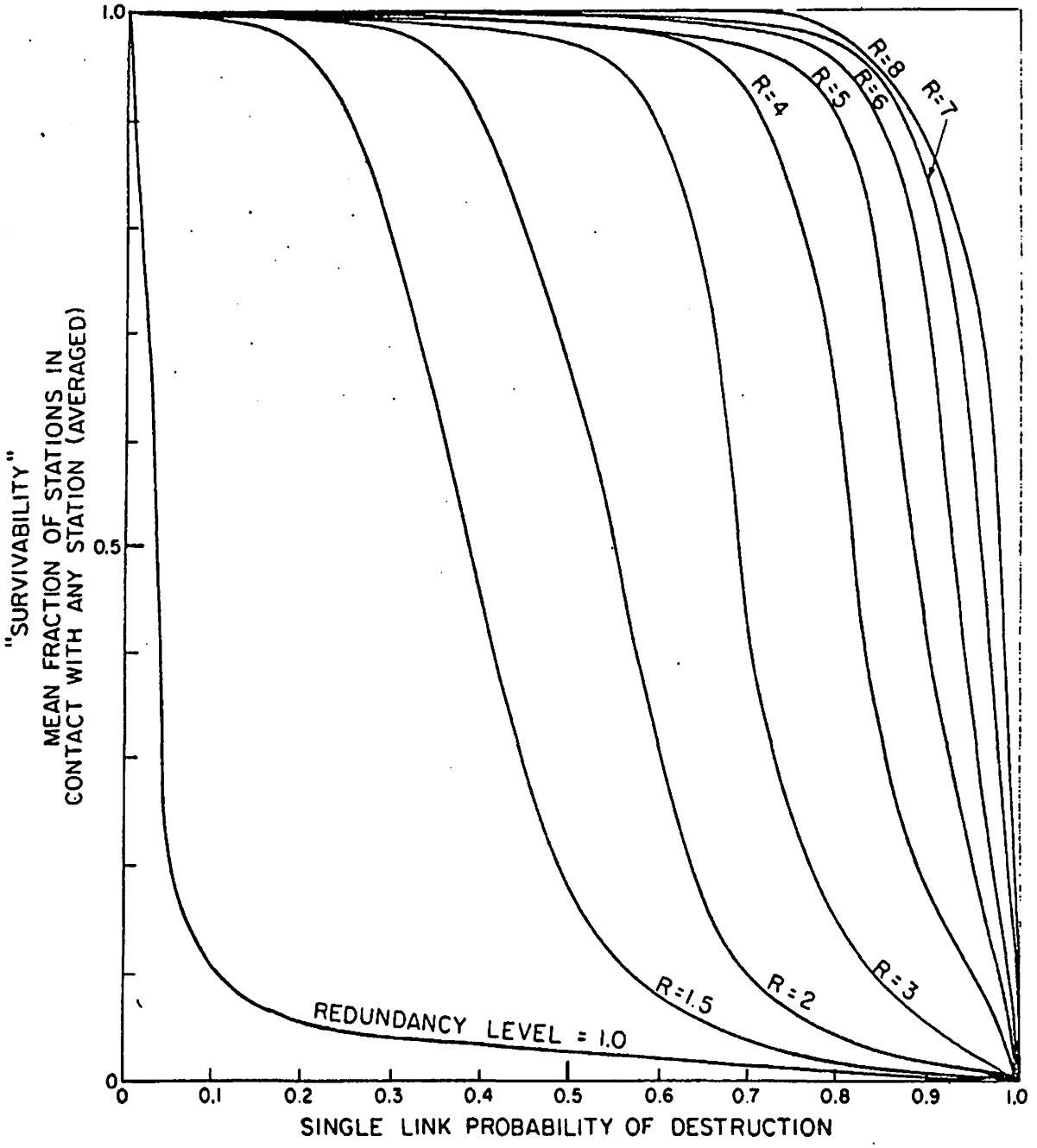



FIG. 5 — Perfect Switching in a Distributed Network — Sensitivity to Link Destruction, 100% of Nodes Operative.

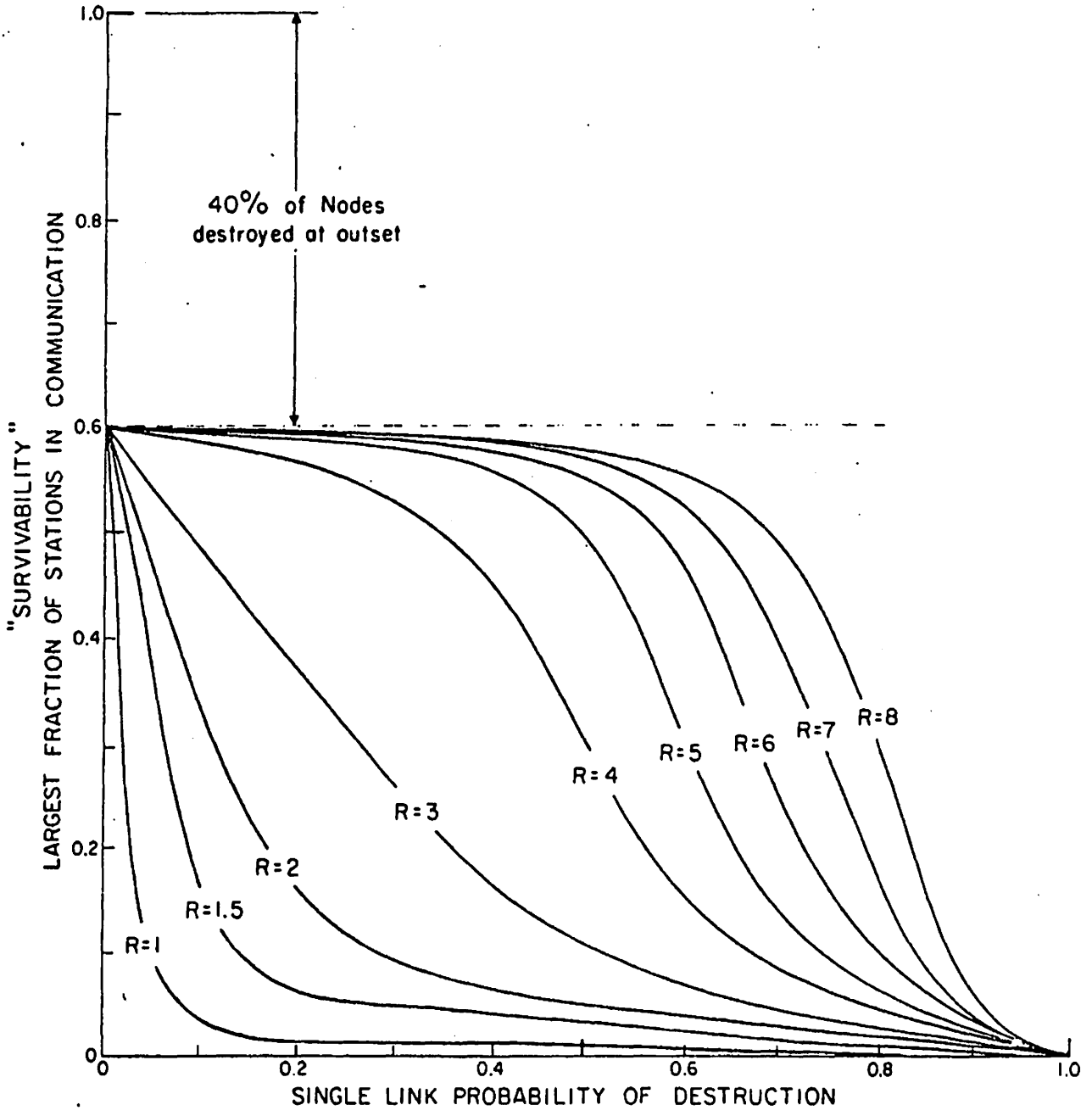



FIG. 6 – Perfect Switching in a Distributed Network — Sensitivity to Link Destruction After 40% Nodes Are Destroyed.

network almost as effectively as perfectly reliable links. Figure 7 examines the result of 100 trial cases in order to estimate the probability density distribution of system performance for a mixture of node and link failures. This is the distribution of cases for 20 percent nodal damage and 35 percent link damage.

DIVERSITY OF ASSIGNMENT

There is another and more common technique for using redundancy than in the method described above in which each station is assumed to have perfect switching ability. This alternative approach is called "diversity of assignment." In diversity of assignment, switching is not required. Instead, a number of independent paths are selected between each pair of stations in a network which requires reliable communications. But, there are marked differences in performance between distributed switching and redundancy of assignment as revealed by the following Monte Carlo simulation.

In the matrix of N separate stations, each ith station is connected to every jth station by three shortest but totally separate independent paths ($i=1,2,3,\ldots,N$; $j=1,2,3,\ldots,N$; $i \neq j$). A raid is laid against the network. Each of the pre-assigned separate paths from the ith station to the jth station is examined. If one or more of the pre-assigned paths survive, communication is said to exist between the ith and the jth station. The criterion of

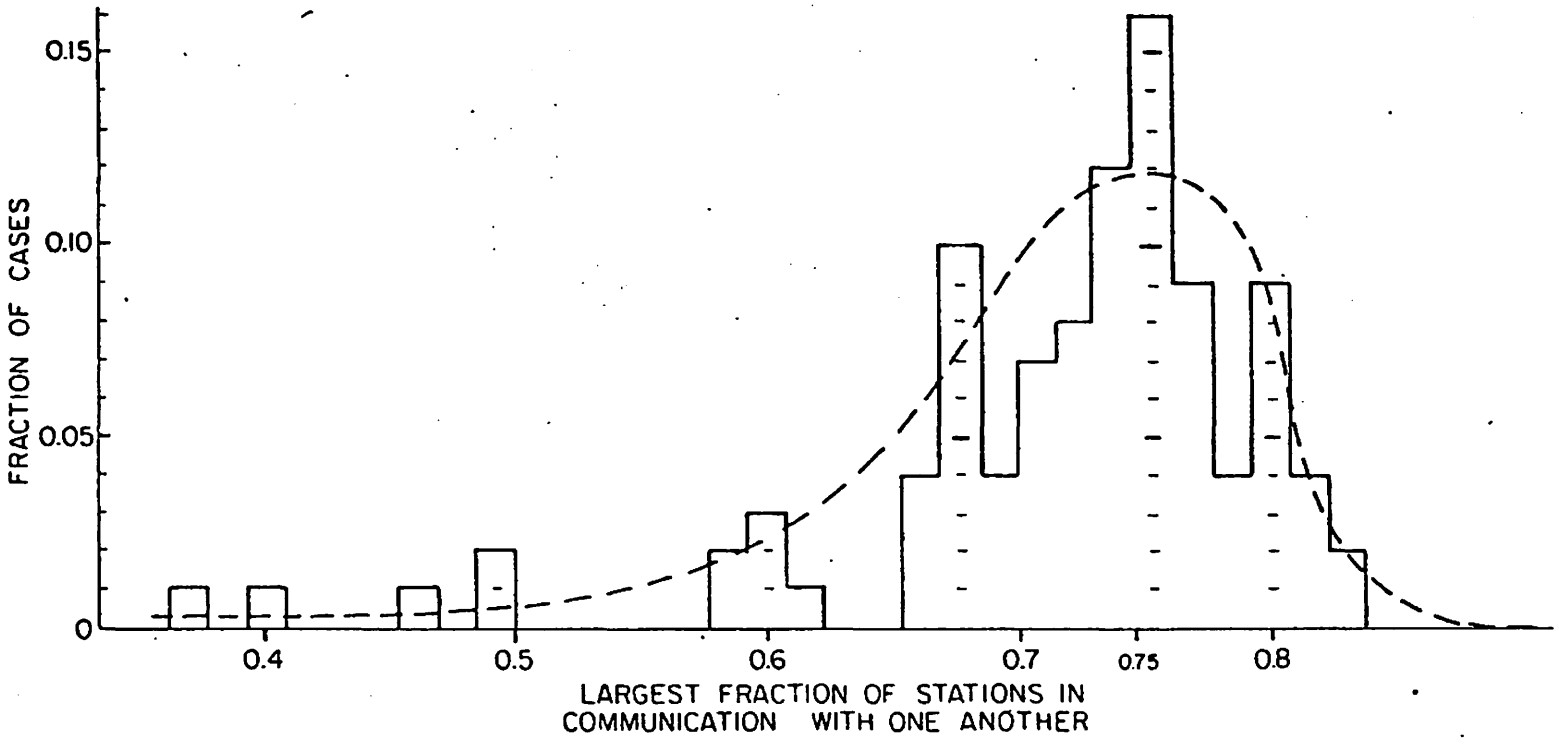



FIG. 7 — Probability Density Distribution of Largest Fraction of Stations in Communication Perfect Switching, R = 3, 100 Cases, 80% Node Survival, 65% Link Survival.

survivability used is the mean number of stations connected to each station, averaged over all stations.

Figure 8 shows, unlike the distributed perfect switching case, that there is a marked loss in communications capability with even slightly unreliable nodes or links. The difference can be visualized by remembering that fully flexible switching permits the communicator the privilege of ex post facto decision of paths. Figure 8 emphasizes a key difference between some present day networks and the fully flexible distributed network we are discussing.

COMPARISON WITH PRESENT SYSTEMS

Present conventional switching systems try only a small subset of the potential paths that can be drawn on a gridded network. The greater the percentage of potential paths tested, the closer one approaches the performance of perfect switching. Thus, perfect switching provides an upper bound of expected system performance for a gridded network; the diversity of assignment case, a lower bound. Between these two limits lie systems composed of a mixture of switched routes and diversity of assignment.

Diversity of assignment is useful for short paths, eliminating the need for switching, but requires survivability and reliability for each tandem element in long haul circuits passing through many nodes. As every component in at least one out of a small number of possible paths

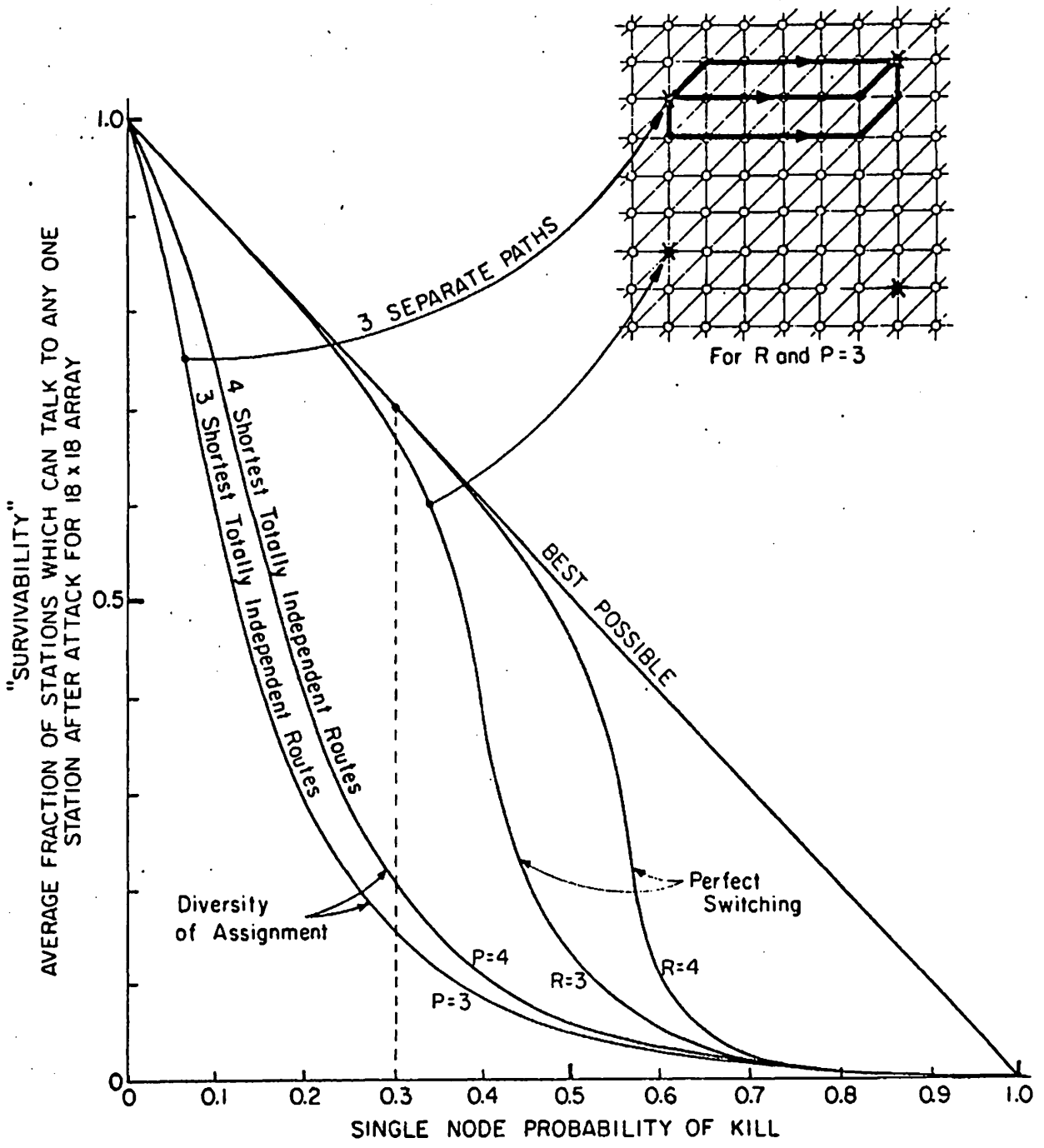



FIG. 8 – Diversity of Assignment vs. Perfect Switching in a Distributed Network.

must be simultaneously operative, high reliability margins and full standby equipment are usual.

ON FUTURE SYSTEMS

We will soon be living in an era in which we cannot guarantee survivability of any single point. However, we can still design systems in which system destruction requires the enemy to pay the price of destroying n of n stations. If n is made sufficiently large, it can be shown that highly survivable system structures can be built--even in the thermonuclear era. In order to build such networks and systems we will have to use a large number of elements. We are interested in knowing how inexpensive these elements may be and still permit the system to operate reliably. There is a strong relationship between element cost and element reliability. To design a system that must anticipate a worst-case destruction of both enemy attack, and normal system failures, one can combine the expected failures expected by enemy attack together with the failures caused by normal reliability problems, provided the enemy does not know which elements are inoperative. Our future systems design problem is that of building very reliable systems out of the described set of unreliable elements at lowest cost. In choosing the communications links of the future, digital links appear increasingly attractive by permitting low cost switching and low cost links. For example, if "perfect

switching" is used, digital links are mandatory to permit tandem connection of many separately connected links without cumulative errors reaching an irreducible magnitude. Further, the signalling measures to implement highly flexible switching doctrines always require digits.

FUTURE LOW COST ALL-DIGITAL COMMUNICATIONS LINKS

When one designs an entire system optimized for digits and high redundancy, certain new communications-link techniques appear more attractive than those common today.

A key attribute of the new media is that it permits formation of new routes cheaply, yet allows transmission on the order of a million or so bits per second, high enough to be economic, but yet low enough to be inexpensively processed with existing digital computer techniques at the relay station nodes. Reliability and raw error rates are secondary. The network must be built with the expectation of heavy damage, anyway. Powerful error removal methods exist.

Some of the communication construction methods that look attractive in the near future include pulse regenerative repeater line, "poor-boy" microwave, TV broadcast station digital transmission, and non-synchronous satellites.

Pulse Regenerative Repeater Line

Samuel B. Morse's regenerative repeater invention for amplifying weak telegraphic signals has recently been

resurrected and transistorized. Morse's electrical relay permits amplification of weak binary telegraphic signals above a fixed threshold. Experiments by various organizations (primarily the Bell Telephone Laboratories) have shown that digital data rates on the order of 1.5 million bits per second can be transmitted over ordinary telephone line at repeater spacings on the order of 6,000 feet for #22 gage pulp paper insulated copper pairs. At present, up to 20 tandemly connected amplifiers have been used without retiming synchronization problems. There appears to be no fundamental reason why either lines of lower loss with corresponding further repeater spacing, or more powerful resynchronization methods cannot be used to extend link distances to in excess of 100 miles. Such distances would be desired for a possible national distributed network.

Power to energize the miniature transistor amplifier is transmitted over the copper circuit itself.

"Poor-Boy" Microwave

While the price of microwave equipment has been declining, there are still untapped major savings. In an analog signal network we require a high degree of reliability and very low distortion for each tandem repeater. However, using digital modulation together with perfect switching we minimize these two expensive considerations from our planning. We would envision the use of almost mass-produced

microwave crystal receiver/klystron oscillator units mounted on "telegraph poles" carrying commercial power. Relay station spacing would probably be on the order of 10+ miles. Further economies can be obtained by only a minimal use of standby equipment and reduction of fading margins. The ability to use alternate paths permits consideration of frequencies normally troubled by rain attenuation problems reducing the spectrum availability problem.

While this technique has not been fully examined, preliminary indications suggest that this may be the cheapest way of building large networks of the type to be described.

T. V. Stations

With proper siting of receiving antennas, broadcast television stations might be used to form additional high data rate links in emergencies.

Non-Synchronous Satellites

The problem of building a reliable network using non-synchronous satellites is somewhat similar to that of building a communications network with unreliable links. When a satellite is overhead, the link is operative. When a satellite is not overhead, the link is out of service. Thus, such links are highly compatible with the type of system to be described.

VARIABLE DATA RATE LINKS

In a conventional circuit switched system each of the tandem links require matched transmission bandwidths. But, in the previous paper,* it was seen that in order to make fullest use of a digital link the post-error-removal data rate would have to vary as it is a function of noise level. The problem then is to build a communication network made up of links of variable data rate to use the communication resource most efficiently.

VARIABLE DATA RATE USERS

Not only will the links of a digital data transmission operate at a variable data rate, so will the users. Many digital transmission applications are highly intermittent in nature, with each potential network user varying his demand from instant to instant. For example, if one transmitted one line of a 60 w.p.m. teletype message over a high-data "express route" operating at 1,500,000 bits per second, a 1/3 millisecond burst would be sent every 12 seconds. Where high data rate transmission links serve many subscribers on a time division basis, both the user and the network links will appear to be operating at a highly variable data rate.

---

*See footnote, p. 1.

COMMON USER

In communications, as in transportation, it is most economic for many users to share a common resource rather than each to build his own system--particularly when supplying intermittent or occasional service. This intermittency of service is highly characteristic of digital communication requirements. Therefore, we would like to consider the interconnection, one day, of many all digital links to provide a resource optimized for the handling of data for many potential intermittent users--a new common-user system.

Figure 9 demonstrates the basic notion. A wide mixture of different digital transmission links is combined to form a common resource divided among many potential users. But, each of these communications links could possibly have a different data rate. How can links of different data rates be interconnected?

USE OF STANDARD MESSAGE BLOCK

Present common carrier communications networks, used for digital transmission, use links and concepts originally designed for another purpose--voice. These systems are built around a frequency division multiplexing link-to-link interface standard. The standard between links is that of data rate. Time division multiplexing appears so natural to data transmission that we might wish to

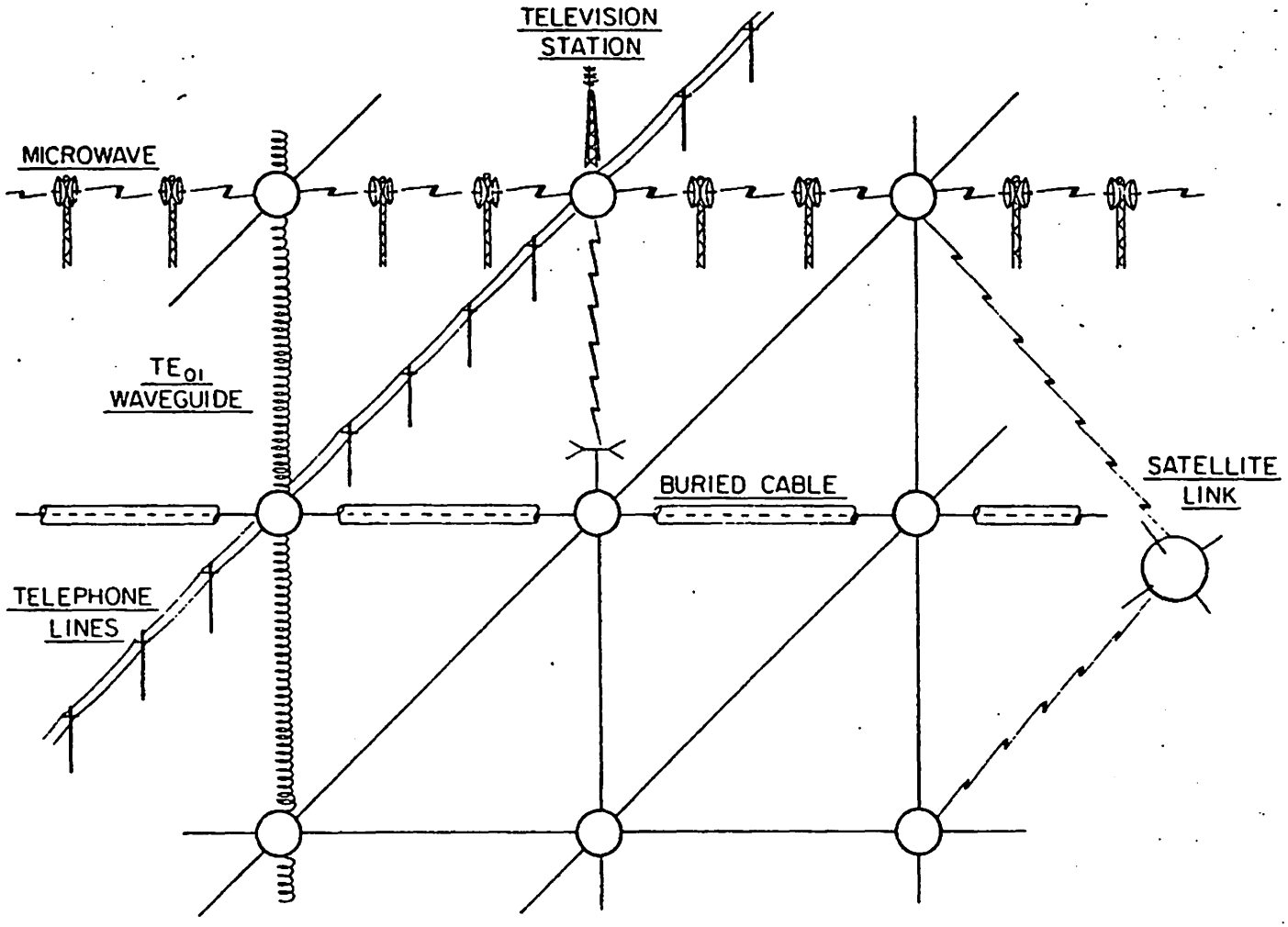



FIG. 9 – All Digital Network Composed of Mixture of Links

consider an alternative approach--a standardized message block as a network interface standard. While a standardized message block is common in many computer-communications applications, no serious attempt has ever been made to use it as a universal standard. A universally standardized message block would be composed of perhaps 1024 bits. Most of the message block would be reserved for whatever type data is to be transmitted, while the remainder would contain housekeeping information such as error detection and routing data, as in Fig. 10.

As we move to the future, there appears to be an increasing need for a standardized message block for our all-digital communications networks. As data rates increase, the velocity of propagation over long links becomes an increasingly important consideration.* We soon reach a point where more time is spent setting the switches in a conventional circuit switched system for short holding-time messages than is required for actual transmission of the data.

Most importantly, standardized data blocks permit many simultaneous users each with widely different bandwidth requirements to economically share a broadband network made up of varied data rate links.

---

*3000 miles at $\simeq$ 150,000 miles/sec. $\simeq$ 50 milliseconds transmission time, T.
1024-bit message at 1,500,000 bits/sec. $\simeq$ 2/3 millisecond message time, M.
$\therefore$ T>>M

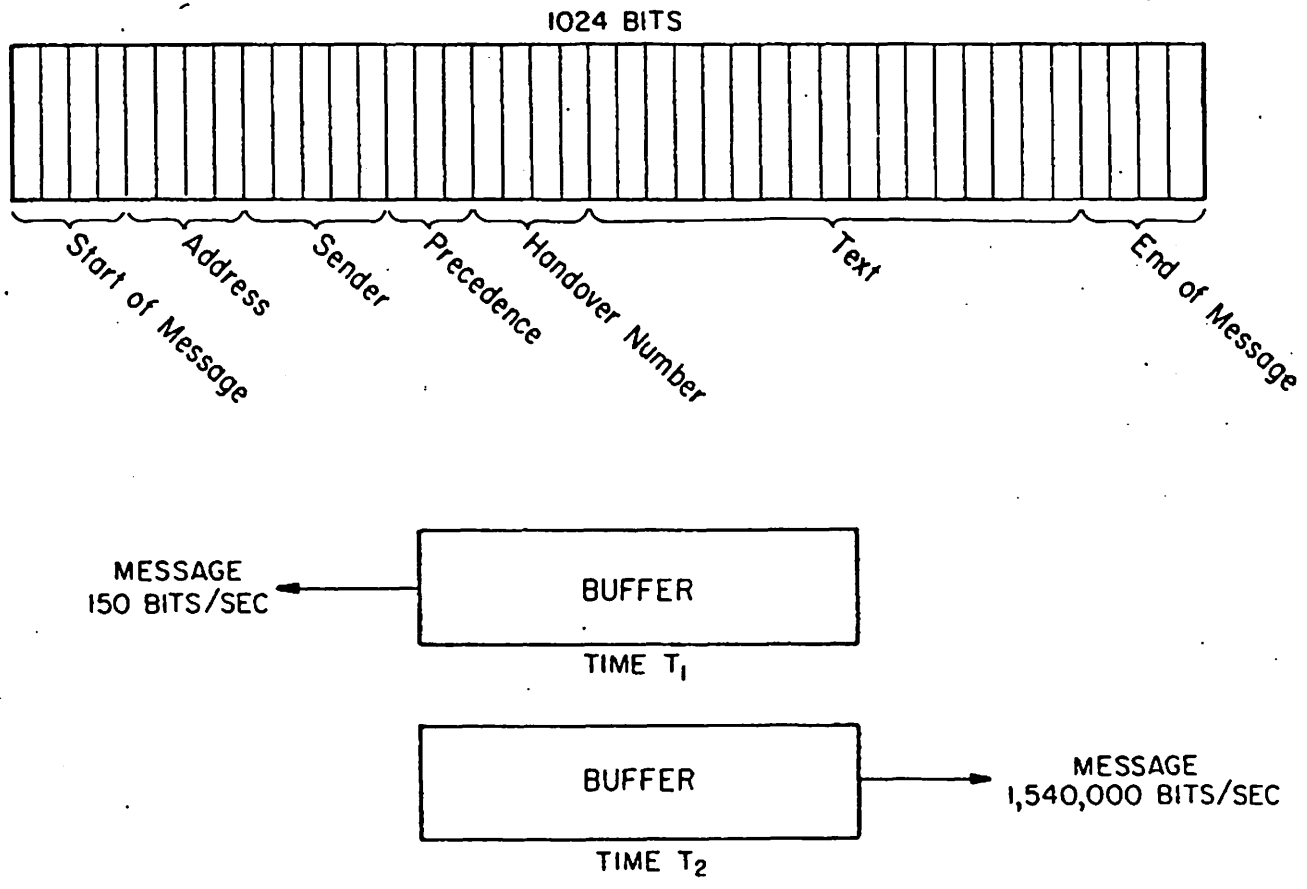



FIG. 10 — Message Block

The standardized message block simplifies construction of very high speed switches. Every user connected to the network can feed data at any rate up to a maximum value. The user's traffic is stored until a full data block is received by the first station. This block is rubber stamped with a heading and return address, plus additional housekeeping information. Then, it is transmitted into the network.

SWITCHING

In order to build a network with the survivability properties shown in Fig. 4, we must use a switching scheme able to find any possible path that might exist after heavy damage. The routing doctrine should find the shortest possible path and avoid self-oscillatory or "ring-around-the-rosey" switching.

We shall explore the possibilities of building a "real-time" data transmission system using store and forward techniques. The high data rates of the future carry us into a hybrid zone between store-and-forward and circuit switching. The system to be described is clearly store-and-forward if one examines the operations at each node singularly. But, the network user who has called up a "virtual connection" to an end station and has transmitted messages across the United States in a fraction of a second might also view the system as a black box providing

an apparent circuit connection across the U.S. There are two requirements that must be met to build such a quasi-real time system. First, the in-transit storage at each node should be minimized to prevent undesirable time delays. Secondly, the shortest instantaneously available path through the network should be found with the expectation that the status of the network will be rapidly changing. Microwave would be subject to fading interruptions and there would be rapid moment-to-moment variations in input loading. These problems place difficult requirements upon the switching. However, the development of digital computer technology has advanced so rapidly that it now appears possible to satisfy these requirements by a moderate amount of digital equipment. What is envisioned is a network of unmanned digital switches implementing a self-learning policy at each node so that overall traffic is effectively routed in a changing environment--without need for a central and possibly vulnerable control point. One particularly simple routing scheme examined is called the "hot-potato" heuristic routing doctrine and will be described in detail.

Torn-tape telegraph repeater stations and our mail system provide examples of conventional store-and-forward switching systems. In these systems, messages are relayed from station-to-station and stacked until the "best" outgoing link is free. The key feature of store-and-

forward transmission is that it allows a high line occupancy factor by storing so many messages at each node that there is a backlog of traffic awaiting transmission. But, the price for link efficiency is the price paid in storage capacity and time delay. However, it was found that most of the advantages of store-and-forward switching could be obtained with extremely little storage at the nodes.

Thus, in the system to be described, each node will attempt to get rid of its messages by choosing alternate routes if its preferred route is busy or destroyed. Each message is regarded as a "hot potato," and the nodes are not wearing gloves. Rather than hold the "hot potato," the node tosses the message to its neighbor, who will now try to get rid of the message.

## THE POSTMAN

The switching process in any store-and-forward system is analogous to a postman sorting mail. A postman sits at each switching node. Messages arrive simultaneously from all links. The postman records bulletins describing the traffic loading status for each of the outgoing links. With proper status information, the postman is able to determine the best direction to send out any letters. So far, this mechanism is general and applicable to all store-and-forward communication systems.

HOT-POTATO HEURISTIC ROUTING DOCTRINE

To achieve real-time operation it is desirable to respond to change in network status as quickly as possible so we shall seek to derive the network status information directly into each message block.

Each standardized message block contains a "to" address, a "from" address, a handover number tag, and error detecting bits together with other housekeeping data. The message block is analogous to a letter. The "from" address is equivalent to the return address of the letter.

The handover number is a tag in each message block set to zero upon initial transmission of the message block into the network. Every time the message block is passed on, the handover number is incremented. The handover number tag on each message block indicates the length of time in the network or path length. This tag is somewhat analogous to the cancellation date of a conventional letter.

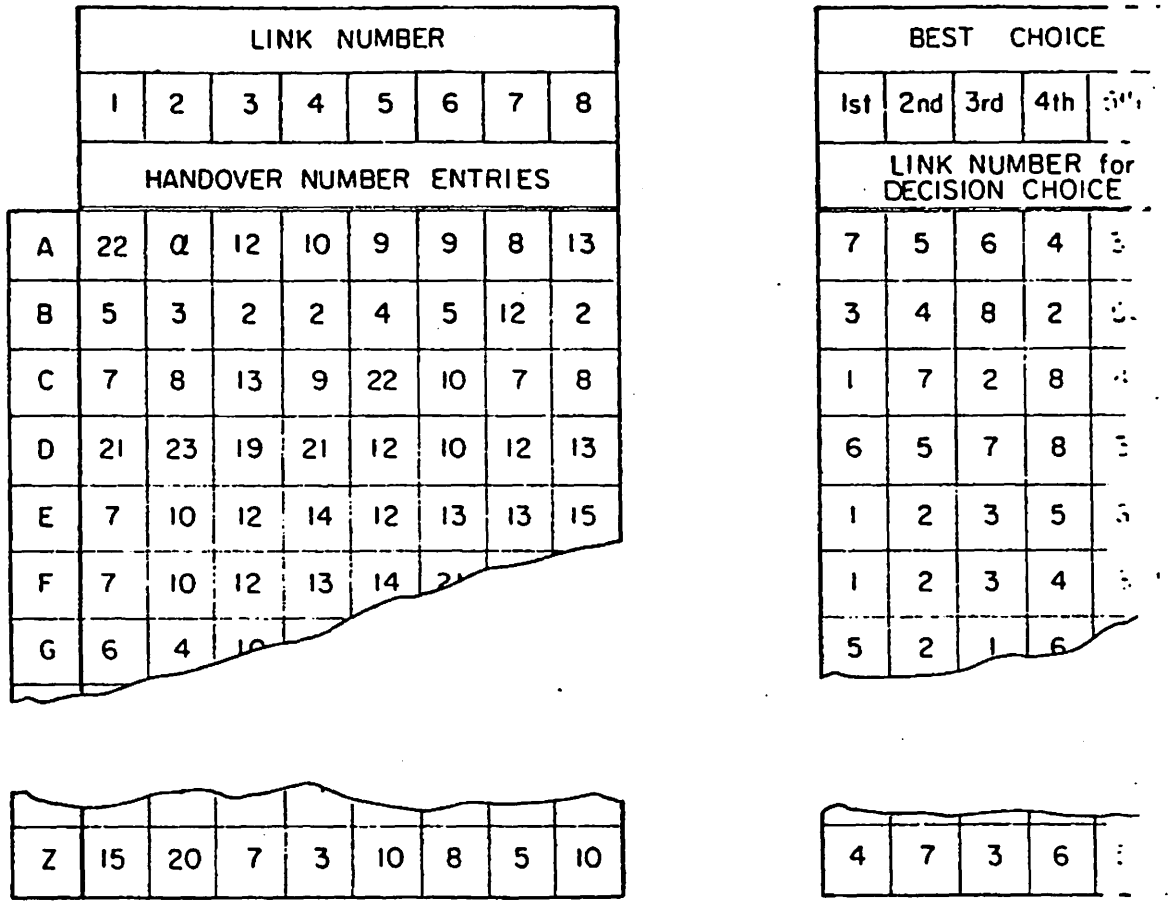
INDUCTIVE DETERMINATION OF BEST PATH

Assuming symmetrical bi-directional links, the postman can infer the "best" paths to transmit mail to any station merely by looking at the cancellation time or the equivalent handover number tag. If the postman sitting in the center of the United States received letters from San Francisco, he would find that letters from San Francisco arriving from channels to the west would come in with later cancellation dates than if such letters had

arrived in a roundabout manner from the east. Each letter carries an implicit indication of its length of transmission path. The astute postman can then deduce that the best channel to send a message to San Francisco is probably the link associated with the latest cancellation dates of messages from San Francisco. By observing the cancellation dates for all letters in transit, information is derived to route future traffic. The return address and cancellation date of recent letters is sufficient to determine the best direction to which to send subsequent letters.

THE HANDOVER NUMBER TABLE

While cancellation dates could conceivably be used on digital messages, it is more convenient to think in terms of a simpler digital analogy--a tag affixed to each message and incremented every time the message is relayed. Figure 11 shows the handover table located in the memory of a single node. A row is reserved for each major station of the network allowed to generate traffic. A column is assigned to each separate link connected to a node. As it was shown that redundancy levels on the order of four can create extremely "tough" networks and additional redundancy brought little, only about eight columns are really needed.



| | LINK NUMBER | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| | HANDOVER NUMBER ENTRIES | | | | | | | |
| A | 22 | α | 12 | 10 | 9 | 9 | 8 | 13 |
| B | 5 | 3 | 2 | 2 | 4 | 5 | 12 | 2 |
| C | 7 | 8 | 13 | 9 | 22 | 10 | 7 | 8 |
| D | 21 | 23 | 19 | 21 | 12 | 10 | 12 | 13 |
| E | 7 | 10 | 12 | 14 | 12 | 13 | 13 | 15 |
| F | 7 | 10 | 12 | 13 | 14 | 21 | | |
| G | 6 | 4 | 10 | | | | | |
| Z | 15 | 20 | 7 | 3 | 10 | 8 | 5 | 10 |

| BEST CHOICE | | | | |
|---|---|---|---|---|
| 1st | 2nd | 3rd | 4th | 5th |
| LINK NUMBER for DECISION CHOICE | | | | |
| 7 | 5 | 6 | 4 | 3 |
| 3 | 4 | 8 | 2 | 6 |
| 1 | 7 | 2 | 8 | 4 |
| 6 | 5 | 7 | 8 | 3 |
| 1 | 2 | 3 | 5 | 6 |
| 1 | 2 | 3 | 4 | 5 |
| 5 | 2 | 1 | 6 | |
| 4 | 7 | 3 | 6 | |

FIG. 11 — The Handover Number Table

PERFECT LEARNING

If the network used perfectly reliable, error free links, we might fill out our table in the following manner. Initially, set entries on the table to high values. Examine the handover number of each message arriving on each line for each station. If the observed handover number is less than the value already entered on the handover number table, change the value to that of the observed handover number. If the handover number of the message is greater than the value on the table, do nothing. After a short time this procedure will shake down the table to indicate the path length to each of the stations over each of the links connected to neighboring stations. This table can now be used to route new traffic. For example, if one wished to send traffic to station C, he would examine the entries for the row listed for station C based on traffic from C. Select the link corresponding to the column with the lowest handover number. This is the shortest path to C. If this preferred link is busy, do not wait, choose the next best link that is free.

DIGITAL SIMULATION OF PERFECT LEARNING

This basic routing procedure was tested by a Monte Carlo simulation of a 7x7 array of stations.* All tables were started completely blank to simulate a worst-case starting condition where no station knew the location of any other station. Within ½ second of simulated real world time, the network had learned the locations of all connected stations and was routing traffic in an efficient manner. The mean measured path length compared very favorably to the absolute shortest possible path length under various traffic loading conditions. Preliminary results indicate that network loadings on the order of 50 per cent of link capacity could be inserted without undue increase of path length. When local busy spots occur in the network, locally generated traffic is intermittently restrained from entering the busy points while the potential traffic jams clear. Thus, to the user, the network appears to be a variable data rate system. If the network is carrying light traffic, any new input line into the network would accept full traffic up to 1.5 million bits per second. But, if every station had heavy traffic and the network became heavily loaded, the total allowable input data rate from any single station in the network might

*Paul Baran and Sharla Boehm, Simulation of a Hot Potato Routing Doctrine (U), The RAND Corporation, RM-3103, (In preparation).

drop to perhaps 0.5 million bits per second. The absolute minimum guaranteed data capacity into the network from any station is a function of the location of the station in the network, redundancy level, and the mean path length of transmitted traffic in the network. The "choking" of input procedure has been simulated in the network and no signs of instability under overload noted. It was found that most of the advantage of store-and-forward transmission can be provided in a system having relatively little memory capacity. The network "guarantees" delivery of all traffic that it has accepted from a user.

FORGETTING AND IMPERFECT LEARNING

We have briefly considered network behavior when all links are working. But, we are also interested in determining network behavior with real world links--some destroyed, while others are being repaired. The network can be made rapidly responsive to the effects of destruction, repair, and transmission fades by a slight modification of the rules for computing the values on the handover number table. In the previous example, the lowest handover number ever encountered for a given origination, or "from" station, and over each link, was the value recorded in the handover number table. But, if some links had failed, our table would not have responded to the change. Thus, we must be more responsive to recent measurements

than old ones. This effect can be included in our calculation by the following policy. Take the most recently measured value of handover number; subtract the previous value found in the handover table; if the difference is positive, add a fractional part of this difference to the table value to form the updated table value. This procedure merely implements a "forgetting" procedure--placing more belief upon more recent measurements and less on old measurements. This device would, in the case of network damage, automatically modify the handover number table entry so as to exponentially and asymptotically approach the true shortest path value. If the difference between measured value minus the table value is negative, the new table value would change by only a fractional portion of the recently measured difference.

This implements a form of sceptical learning. Learning will take place even with occasional errors. Thus, by the simple device of using only two separate "learning constants," depending whether the measured value is greater or less than the table value, we can provide a mechanism that permits the network routing to be responsive to varying loads, breaks, and repairs. This learning and forgetting technique has been simulated for a few limited cases and was found to work well.

ADAPTATION TO ENVIRONMENT

This simple simultaneous learning and forgetting mechanism implemented independently at each node causes the entire network to suggest the appearance of an adaptative system responding to gross changes of environment in several respects, without human intervention. For example, consider self-adaptation to station location. A station, Able, normally transmitted from one location in the network, as shown in Fig. 12 (a). If Able moved to the location shown in Fig. 12 (b), all he need do to announce his new location is to transmit a few seconds of dummy traffic. The network will quickly relearn the new location and direct traffic toward Able at his new location. The links could also be cut and altered, yet the network would relearn. Each node sees its environment through myopic eyes by only having links and link status information to a few neighbors. There is no central control; only a simple local routing policy is performed at each node, yet the overall system adapts.

LOWEST COST PATH

We seek to provide the lowest cost path for data to be transmitted between users. When we consider complex networks, perhaps spanning continents, we encounter the problem of building networks with links of widely different data rates. How can paths be taken to encourage

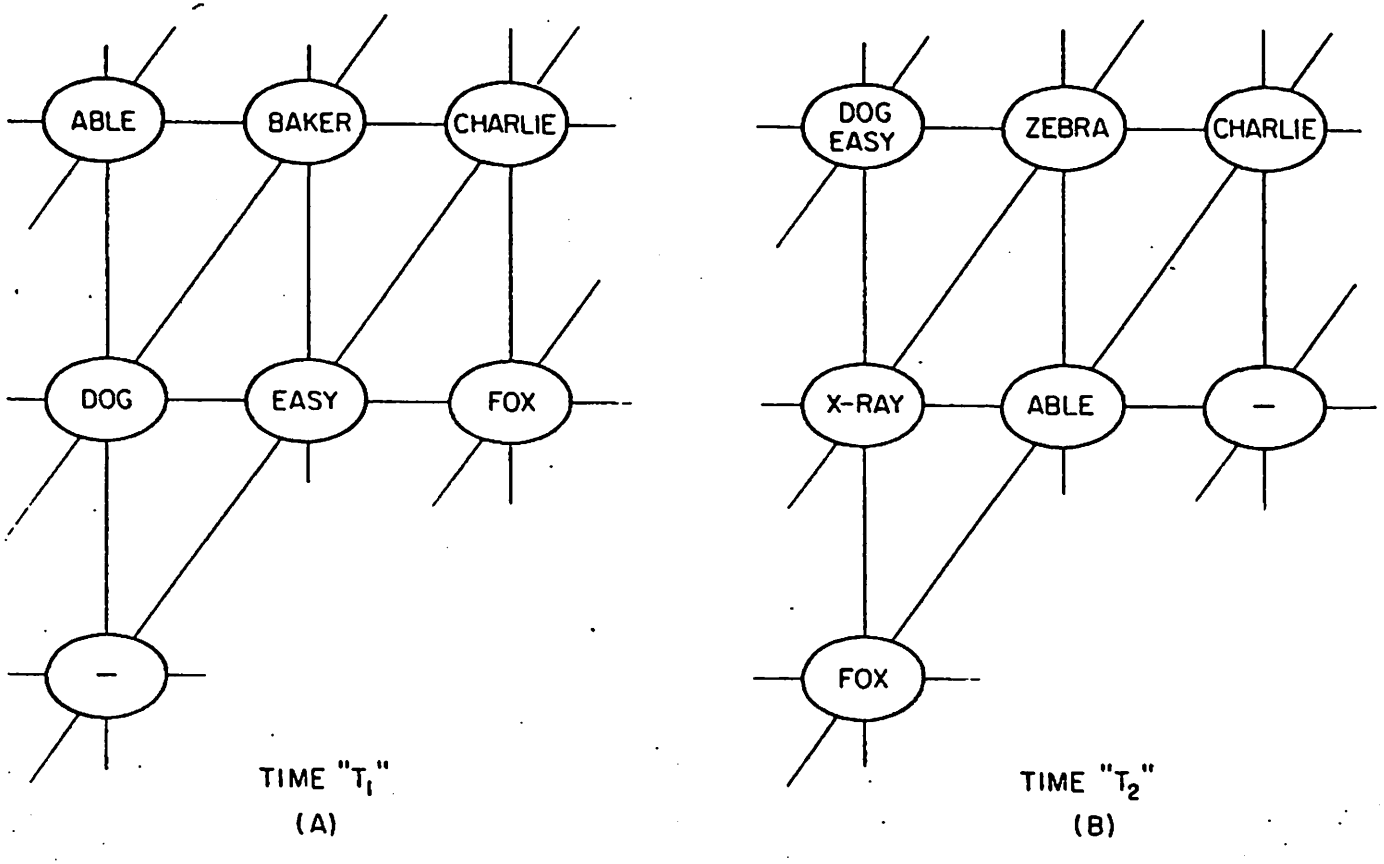



FIG. 12 – Adaptability to Change of User Location

most use of the least expensive links? The fundamentally simple adaptation technique can again be used. Instead of incrementing the handover by a fixed amount, each time a message is relayed, set the increment to correspond to link cost/bit of the transmission link. Thus, instead of the "instantaneously shortest non-busy path" criterion, the path taken will be that offering the cheapest transportation cost from user to user that is available. The technique can be further extended by placing priority and cost bounds in the message block itself, permitting certain users more of the communication resource during periods of heavy network use.

WHERE WE STAND TODAY

Although it is premature at this time to know all the problems involved in such a network and understand all costs, there are reasons to suspect that we may not wish to build future digital communication networks exactly the same way the nation has built its analog telephone plant.

There is an increasingly repeated statement made that one day we will require more capacity for data transmission than needed for voice. If this statement is correct, then it would appear prudent to broaden our planning consideration to include new concepts for future data network directions. Otherwise, we may stumble into being boxed in with the

uncomfortable restraints of communications links and switches originally designed for high quality analog transmission. New digital computer techniques using redundancy make cheap unreliable links potentially usable. Some sort of a switched network compatible with these links appears appropriate to meet this new upcoming demand for digital service.

Of course, we could use our existing circuit switching techniques. But, a system with greater capacity than the long lines of telephone plants might best be designed for such data transmission and survivability at the outset. Such a system should economically permit switching of very short blocks of data from a large number of users simultaneously with intermittent large volumes among a smaller set of points. Considering the size of the market there appears to be an incommensurately small amount of thinking about a national data plant designed primarily for data.

Is it time now to start thinking about a new and possibly non-existant public utility, a common user digital data communication plant designed specifically for the transmission of digital data among a large set of subscribers?

Is it time to consider the detailed format of a standard message block as a possible new data standard of the future?

DECLARATION OF SCOTT BRADNER

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

# Appendix H

**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-00662-TSE |

**OBJECTIONS AND RESPONSES BY DEFENDANTS NATIONAL SECURITY AGENCY AND ADM. MICHAEL S. ROGERS, DIRECTOR, TO PLAINTIFF'S FIRST AND SECOND SETS OF REQUESTS FOR ADMISSION**

Pursuant to Rule 36 of the Federal Rules of Civil Procedure and District of Maryland Local Rule 104, Defendants National Security Agency ("NSA") and Adm. Michael S. Rogers, Director of the NSA, in his official capacity (together, the "NSA Defendants"), by their undersigned attorneys, object and respond as follows to Plaintiff Wikimedia Foundation's first and second sets of Requests for Admission, dated November 7 and 29, 2017, respectively.

**GENERAL OBJECTIONS AND OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS**

1. The NSA Defendants object to Plaintiff's Requests for Admission to the extent, as set forth in response to specific requests below, that they are improper attempts to use requests for admission as discovery devices, specifically, as interrogatories.

2. The NSA Defendants object to Plaintiff's Requests for Admission to the extent, as set forth in response to specific requests below, that they seek information regarding the intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

3. The NSA Defendants object to Plaintiff's Requests for Admission to the extent, as set forth in response to specific requests below, they seek information that is irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

4. As set forth in response to specific requests below, the NSA Defendants object to the definition of the term "Circuit" as vague and ambiguous insofar as it is meant, by its reference to the use of that term 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" (the "PCLOB Section 702 Report") to assign the term "Circuit" a meaning other than its ordinary meaning in the telecommunications industry. The PCLOB is an independent agency within the Executive Branch, and the NSA Defendants do not have information regarding what, if anything, that entity intended by the term "Circuit" beyond the ordinary meaning of that term within the telecommunications industry as understood by the NSA Defendants.

5. As set forth in response to specific requests below, the NSA Defendants object to the definition of the term "Internet Transaction" as vague and ambiguous insofar as it is meant, by its reference to the use of that term in the PCLOB Section 702 Report, to assign the term "Internet Transaction" a meaning other than that understood by the NSA Defendants. The PCLOB is an independent agency within the Executive Branch, and the NSA Defendants do not have information regarding what, if anything, that entity intended by the term "Internet Transaction" beyond the meaning of that term as understood by the NSA Defendants.

6. As set forth in response to specific requests below, the NSA Defendants object to the definition of "Review" as compound, unduly burdensome and oppressive, and so vague and ambiguous as to render specific requests in which it is used incapable of reasoned response.

7. As set forth in response to specific requests below, the NSA Defendants object to the definition of "Interacted With" as compound, and, insofar as it incorporates the definition of "Review," also as unduly burdensome and oppressive, and so vague and ambiguous as to render specific requests in which it is used incapable of reasoned response.

8. As set forth in response to specific requests below, the NSA Defendants object to Plaintiff's Requests for Admission to the extent that they seek information that is protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

9. The following objections and responses are based upon information currently known to the NSA Defendants, and they reserve the right to supplement or amend their objections and responses should additional or different information become available.

10. Nothing contained in the following objections and responses shall be construed as a waiver of any applicable objection or privilege as to any request or as a waiver of any objection or privilege generally. Inadvertent disclosure or unauthorized disclosure of information subject to a claim of privilege shall not be deemed a waiver of such privilege.

**OBJECTIONS AND RESPONSES TO FIRST SET OF 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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 1 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 1 as unduly burdensome and oppressive insofar as it requests that the NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

**RESPONSE:** Subject to the objections stated above, and without waiving them, the NSA Defendants respond that it is difficult to determine the exact number of international submarine telecommunications cables that carry Internet communications directly into or out of the United States, because it is not publicly known whether particular cables carry Internet communications as opposed to telephonic or private-network communications. The Federal Communications Commission, which issues licenses to own and operate submarine cables and associated cable landing stations located in the United States, most recently reported that approximately 45 privately owned trans-ocean fiber optic cables (also referred to in the report as cable systems) landing in the United States or its territories were in service as of December 31, 2015. *See* Federal Communications Commission, International Bureau Report, 2015 U.S. International Circuit Capacity Data (August 2017), at 4 & Tables 4(A) & 4(B) at T-5 to T-8, available at https://apps.fcc.gov/edocs_public/attachmatch/DOC-346376A2.pdf. Telecommunications market research and consulting firm Telegeography publishes an online Submarine Cable Landing Directory, https://www.telegeography.com/telecom-resources/submarine-cable-landing-directory, which lists 45-50 privately owned international undersea cable systems landing in the United States or its territories, many of which, however, contain multiple cables or legs. Telegeography also publishes online a map purporting to depict the international submarine cables connecting the United States with other nations as of December 11, 2017, available at https://www.submarinecablemap.com.

The NSA Defendants respond further that, according to data available from Telegeography, international submarine cables typically contain 2-8 pairs of fiber-optic cables. Each fiber-optic pair is typically capable of carrying between approximately 15 and 120 individual communications circuits on different light wavelengths, depending on age and technology used. As a result, an individual submarine cable may carry between approximately

30 and 960 communications circuits. (Individual circuits may be subdivided further to create multiple "virtual circuits" through application of various technologies.) Each wavelength carried on a fiber-optic pair is typically capable of transporting between 10 and 100 gigabits of data per second (10-100 Gbps), meaning that a typical submarine cable can carry between approximately 300 and 96,000 Gbps of data.

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 2 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 2 as unduly burdensome and oppressive insofar as it requests that NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

**RESPONSE:** Subject to the objections stated above, and without waiving them, the NSA Defendants respond that, as noted in response to Request for Admission No. 1, above, it is not publicly known whether particular international submarine telecommunications cables carry Internet communications as opposed to telephonic or private-network communications, and it is therefore difficult as well to determine the exact number of points at which the cables carrying Internet communications make landfall within the United States. Telegeography's online Submarine Cable Landing Directory, https://www.telegeography.com/telecom-resources/submarine-cable-landing-directory, indicates that international undersea cable systems currently in service make landfall within the territory of the United States at approximately 75-80 locations.

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 3 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 3 as unduly burdensome and oppressive insofar as it requests that NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

**RESPONSE:** Subject to the objections stated above, and without waiving them, the NSA Defendants respond that yes, the Internet backbone includes but is not limited to international submarine telecommunications cables that carry Internet communications.

**REQUEST FOR ADMISSION NO. 4:** Admit that the INTERNET BACKBONE includes high-capacity terrestrial cables that carry traffic within the UNITED STATES.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 4 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 4 as unduly burdensome and oppressive insofar as it requests that NSA Defendants produce information regarding the telecommunications infrastructure that is equally available to the Plaintiff as it is to the NSA Defendants from public sources.

**RESPONSE:** Subject to the objections stated above, and without waiving them, the NSA Defendants respond that yes, the Internet backbone includes but is not limited to high-capacity terrestrial telecommunications cables that carry Internet communications 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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 5 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 5 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 6 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 6 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants also object to Request for Admission No. 6 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

**RESPONSE:** Subject to the objections stated above, and without waiving them, the NSA Defendants respond that in the course of the Upstream Internet collection process, certain

Internet transactions transiting the Internet backbone networks of certain electronic communication service providers are filtered for the purpose of excluding wholly domestic communications; are then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures; and must pass through both the filter and the screen before they can be ingested into Government databases.

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 7 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 7 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 8 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 8 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants also object to Request for Admission No. 8 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

**RESPONSE:** Subject to the objections stated above, and without waiving them, the NSA Defendants respond that in the course of the Upstream Internet collection process, certain Internet transactions transiting the Internet backbone networks of certain electronic communication service providers are filtered for the purpose of excluding wholly domestic communications; are then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures; and must pass through both the filter and the screen before they can be ingested into Government databases.

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 9 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 9 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. §3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 10 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 10 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants also object to Request for Admission No. 10 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

**RESPONSE:** Subject to the objections stated above, and without waiving them, the NSA Defendants respond that in the course of the Upstream Internet collection process, certain Internet transactions transiting the Internet backbone networks of certain electronic communication service providers are filtered for the purpose of excluding wholly domestic communications; are then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures; and must pass through both the filter and the screen before they can be ingested into Government databases.

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 11 as an improper attempt to use a request for admission as a discovery device, specifically, as an

interrogatory. The NSA Defendants also object to Request for Admission No. 11 because what the NSA "consider[s]" the collection of an Internet communication to be, within the meaning of the 2014 NSA Section 702 Minimization Procedures or otherwise, is irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

The NSA Defendants also object to Request for Admission No. 11 to the extent that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1). Finally, the NSA Defendants object to Request for Admission No. 11 insofar as the definition of "Reviews," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

**RESPONSE:** Subject to the objections stated above, and without waiving them, the NSA Defendants respond that the NSA considers the term "collection" as it applies to the Upstream Internet collection process, whether in the 2014 NSA Section 702 Minimization Procedures or otherwise, to be the ingestion of Internet transactions into Government databases after they have been filtered for the purpose of excluding wholly domestic communications, and then screened to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures.

**REQUEST FOR ADMISSION NO. 12:** Admit that, in the course of Upstream surveillance, the NSA RETAINS WHOLLY DOMESTIC COMMUNICATIONS.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 12 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 12 because it

seeks information that is irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

**RESPONSE:** Subject to the objections stated above, and without waiving them, the NSA Defendants admit that, as found by the Privacy and Civil Liberties Oversight Board, technical measures taken to prevent acquisition of wholly domestic communications in the Upstream Internet collection process do not operate perfectly. However, the current NSA Section 702 Minimization Procedures require that wholly domestic communications "be promptly destroyed upon recognition," subject to limited exceptions described in Section 5 therein.

**REQUEST FOR ADMISSION NO. 13:** Admit that the NSA conducts Upstream surveillance on multiple INTERNET BACKBONE CIRCUITS.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 13 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants further object to Request for Admission No. 13 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

**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).

**OBJECTION:** The NSA Defendants object to Request for Admission No. 14 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants also object to Request for Admission No. 14 on the ground

that it attributes the phrase "international Internet link" to a Government document when in fact the phrase is taken from an opinion of the Foreign Intelligence Surveillance Court that does not purport to quote directly from the referenced Government document. *See* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011). Whether the phrase "international Internet link" is contained within the referenced Government document is information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. §3605(a).

The NSA Defendants further object to Request for Admission No. 14 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

**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).

**OBJECTION:** The NSA Defendants object to Request for Admission No. 15 as an improper attempt to use a request for admission as a discovery device, specifically, as an interrogatory. The NSA Defendants also object to Request for Admission No. 15 as vague and ambiguous insofar as it does not specify where or in what context the NSA Defendants allegedly use the term "chokepoints" or "choke points." To the extent that Plaintiff's reference to that term alludes to what is described in the Amended Complaint as an "NSA slide," *see* Am. Compl. ¶ 68, the NSA Defendants object to this request as implicitly seeking information (which can be neither confirmed nor denied) regarding the authenticity of the purported slide, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

The NSA Defendants further object to Request for Admission No. 15 on the grounds that it seeks information (which can be neither confirmed nor denied) regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a), and which is also protected from disclosure by the state secrets privilege, and the statutory privilege under 50 U.S.C. § 3024(i)(1).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 16 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit A "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit A as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 16 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 17 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit A as evidence of intelligence activities allegedly conducted by the NSA, on the grounds that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 18 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit A as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 19 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit B "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit B as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 19 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 20 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit B as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected

from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 21 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit B as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 22 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit C "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit C as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 22 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 23 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in

Exhibit C as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 24 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit C as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 25 as irrelevant, and as vague and ambiguous insofar as it does not specify what kind of document Plaintiff claims Exhibit D "genuine[ly]" to be. To the extent that Plaintiff seeks to establish the authenticity of Exhibit D as evidence of intelligence activities allegedly conducted by the NSA, Defendants also object to Request for Admission No. 25 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 26 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit D as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 27 as irrelevant, and, to the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit D as evidence of intelligence activities allegedly conducted by the NSA, on the ground that this request seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** To the extent that Plaintiff seeks to establish the authenticity of Exhibit E as evidence of targeting procedures allegedly used by the NSA in 2009, the NSA Defendants object to Request for Admission No. 28 (i) as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case, *see*

October 3, 2017, Order, ECF No. 117 at 1, (ii) as irrelevant, in particular, to Plaintiff's standing to seek prospective relief, and (iii) on the ground that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** To the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit E as evidence of intelligence activities allegedly conducted by the NSA in 2009, the NSA Defendants object to Request for Admission No. 29 as irrelevant and on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** To the extent Plaintiff seeks to establish the admissibility of statements made in Exhibit E as evidence of intelligence activities allegedly conducted by the NSA in 2009, the NSA Defendants object to Request for Admission No. 30 as irrelevant and on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(1) and 50 U.S.C. § 3605(a).

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 31 as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

**RESPONSE:** Subject to the objection stated above, and without waiving it, the NSA Defendants admit that Exhibit 1 hereto is a true and correct (public) copy of the "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.

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 32 as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

**RESPONSE:** Denied. The 2014 NSA Section 702 Minimization Procedures, Exhibit 1 hereto, were adopted by the Attorney General of the United States, in consultation with the Director of National Intelligence, as attested by the Attorney General's signature thereto.

**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.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 33 as irrelevant to jurisdictional issues, which are the only matters as to which the Court has authorized discovery in this case. *See* October 3, 2017, Order, ECF No. 117 at 1.

**RESPONSE:** Denied. The 2014 NSA Section 702 Minimization Procedures, Exhibit 1 hereto, were adopted by the Attorney General of the United States, in consultation with the Director of National Intelligence, as attested by the Attorney General's signature thereto.

**OBJECTIONS AND RESPONSES TO SECOND SET OF REQUESTS FOR ADMISSION**

**REQUEST FOR ADMISSION NO. 34:** Admit that, in conducting Upstream surveillance, the NSA has COPIED at least one WIKIMEDIA INTERNET COMMUNICATION.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 34 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1). The NSA Defendants further object to Request for Admission No. 34 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

**REQUEST FOR ADMISSION NO. 35:** Admit that, in conducting Upstream surveillance, the NSA has REVIEWED the content of at least one WIKIMEDIA INTERNET COMMUNICATION.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 35 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1). The NSA Defendants further object to Request for Admission No. 35 on the

grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

The NSA Defendants also object to Request for Admission No. 35 insofar as the definition of "Review[ed]," by encompassing so many fundamentally different actions, renders this request compound, unduly burdensome and oppressive, vague and ambiguous, and incapable of reasoned response.

**REQUEST FOR ADMISSION NO. 36:** Admit that, in conducting Upstream surveillance, the NSA has RETAINED at least one WIKIMEDIA INTERNET COMMUNICATION.

**OBJECTION:** The NSA Defendants object to Request for Admission No. 36 on the grounds that it seeks information (which can be neither confirmed nor denied) that is protected from disclosure by the state secrets privilege and the statutory privilege under 50 U.S.C. § 3024(i)(1). The NSA Defendants further object to Request for Admission No. 36 on the grounds that it seeks information regarding alleged intelligence activities of the NSA, which is absolutely protected from disclosure by 50 U.S.C. § 3605(a).

Dated: January 8, 2018

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
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
Email: james.gilligan@usdoj.gov

*Counsel for the NSA Defendants*

# EXHIBIT 1

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2014 JUL 29 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

DECLARATION OF SCOTT BRADNER

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

# Appendix I

# What do parrots and BGP routers have in common?

David Hauweele*, Bruno Quoitin
University of Mons (UMONS)
{first.last}@umons.ac.be

Cristel Pelsser†
University of Strasbourg
pelsser@unistra.fr

Randy Bush
Internet Initiative Japan (IIJ)
randy@psg.com

## ABSTRACT

The Border Gateway Protocol propagates routing information accross the Internet in an incremental manner. It only advertises to its peers changes in routing. However, as early as 1998, observations have been made of BGP announcing the same route multiple times, causing router CPU load, memory usage and convergence time higher than expected.

In this paper, by performing controlled experiments, we pinpoint multiple causes of duplicates, ranging from the lack of full RIB-Outs to the discrete processing of update messages. To mitigate these duplicates, we insert a cache at the output of the routers. We test it on public BGP traces and discuss the relation of the cache performance with the existence of bursts of updates in the trace.

## 1. INTRODUCTION

The Border Gateway Protocol [1] (BGP) is the de facto standard used to exchange inter-AS routing information on the Internet. Its correct and scalable behavior is critical to the operation of the Internet. One of the keys to BGP scalability is the use of *incremental routing updates*: only changes in destination prefix reachability are advertised. These changes include the reachability of a new prefix, the unreachability of an existing destination (withdrawal), or a modification of the path attributes associated with a destination. Path attributes are involved in routing decisions and also ensure proper protocol behavior such as avoiding routing loops. According to the protocol specification, a BGP speaker should not issue an update containing the same BGP information as was most recently advertised for the prefix.

Anomalous BGP behavior has been observed as early as 1998 [2]. Based on a 9 months trace of the BGP traffic exchanged between backbone networks, Labovitz et al. showed lack of aggregation and high routing instability with up to 99% of exchanged routing information not being related to topological changes. In particular, they observed the occurrence of redundant BGP update messages that they called *duplicate updates*. At that time, most of the duplicates where due to bogus stateless BGP implementations. The authors noted that the observed high level of instability was detrimental to the operations of the Internet, causing high router CPU load, making routers unresponsive and in the worst cases leading to packet or routing information losses. In addition, they may sometimes trigger unreachability when interacting with route flap damping [3].

Several studies later revisited BGP dynamics [4–8] and its impact on router CPU load [9], some focused on BGP duplicates. Although the number of pathological updates declined over time, duplicates still constitute a significant part of the BGP traffic with up to 15% of the updates observed at RIPE monitors in 2006 [5]. It was later shown that the duplicate problem is even worse for routers in the core of the Internet with the portion of duplicates varying from 7% to 60% in 2008 [7]. More recently, in 2009, Park et al. [6] studied over 90 RouteViews/RIPE monitors and showed that the duplicates make up 13.5% of the aggregated BGP traffic. Routers can receive up to 86.4% of duplicates during their busiest time. These previous works show that duplicates are a continuing problem. We confirm this observation by looking at all sessions from EQUINIX, ISC, LINX and WIDE RouteViews collectors from 2009 to 2014. 48.5% of the traces we observed had more than 10% of duplicates. The traces also display a high variability with an average of $(18.84 \pm 22.31)\%$ duplicates. Finally, [6] hinted that a change in attributes attached to iBGP routes may trigger eBGP duplicates. To the best of our knowledge, so far, no thorough study has explained their origin or tried to mitigate the problem.

In this paper, we make the following contributions:

- We discuss in Section 2 the causes of today's duplicates. Although the majority of duplicates in 1998 were bogus route withdrawals, this is not the case today (less than 0.5% on almost all traces). To understand what causes duplicates, we inject carefully crafted BGP updates into a router and we correlate the input and output BGP traffic. Based on this, we identify different causes for duplicates. Most duplicates today are due to implementions trading off between memory footprint and statefulness.

- In Section 3, we devise a caching mechanism that mitigates duplicates. The benefit of using a cache is that the amount of memory used can be controlled. We evaluate the efficiency of our caching mechanism on several real world BGP traces, using several replacement strategies. We show that our cache significantly reduces duplicates for prefixes in the default free zone even with a small cache size.

## 2. THE ORIGIN OF DUPLICATES

To investigate the origin of BGP duplicates, we follow two different approaches. First we look at a router that receives live BGP feeds. We capture all the BGP traffic and we man-

*David started this work during his internship at IIJ.

†The credits go to IIJ for supporting Cristel's work.

ually correlate duplicates observed in the outbound traffic with messages in the inbound traffic. This is an approach similar to that used by Park et al. in [6] that gives us some initial insight on potential causes for duplicates.

Second, we perform a fully controlled experiment where we inject crafted sequences of messages into a test router. We then look for duplicates in the output messages. Our experiment allows to confirm the hypotheses of Park et al. on the origin of duplicates. We also go much further as we establish three additional causes for duplicates.

This section explains our methodology and subsequent observations.

## 2.1 Definitions

We define a duplicate as a *redundant* prefix advertisement with the *same attributes* as the most recent update for this prefix on the same session and not interleaved with a withdrawal or a session reset. This definition is stricter than the one in [2] where an update is considered a duplicate (AADup) if its AS-Path and Next-Hop do not change. When we count duplicates, we include the initial duplicated route advertisement.

We also define the *ratio of duplicates* as the number of duplicates (including the original messages) over the total number of messages. With this definition, a trace where every advertisement is duplicated will have a ratio of 100%.

## 2.2 Real BGP feed experiment

The objective of this experiment is to manually investigate some occurrences of duplicates by correlating the duplicates observed at the output of a router with the messages it receives. Our setup is shown in Fig. 1. Devices $r0$, $r1$ (Cisco) and $r2$ (Juniper) are real routers while *mon*0 is a dedicated host running a software BGP router (Quagga).

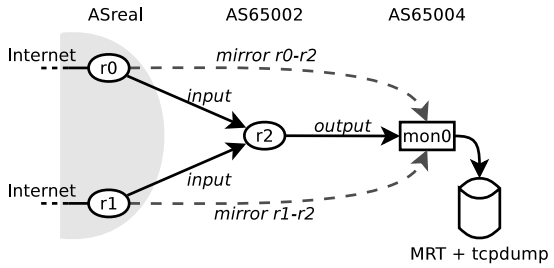


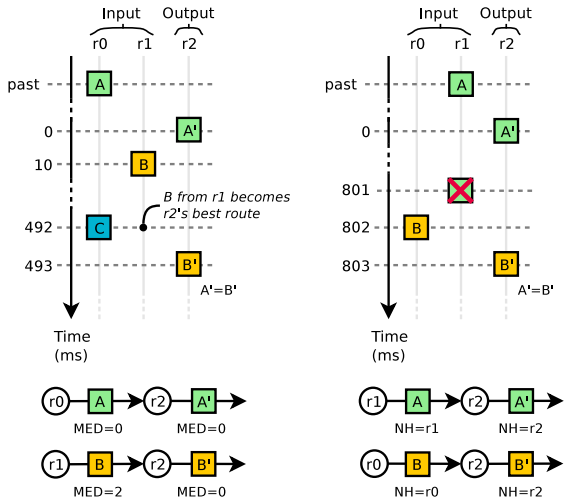

Figure 1: Setup for the I/O correlation.

The router under test is $r2$. It receives BGP messages from $r0$ and $r1$ through *input* eBGP sessions. After selecting its best routes, $r2$ sends BGP messages over a single *output* eBGP session to *mon*0. The routes learned by $r0$ and $r1$ are from real BGP feeds received in September 2013 for a duration of 23 days.

The *mon*0 host captures all the BGP messages received on the *mirror* and *output* sessions. The *mirror* sessions (dashed lines on Fig. 1) allow to capture the *input* routes advertised by the upstream routers $r0$ and $r1$. To reduce timing differences between the *input* and *mirror* sessions, both sessions are placed in the same update group on $r0$ and $r1$. The *Minimum Route Advertisement Interval* (MRAI) is also set to zero on these routers.

The messages are stored in MRT format. MRT records route advertisements, route changes and route withdrawals. Each record contains a timestamp and the path attributes. TCP-level traces of all the BGP messages received are also captured. This allows us to validate the MRT capture and dwelve deeper in the BGP message packet details e.g. to check the ordering of attributes.

We describe in the following paragraphs two common cases we observed. The first case involves the Multi-Exit-Discriminator (MED) attribute while the second case involves a rewritten Next-Hop. We do not know the exact frequency of these cases, as we have to manually extract the data.




(a) MED case (b) Next-Hop case

Figure 2: Common causes of duplicates. Timeline of the updates seen at the output of each router.

In the MED case, illustrated in Fig. 2a, we believe the duplicate is caused by a MED attribute stripped at the output of $r2$. Three different *input* routes are involved, all for the same IPv4 prefix. The first route, $A$, has an AS-Path of length 5 and a MED value of 0. The second route, $B$, has the same AS Path as $A$ but a MED value of 2. The third route, $C$, has an AS Path of length 6 and a MED value of 0. At time 0ms, $r2$ announces route $A$ learned from $r0$. Before announcing $A$, $r2$ updates the AS-Path and strips the MED, which produces route $A'$. At time 10ms, $r1$ announces route $B$ to $r2$. The decision process of $r2$ ranks route $A$ better than route $B$, causing no change in $r2$'s best route. At time 492ms, $r0$ announces to $r2$ route $C$ which has a longer AS-Path. Route $C$ implicitly withdraws route $A$. As a consequence, $r2$ now selects route $B$ as best. Before announcing $B$, $r2$ strips the MED value, producing $B'$. *Output* routes $A'$ and $B'$ are equal, hence $B'$ is a duplicate of $A'$.

In the case illustrated in Fig. 2b, we believe the duplicate is caused by the next-hop attribute. This case involves two routes. Route $A$ announced first by router $r1$, is selected as best by $r2$ and announced on the *output* session at time 0ms. Before announcing route $A$, $r2$ rewrites the next-hop and emits route $A'$. At time 801ms, router $r1$ explicitly withdraws route $A$. At time 802ms, router $r0$ announces route $B$ although it does not trigger any change in $r2$ yet. Finally, at time 803ms, router $r2$ selects route $B$ as best. Before announcing route $B$, $r2$ rewrites the next-hop value with its own IP address, leading to route $B'$. Routes $A$ and $B$ only differ by their next-hop (resp. $r1$ and $r0$), hence routes $A'$ and $B'$ are identical.

## 2.3 Controlled experiment

To confirm the hypotheses of the previous section, we perform the same input/output matching in a fully controlled experiment. We systematically test a large set of situations that may not have appeared in the setting with a real, live BGP feed. We are able to find additional causes of duplicates and pinpoint more precisely the reasons behind these duplicates.

The setup depicted in Fig. 3 is similar to the previous experiment except we use a machine *inj*0, running Linux, to inject crafted updates to the router under test, $r0$, and another to capture its *output*. Router $r0$ is a Cisco 7200 running IOS v15.3. On *inj*0, we use ExaBGP [10] to inject synthetic updates. The monitoring host *mon*0 collects the routes observed on the *output* and *mirror* sessions with a Quagga BGP daemon and with tcpdump. The *mirror* session is used to validate *inj*0's program. We check the ability of this program to send BGP messages accurately. We measure that the minimum interval between two consecutive updates sent by ExaBGP is 1ms.

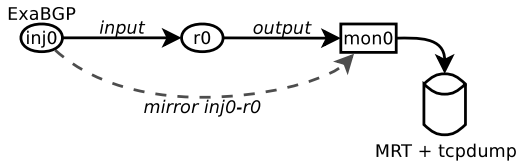



Figure 3: Setup for the injection.

Table 1 summarizes the results of the injection experiment. Due to space limitations, only results for a small number of test cases are presented. For each experiment, the first column shows the average delay between messages observed on the *input* and its standard deviation. Second column shows the same information for the *output*. The last column shows the ratio of duplicates. That is, the number of duplicates including the initial update over the number of updates (see Section 2.1).

| Test case | Input (ms) | Output (ms) | Dup. |
|---|---|---|---|
| `NotVisible` | – | – | 100% |
| `RFlap` (1 ms) | $1.23 \pm 0.50$ | $3.47 \pm 3.46$ | 69.0% |
| `RFlap` (2 ms) | $2.07 \pm 0.39$ | $2.84 \pm 0.99$ | 25.9% |
| `RFlap` (3 ms) | $3.07 \pm 0.44$ | $3.06 \pm 0.48$ | 0.1% |
| `AFlap` (1 ms) | $1.22 \pm 0.69$ | $3.74 \pm 17.25$ | 95.1% |
| `AFlap` (2 ms) | $2.07 \pm 0.36$ | $2.07 \pm 0.10$ | 4.7% |
| `AFlap` (3 ms) | $3.07 \pm 0.44$ | $3.06 \pm 0.09$ | 0.1% |

Table 1: Results of selected injection test cases.

### 2.3.1 *Internal / non-transitive / filtered attributes*

This first set of experiments (`NotVisible`) considers the case of attributes whose changes should not be visible from the outside of an AS as they are either internal, non-transitive or filtered/rewritten by output policies. The objective of these experiments is to test whether or not such attributes could cause duplicate routes to be sent by the router.

For this purpose, we repeatedly send a sequence of 2 route updates $(A, B)$ for the same destination prefix. Route $B$ differs from route $A$ for only a specific internal / non-transitive / filtered attribute. The expected behavior is as follows. When route $A$ is received, it is selected as best as there is no other choice. It is then propagated on the output session. When route $B$ is received, it replaces route $A$ (implicit withdraw). Route $B$ should not be propagated to the *output* session as it differs from route $A$ only by an attribute that is either internal, non-transitive, or removed by a filter. Hence, on the *output* session, routes $A$ and $B$ are identical.

We observe a duplicate ratio of 100% for experiments in this class, as shown in Table 1 for the `NotVisible` test case. The router was not able to detect that the second route was a duplicate of the previous. We explain this behavior on the statelessness of the BGP implementation.

These results held for the following attributes: MED, Local Pref, Cluster List, and Originator ID. We also observed a 100% duplicates ratio for non-transitive Community values, for Community values stripped by outgoing policies and for rewritten Next-Hop (as already observed in Section 2.2).

### 2.3.2 *Fast flapping route*

In a second set of experiments (`RFlap`) we investigate the impact of a flapping route on the generation of duplicates. The experiment relies on the repetition of a simple sequence of 2 BGP updates $(A, W)$ for the same prefix. $A$ announces a route while $W$ withdraws it.

The objective of this experiment is to trigger duplicates by forcing a route to change multiple times before the router has the opportunity to propagate it. To understand this behavior, we need to refine our model of how a router generates updates. When a route towards a prefix changes, the main BGP process does not send an update immediately. Instead, this task is delegated to a separate thread that periodically reads the RIB and advertises the routes marked as changed.

The following scenario illustrates how the transmission of a duplicate update can be caused. When the first Announce is received, the route is marked as changed in the RIB. The RIB is then scanned and an update is sent. Then, the Withdraw is received and the route is again marked as changed. However, before the RIB is scanned, the third message (second Announce) is received and the route is again marked as changed. When the RIB is scanned, the second Announce, identical to the first one is sent. It is a duplicate as the router did not have time to send a Withdraw between the two Announces.

We repeat this experiment with increasing delay between updates: 1ms, 2ms and 3ms. The results are in Table 1 for test case `RFlap`. We observe that with a 1ms interval, almost 70% of output updates are duplicates. When the interval between input updates increases, the ratio of duplicates decreases. With a 2ms interval, the ratio is almost 26% and at 3ms, there are almost no duplicates.

We also tested the impact of the MRAI on the generation of duplicates. We conducted the same experiment with a larger interval of 2 seconds and a MRAI set to 6 seconds. With this experiment we still generated more than 30% of duplicates.

### 2.3.3 *Flapping attribute*

This third set of experiments (`AFlap`) looks at flapping attributes. The principle is identical to the *RFlap* experiment except that the second message is not a withdraw but an update with a transitive attribute that flaps from one value to another and back. As an example, we present the results for routes where the origin AS in the AS-Path has value $x$ in the first and third updates and has value $y \neq x$ in the sec-

ond update. We see in Table 1 for the `AFlap` test cases that the ratio of duplicates decreases with an increasing interval between the *input* BGP messages.

The explanation for these results is analogous to the *RFlap* experiment. When the interval between messages is small, the router marks the route as changed after the second message, but the third message, reversing the second update, is received before the second message is propagated downstream.

## 3. MITIGATING DUPLICATES

In Section 2, we found several causes explaining the generation of duplicates. According to the BGP specification, such duplicates should not appear. When a router advertises a route for a given prefix, it should store this route in the RIB-Out associated with the peer. When it later advertises a route for the same prefix, it looks at the current entry in the RIB-Out. If the current entry is the same as the new advertisement, the router does not send it because it would be a duplicate update.

We found out that although most router implementations support a RIB-Out, the implementation might be partial or operators might disable it to spare memory, especially on older hardware. Some vendors [11] explicitly recommend to disable the RIB-Out when the router has a large number of peers.

For this reason, we need to devise a solution that is not a full RIB-out but that still significantly reduces the number of BGP duplicates. This new mechanism must come at a lower cost than a RIB-Out in terms of memory consumption.

To obtain a baseline on the possible load reduction, we count the legitimate updates after filtering all duplicates. We compare this count to the number of updates in the original trace. We use a BGP trace obtained from the Equinix RouteViews collector and focus on the session with peer AS5769 (EQUIX-1). Fig. 4 shows two 12 hours excerpts of this session starting on 2013-9-17 at 0:00 (left) and 2013-9-18 at 4:00 (right). The Figure shows the total amount of updates received during the last hour (dark gray) and the same information after all duplicates have been filtered (light gray). On the left the trace has a relatively low rate of duplicates. We observe an average of 5,188 duplicates per hour. By filtering all duplicates, the number of updates on this period is reduced by an average factor of 1.62. On the right the trace features two large spikes of updates. On the largest spike, we count $5.46 * 10^5$ duplicates. By filtering all duplicates, the number of updates in this spike is reduced by a factor of 5.08.

We observe that a significant reduction in BGP traffic can be achieved by filtering duplicate updates. If CPU usage is proportional to the number of updates, sizable improvement in performance can be expected by getting rid of duplicates especially on small routers with limited CPU.

### 3.1 Caching router

Instead of a RIB-Out, we propose a small cache at the output of the router which can significantly reduce the number of duplicates at a far less memory cost. The advantage of this solution is that it can easily be added to the output of a router with little modifications of the BGP implementation.

A cache at the output of the router works similarly to a RIB-Out but using less memory. When a cache reaches its maximum capacity, it must remove one of its entries to add

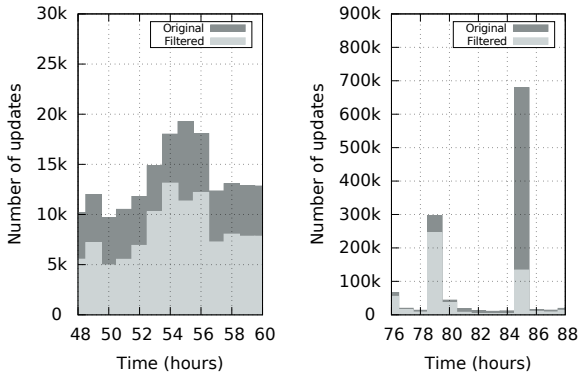



Figure 4: Two excerpts of the EQUIX-1 trace. Low rate of duplicates on the left. Spikes of duplicates on the right. We compare the original trace to the same trace with all duplicates filtered.

| Name | Eviction strategy |
|---|---|
| `lru` / `mru` | Least/most recently queried entry. |
| `lrh` / `mrh` | Least/most recently hit entry. |
| `lfu` / `mfu` | Least/most frequently queried entry. |
| `lfh` / `mfh` | Least/most frequently hit entry. |
| `random` | Random entry. |

Table 2: Eviction strategies

a new prefix. There are multiple ways to choose which prefix to remove when the cache is full. These selection methods are called *eviction strategies*. A cache is defined by its size and its eviction strategy.

In our case, the cache can be viewed as an Abstract Data Type (ADT) with the following operations: `query`, `remove` and `clear`. The `query` operation tells if an entry for a given key and value exists. If the given value is different from the entry in the cache, the entry is updated. If the cache does not contain an entry for this key, it adds this new entry to the cache. When the size reaches the cache limit, the cache eviction strategy comes into play. An entry is removed before the addition of the new entry to the cache. These two cases are considered *miss* queries. Instead, if the cache contains an entry for this key with the same value, the query is considered a *hit*.

The `remove` operation takes a key and if it exists, removes the associated entry from the cache. The `clear` operation removes all entries from the cache.

When the router advertises a given prefix and set of attributes, it queries the cache with the prefix as the key and the set of attributes as the value. In the case of a hit, the advertisement is a duplicate caught by the cache, and the router inhibits the advertisement. In the case of a miss, an advertisement is sent to the peer. When the router withdraws a given prefix, it removes the cache entry with the prefix as key and sends the withdraw to the peer. Finally when the router opens or reopens a session, the cache content is cleared and the router sends an open message to the peer.

### 3.2 Evaluation methodology

We assess the performance of the cache with the different eviction strategies listed in Table 2. The `random` cache

uses a pseudo random number generator to select an entry to remove. We use this strategy as a baseline to determine if other strategies are able to exploit characteristics of the input trace or if there is no specific pattern to exploit. Any such strategy should perform better in average than the random strategy.

In order to test the performance of the cache, we replay through the cache a previously captured trace. The cache then filters the duplicates. Since time does not matter for the eviction strategy, the cache can replay the trace without taking into account the elapsed time between each message. As a result it is possible to simulate the behavior of the cache on a captured trace much more rapidly than playing it directly on a router.

We use the Minimum Collection Time [12] (MCT) algorithm to accurately identify the start and duration of the routing table transfers in the BGP trace. We add an implicit OPEN message at the beginning of each detected table transfer so that updates within the table transfer do not count as duplicates.

## 3.3 Dataset

We measured the updates rate and duplicates ratio of several sessions at the RouteViews collectors from 2009 to 2014. We observed that the duplicate ratio was higher than 10% on 48.5% of the traces. The quantity of updates and duplicates also varies greatly from one session to another. The average rate of updates and duplicates per week across all traces observed in 2014 is of $(3.6 \pm 10.8)$ millions updates and $(1.0 \pm 3.7)$ millions duplicates respectively.

In order to take this variability into account, we apply the cache on three different sessions obtained from RouteViews collectors during one week period. We choose these three sessions as they contain a significant number of updates ($> 1$ million/week) but exhibit 3 extreme behaviours for what concerns the duplicates. Fig. 5 shows the hourly number of duplicates over time for these three traces.

| | EQUIX-1 | EQUIX-2 | WIDE |
|---|---|---|---|
| **Peer ASN** | 5769 | 2914 | 7500 |
| **Start** | 2013-09-15 | 2014-10-15 | 2013-09-15 |
| **End** | 2013-09-22 | 2014-10-22 | 2013-09-22 |
| **Updates** | $4.5 * 10^6$ | $1.55 * 10^7$ | $1.2 * 10^6$ |
| **Duplicates** | 59.38% | 98.36% | 2.17% |
| **Spikes** | Large | No | Small |

Table 3: Characteristics of three different traces.

Table 3 summarizes the characteristics of the traces. The number of updates and the ratio of duplicates observed vary greatly from one trace to another. The first trace, EQUIX-1, exhibits a large number of updates ($4.5{*}10^6$) and a high ratio of duplicates (59.38%), a large fraction of which (41%) visible as two large spikes of duplicates. In comparison EQUIX-2 has a higher number of updates ($1.55 * 10^7$) and a higher ratio of duplicates (98.36%) but displays no major spike. Finally the WIDE trace has a very low ratio of duplicates ($1.2 * 10^6$) and does not contain any large spike.

## 3.4 Results

We apply the cache on the WIDE and EQUIX-1 traces presented in Section 3.3. We also apply the cache on the third trace, EQUIX-2 with a fixed size of 65k entries and

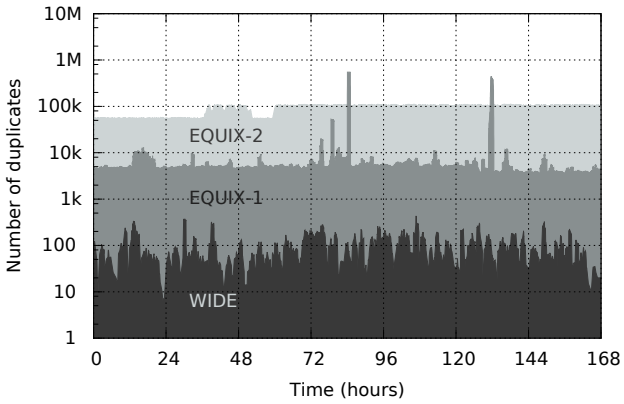



Figure 5: Three traces with different duplicates ratio. Each point shows the number of duplicates seen during the last hour.

| Cache | WIDE 32k | WIDE 65k | EQUIX-1 32k | EQUIX-1 65k |
|---|---|---|---|---|
| No cache | 2.172% | | 59.38% | |
| `lfh` | 1.351% | 0.885% | 49.14% | 45.50% |
| `lfu` | 1.324% | 0.818% | 49.09% | 45.45% |
| `lrh` | 0.040% | **0.009%** | 42.91% | 42.27% |
| `lru` | **0.039%** | 0.016% | **42.90%** | 42.25% |
| `mfh` | 1.556% | 1.121% | 53.85% | 50.30% |
| `mfu` | 0.830% | 0.173% | 52.97% | 48.17% |
| `mrh` | 1.555% | 1.078% | 53.34% | 49.68% |
| `mfu` | 1.518% | 1.014% | 52.93% | 49.04% |
| `random` | 0.042% | 0.020% | 42.98% | **41.87%** |

Table 4: Percentage of duplicates at the output of the EQUIX-1 and WIDE traces for different cache eviction strategies and sizes expressed in number of different routes.

the `lru` strategy. These traces were captured at different locations and time. They show different behaviours against which we test our solution.

Table 4 summarizes the percentage of duplicates found at the output of the WIDE and EQUIX-1 traces for two cache sizes, 32768 (32k) and 65536 (65k) different routes, and multiple strategies. The first line gives the duplicate ratio of the original trace (no cache applied). For the WIDE trace, the `lru` and `lrh` eviction strategies provide the best results. The best cache, `lrh`, reduces the original duplicate ratio by a factor 241. Further, the larger cache provides better results. In the case of the WIDE trace, the `lru` cache is 2.44 times as effective in filtering the duplicates with a cache that is twice as large.

On the EQUIX-1 trace, the cache performs poorly. With a 32k cache, the best results are achieved with the `lru` strategy. However, the output duplicate ratio remains high, at 42.9%. Doubling the cache size does not provide as much benefit as with the WIDE trace. Moreover, a striking result is that in the case of the large cache, the `random` eviction performs better than the other techniques. This indicates that the eviction strategies are not able to properly exploit the characteristics of the trace.

These results suggest that a higher duplicate ratio inhibits the performance of the cache. However, when we apply the `lru` cache of 65k on the EQUIX-2 trace, which exhibits a

higher duplicates ratio than EQUIX-1, the duplicate ratio drops from 98.36% to 5.83%. This reduces the number of updates for the trace by a factor of 50.

This shows that a cache is able to filter a session with a very high number of duplicates. I.e., the performance does not depend on the number of duplicates but rather on other characteristics of the trace. Actually, it depends on the number of distinct prefixes at the origin of those duplicates. During the EQUIX-2 trace this number stays at an average of 1000 prefixes per hour. During the EQUIX-1 trace this number stays at the same value most of the time. However when the largest spike of duplicates occurs more than $2*10^5$ distinct prefixes are involved during less than one hour. As a result the cache did not retain most of the route changes occurring during this period. Hence subsequent duplicates caused by these routes were not filtered by the cache.

### 3.5 Discussion

Although a cache is effective in filtering feeds with a high ratio of duplicates (e.g. EQUIX-2), we observed that spikes of updates involving a large number of distinct prefixes are detrimental to the performance of the cache. These spikes can have multiple origins. First, spikes of updates can be caused by large routing events beyond the router. Second, spikes can be caused by routing table transfers following a session reset or a change in outbound policies. It is indeed common for network operators to prompt a table transfer with a ROUTE REFRESH message in order to apply changes in their inbound policies. However spikes in this second category must have been filtered by the MCT algorithm applied beforehand.

While we can explain the origin of spikes, we do not know if these spikes represent a frequent feature of the BGP sessions. We now measure the maximum spike size in term of distinct prefixes for all RouteViews sessions we observed during the year 2014. We also apply a `lru` cache of 65k entries on all these traces to map the performance of the cache to the size of the spikes observed in the sessions. The sample size for all measured sessions is of 1339 traces.

We define attenuation as the ratio of the number of duplicates seen in the original trace over the number of duplicates seen after the cache. The average attenuation of duplicates for all observed traces is 300.47. If we distinguish the traces by the size of their maximum spikes, the average attenuation for traces with spikes larger and smaller than the size of the cache are 1.26 and 370.06 respectively.

The existence of updates spikes can negatively impact the possibility to mitigate the duplicates. We measured the presence of spikes among all observed sessions in 2014. For this purpose, we consider there is a spike in a trace when more than 65k distinct prefixes at the origin of future duplicates are transferred in less than one hour. According to this definition, 11.73% of the traces displayed large spikes of duplicates.

## 4. CONCLUSION

Redundant consecutive BGP announcements consume unnecessary bandwidth and CPU in routers. In addition, these messages delay the propagation of useful routing information. We observed that BGP sessions exhibit different behaviors. For some session the number of duplicates is low. But other sessions can exhibit a very high ratio of duplicates. We identified large spikes of duplicates in 11.73% of the sessions we observed in 2014. This may be a problem on chatty sessions.

We then identified three causes of duplicates: changes in attributes that are not propagated further, flapping of routes or attributes and, finally, incorrect implementations for sets in AS-Paths. We verified these causes by performing thorough controlled experiments.

To mitigate the problem we propose use of a cache to find the right trade-off between additional memory consumption and the reduction of duplicates. We show that the performance of a cache highly depends on the characteristics of the BGP trace, in addition to the eviction strategy. While a cache is suitable on some traces, it is not always the case. The current trend of pushing control functions outside the router, to devices that are not as limited memory-wise, opens the door to full Adj-RIB-Outs and thus enable to avoid using pretty hacks to get rid of BGP duplicates completely in the future.

## 5. REFERENCES

[1] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," RFC 4271, Jan. 2006.

[2] C. Labovitz, G. R. Malan, and F. Jahanian, "Internet routing instability," *IEEE/ACM Transactions on Networking*, vol. 6, no. 5, pp. 515–528, 1998.

[3] C. Pelsser, O. Maennel, P. Mohapatra, R. Bush, and K. Patel, "Route flap damping made usable," in *Passive and Active Measurement*, 2011, pp. 143–152.

[4] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed internet routing convergence," *ACM SIGCOMM CCR*, vol. 30, no. 4, pp. 175–187, 2000.

[5] J. Li, M. Guidero, Z. Wu, E. Purpus, and T. Ehrenkranz, "BGP routing dynamics revisited," *ACM SIGCOMM CCR*, vol. 37, no. 2, pp. 5–16, 2007.

[6] J. H. Park, D. Jen, M. Lad, S. Amante, D. McPherson, and L. Zhang, "Investigating occurrence of duplicate updates in BGP announcements," in *Passive and Active Measurement*, 2010, pp. 11–20.

[7] A. Elmokashfi, A. Kvalbein, and C. Dovrolis, "BGP churn evolution: a perspective from the core," *IEEE/ACM Transactions on Networking*, vol. 20, no. 2, pp. 571–584, 2012.

[8] A. Elmokashfi and A. Dhamdhere, "Revisiting bgp churn growth," *ACM SIGCOMM CCR*, vol. 44, no. 1, pp. 5–12, Dec. 2013.

[9] S. Agarwal, C. Chuah, S. Bhattacharyya, and C. Diot, "Impact of BGP dynamics on router CPU utilization," in *Passive and Active Network Measurement*, 2004, pp. 278–288.

[10] "ExaBGP," http://github.com/Exa-Networks/exabgp, 2014.

[11] "EXOS," http://documentation.extremenetworks.com/exos_commands/EXOS_All/EXOS_Commands_All/r_disable-bgp-adjribout.shtml, 2015.

[12] P.-C. Cheng, B. Zhang, D. Massey, and L. Zhang, "Identifying BGP routing table transfers," *Computer Networks*, vol. 55, no. 3, pp. 636–649, 2011.

DECLARATION OF SCOTT BRADNER

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

# Appendix J

# EXHIBIT A

# Report on International Submarine Cables Landing in the US

Source: underlying data cloned from https://github.com/telegeography/www.submarinecablemap.com, most recent commit at 2018-01-02 14:09:33-05:00 (7d7cd9e8096d624717f2b4e56ebc72831e2ba7f6)

- US Landing Points for International Submarine Cables
- International Submarine Cables Landing in the US

# US Landing Points for International Submarine Cables

## Landing 1

## Bandon, Oregon, United States

Location: (124.4°W, 43.12°N)

1 International Cable:

- FASTER

  Owners:
  Google, KDDI, SingTel, China Telecom, China Mobile, Global Transit
  Other Countries:
  Japan, Taiwan

## Landing 2

## Bellport, New York, United States

Location: (72.94°W, 40.76°N)

1 International Cable:

- Yellow

  Owners:
  Level 3
  Other Country:
  United Kingdom

# Landing 3 Boca Raton, FL, United States

Location: (80.09°W, 26.35°N)

6 International Cables:

- South America-1 (SAm-1)

  Owners:
  Telxius
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

- Bahamas Internet Cable System (BICS)

  Owners:
  Caribbean Crossings
  Other Country:
  Bahamas

- Monet

  Owners:
  Angola Cables, Google, Algar Telecom, Antel Uruguay
  Other Country:
  Brazil

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

- GlobeNet

  Owners:
  BTG Pactual
  Other Countries:
  Bermuda, Brazil, Colombia, Venezuela

- Colombia-Florida Subsea Fiber (CFX-1)

  Owners:
  C&W Networks
  Other Countries:
  Colombia, Jamaica

## Landing 4

## Brookhaven, New York, United States

Location: (72.91°W, 40.77°N)

1 International Cable:

- Atlantic Crossing-1 (AC-1)

  Owners:
  Level 3
  Other Countries:
  Germany, Netherlands, United Kingdom

## Landing 5

## Buffalo, New York, United States

Location: (78.88°W, 42.89°N)

1 International Cable:

- Crosslake Fibre

  Owners:
  Crosslake Fibre
  Other Country:
  Canada

## Landing 6

## Charlestown, Rhode Island, United States

Location: (71.65°W, 41.41°N)

1 International Cable:

- Challenger Bermuda-1 (CB-1)

  Owners:
  Cable Co.
  Other Country:
  Bermuda

## Landing 7

## El Segundo, California, United States

Location: (118.4°W, 33.92°N)

1 International Cable:

- Pacific Light Cable Network (PLCN)

  Owners:
  Pacific Light Data Communication Co. Ltd., Google, Facebook
  Other Countries:
  China, Philippines, Taiwan

## Landing 8

## Grover Beach, California, United States

Location: (120.6°W, 35.12°N)

2 International Cables:

- Pan-American Crossing (PAC)

  Owners:
  Level 3
  Other Countries:
  Costa Rica, Mexico, Panama

- Pacific Crossing-1 (PC-1)

  Owners:
  NTT
  Other Country:
  Japan

## Landing 9 Harbour Pointe, Washington, United States

Location: (122.3°W, 47.89°N)

1 International Cable:

- Pacific Crossing-1 (PC-1)

  Owners:
  NTT
  Other Country:
  Japan

## Landing 10 Hermosa Beach, California, United States

Location: (118.4°W, 33.86°N)

2 International Cables:

- JUPITER

  Owners:
  Amazon, Facebook, NTT, PLDT, PCCW, Softbank Telecom
  Other Countries:
  Japan, Philippines

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

**Landing 11**

## Hillsboro, Oregon, United States

Location: (123°W, 45.52°N)

2 International Cables:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

# Landing 12 Hollywood, Florida, United States

Location: (80.16°W, 26.01°N)

4 International Cables:

- Columbus-III

  Owners:
  Telecom Italia Sparkle, AT&T, Verizon, Telefonica, Portugal Telecom, Tata Communications, Ukrtelecom, Telkom South Africa, Telecom Argentina, Instituto Costarricense de Electricidad, Embratel, Cyta
  Other Countries:
  Italy, Portugal, Spain

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Maya-1

  Owners:
  Verizon, AT&T, Sprint, Hondutel, Telefonica, Orbitel, Telecom Italia Sparkle, C&W Networks, Entel Chile, Embratel, ETB, Axtel, Instituto Costarricense de Electricidad, Proximus, Prepa Networks, Orange, Tricom, RSL Telecom, América Móvil
  Other Countries:
  Cayman Islands, Colombia, Costa Rica, Honduras, Mexico, Panama

## Landing 13 Island Park, New York, United States

Location: (73.66°W, 40.6°N)

1 International Cable:

- FLAG Atlantic-1 (FA-1)

  Owners:
  Global Cloud Xchange
  Other Countries:
  France, United Kingdom

## Landing 14 Isla Verde, Puerto Rico, United States

Location: (66.02°W, 18.44°N)

3 International Cables:

- Saint Maarten Puerto Rico Network One (SMPR-1)

  Owners:
  TelEm Group, Dauphin Telecom
  Other Countries:
  Saint Martin, Sint Maarten

- ARCOS

  Owners:
  C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
  Other Countries:
  Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

- Antillas 1

  Owners:
  AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
  Other Country:
  Dominican Republic

## Landing 15 Jacksonville, Florida, United States

Location: (81.66°W, 30.33°N)

3 International Cables:

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- South America Pacific Link (SAPL)

  Owners:
  Ocean Networks
  Other Countries:
  Chile, Panama

- Pacific Caribbean Cable System (PCCS)

  Owners:
  C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
  Other Countries:
  Aruba, Colombia, Curaçao, Ecuador, Panama

## Landing 16 Kahe Point, Hawaii, United States

Location: (158.1°W, 21.35°N)

1 International Cable:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

## Landing 17

## Kapolei, HI, United States

Location: (158.1°W, 21.34°N)

1 International Cable:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

## Landing 18

## Kawaihae, Hawaii, United States

Location: (155.8°W, 20.04°N)

1 International Cable:

- Honotua

  Owners:
  OPT French Polynesia
  Other Country:
  French Polynesia

## Landing 19

## Keawaula, Hawaii, United States

Location: (158.2°W, 21.43°N)

2 International Cables:

- Telstra Endeavour

  Owners:
  Telstra
  Other Country:
  Australia

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

## Landing 20

## Los Angeles, California, United States

Location: (118.2°W, 34.05°N)

1 International Cable:

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

## Landing 21 Lynn, Massachusetts, United States

Location: (70.95°W, 42.46°N)

1 International Cable:

- GTT Atlantic

  Owners:
  GTT
  Other Countries:
  Canada, Ireland, United Kingdom

## Landing 22 Makaha, Hawaii, United States

Location: (158.2°W, 21.46°N)

3 International Cables:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

- South America Pacific Link (SAPL)

  Owners:
  Ocean Networks
  Other Countries:
  Chile, Panama

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

## Landing 23

## Manasquan, New Jersey, United States

Location: (74.05°W, 40.12°N)

3 International Cables:

- TAT-14

  Owners:
  BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
  Other Countries:
  Denmark, France, Germany, Netherlands, United Kingdom

- Gemini Bermuda

  Owners:
  C&W Networks
  Other Country:
  Bermuda

- Apollo

  Owners:
  Vodafone
  Other Countries:
  France, United Kingdom

## Landing 24

## Manchester, California, United States

Location: (123.7°W, 38.97°N)

1 International Cable:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

## Landing 25

## Miramar, Puerto Rico, United States

Location: (66.08°W, 18.45°N)

2 International Cables:

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Antillas 1

  Owners:
  AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
  Other Country:
  Dominican Republic

## Landing 26

## Morro Bay, California, United States

Location: (120.8°W, 35.37°N)

2 International Cables:

- Japan-U.S. Cable Network (JUS)

  Owners:
  Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
  Other Country:
  Japan

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

## Landing 27

## Naples, FL, United States

Location: (81.8°W, 26.14°N)

1 International Cable:

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

## Landing 28

## Nedonna Beach, Oregon, United States

Location: (123.9°W, 45.64°N)

1 International Cable:

- Trans-Pacific Express (TPE) Cable System

  Owners:
  China Telecom, China Unicom, Chunghwa Telecom, KT, Verizon, NTT, AT&T
  Other Countries:
  China, Japan, Taiwan

## Landing 29

## North Miami Beach, Florida, United States

Location: (80.16°W, 25.93°N)

1 International Cable:

- ARCOS

  Owners:
  C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
  Other Countries:
  Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

## Landing 30

## Northport, New York, United States

Location: (73.34°W, 40.91°N)

1 International Cable:

- FLAG Atlantic-1 (FA-1)

  Owners:
  Global Cloud Xchange
  Other Countries:
  France, United Kingdom

## Landing 31

## Pacific City, OR, United States

Location: (124°W, 45.2°N)

2 International Cables:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

- New Cross Pacific (NCP) Cable System

  Owners:
  China Telecom, China Unicom, Chunghwa Telecom, KT, China Mobile, Microsoft, Softbank Telecom
  Other Countries:
  China, Japan, Taiwan

## Landing 32

## Pago Pago, American Samoa

Location: (170.7°W, -14.28°N)

2 International Cables:

- Hawaiki

  Owners:
  Hawaiki Cable Company
  Other Countries:
  Australia, New Zealand

- Samoa-American Samoa (SAS)

  Owners:
  American Samoa Government, Elandia
  Other Country:
  Samoa

# Landing 33 Piti, Guam

Location: (-144.7°W, 13.46°N)

5 International Cables:

- HANTRU1 Cable System

  Owners:
  Hannon Armstrong, Federated States of Micronesia Telecommunications Company, Marshall Islands Telecommunications Authority
  Other Country:
  Federated States of Micronesia

- PIPE Pacific Cable-1 (PPC-1)

  Owners:
  TPG
  Other Countries:
  Australia, Papua New Guinea

- Hong Kong-Guam (HK-G)

  Owners:
  RTI Connectivity
  Other Country:
  China

- Tata TGN-Pacific

  Owners:
  Tata Communications
  Other Country:
  Japan

- SEA-US

  Owners:
  RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
  Other Countries:
  Federated States of Micronesia, Indonesia, Palau, Philippines

## Landing 34

# Redondo Beach, California, United States

Location: (118.4°W, 33.84°N)

1 International Cable:

- Unity/EAC-Pacific

  Owners:
  Telstra, Google, Global Transit, SingTel, KDDI, Airtel (Bharti)
  Other Country:
  Japan

# Landing 35 San Juan, Puerto Rico, United States

Location: (66.11°W, 18.47°N)

7 International Cables:

- America Movil Submarine Cable System-1 (AMX-1)

  Owners:
  América Móvil
  Other Countries:
  Brazil, Colombia, Dominican Republic, Guatemala, Mexico

- South America-1 (SAm-1)

  Owners:
  Telxius
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

- Deep Blue Cable

  Owners:
  Deep Blue Cable
  Other Countries:
  Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

- Global Caribbean Network (GCN)

  Owners:
  Leucadia National Corporation, Loret Group
  Other Country:
  Guadeloupe

- Pacific Caribbean Cable System (PCCS)

  Owners:
  C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
  Other Countries:
  Aruba, Colombia, Curaçao, Ecuador, Panama

- Southern Caribbean Fiber

  Owners:
  Digicel
  Other Countries:
  Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

- BRUSA

Owners:
Telxius
Other Country:
Brazil

## Landing 36 San Luis Obispo, California, United States

Location: (120.7°W, 35.29°N)

1 International Cable:

- Asia-America Gateway (AAG) Cable System

Owners:
Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
Other Countries:
Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

## Landing 37 Sarasota, Florida, United States

Location: (82.54°W, 27.34°N)

1 International Cable:

- AURORA

Owners:
FP Telecommunications
Other Countries:
Belize, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Honduras, Mexico, Nicaragua, Panama

## Landing 38

## Shirley, New York, United States

Location: (72.87°W, 40.8°N)

2 International Cables:

- AEConnect (AEC)

  Owners:
  Aqua Comms
  Other Country:
  Ireland

- Apollo

  Owners:
  Vodafone
  Other Countries:
  France, United Kingdom

## Landing 39

## Spanish River Park, Florida, United States

Location: (80.07°W, 26.38°N)

1 International Cable:

- Bahamas Internet Cable System (BICS)

  Owners:
  Caribbean Crossings
  Other Country:
  Bahamas

**Landing 40**

## Spencer Beach, Hawaii, United States

Location: (155.8°W, 20.02°N)

1 International Cable:

- Southern Cross Cable Network (SCCN)

  Owners:
  Spark New Zealand, SingTel Optus, Verizon
  Other Countries:
  Australia, Fiji, New Zealand

# Landing 41

## St. Croix, Virgin Islands, United States

Location: (64.82°W, 17.77°N)

5 International Cables:

- South American Crossing (SAC)/Latin American Nautilus (LAN)

  Owners:
  Level 3, Telecom Italia Sparkle
  Other Countries:
  Argentina, Brazil, Chile, Colombia, Panama, Peru, Venezuela

- Americas-II

  Owners:
  Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
  Other Countries:
  Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

- Pan American (PAN-AM)

  Owners:
  AT&T, Telefonica del Peru, Softbank Telecom, Telecom Italia Sparkle, Sprint, CANTV, Tata Communications, Telefónica de Argentina, Telstra, Verizon, Entel Chile, Telecom Argentina, Telconet, Instituto Costarricense de Electricidad, C&W Networks, Embratel
  Other Countries:
  Aruba, Chile, Colombia, Ecuador, Panama, Peru, Venezuela

- Global Caribbean Network (GCN)

  Owners:
  Leucadia National Corporation, Loret Group
  Other Country:
  Guadeloupe

- Southern Caribbean Fiber

  Owners:
  Digicel
  Other Countries:
  Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

## Landing 42 Tanguisson Point, Guam

Location: (-144.8°W, 13.55°N)

2 International Cables:

- Asia-America Gateway (AAG) Cable System

  Owners:
  Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
  Other Countries:
  Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

- Australia-Japan Cable (AJC)

  Owners:
  Softbank Telecom, Telstra, Verizon, AT&T
  Other Countries:
  Australia, Japan

## Landing 43 Tuckerton, New Jersey, United States

Location: (74.34°W, 39.6°N)

2 International Cables:

- TAT-14

  Owners:
  BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
  Other Countries:
  Denmark, France, Germany, Netherlands, United Kingdom

- GlobeNet

  Owners:
  BTG Pactual
  Other Countries:
  Bermuda, Brazil, Colombia, Venezuela

## Landing 44

## Tumon Bay, Guam

Location: (-144.8°W, 13.51°N)

2 International Cables:

- Guam Okinawa Kyushu Incheon (GOKI)

  Owners:
  AT&T
  Other Country:
  Japan

- Australia-Japan Cable (AJC)

  Owners:
  Softbank Telecom, Telstra, Verizon, AT&T
  Other Countries:
  Australia, Japan

## Landing 45

## Vero Beach, Florida, United States

Location: (80.39°W, 27.64°N)

1 International Cable:

- Bahamas 2

  Owners:
  AT&T, Telefonica, Verizon
  Other Country:
  Bahamas

## Landing 46

## Virginia Beach, Virginia, United States

Location: (76.06°W, 36.76°N)

3 International Cables:

- MAREA

  Owners:
  Facebook, Microsoft, Telxius
  Other Country:
  Spain

- Midgardsormen

  Owners:
  Midgardsormen
  Other Country:
  Denmark

- BRUSA

  Owners:
  Telxius
  Other Country:
  Brazil

## Landing 47

## Wall Township, New Jersey, United States

Location: (74.06°W, 40.15°N)

2 International Cables:

- Tata TGN-Atlantic

  Owners:
  Tata Communications
  Other Country:
  United Kingdom

- Seabras-1

  Owners:
  Seaborn Group
  Other Country:
  Brazil

# International Submarine Cables Landing in the US

## Cable 1 AEConnect (AEC)

More info:
http://www.aquacomms.com
Owners:
Aqua Comms
Length:
5,536 km
US Landing Point:

- Shirley, New York, United States

Other Country:
Ireland

## Cable 2 America Movil Submarine Cable System-1 (AMX-1)

More info:
http://www.americamovil.com
Owners:
América Móvil
Length:
17,800 km
US Landing Points:

- Hollywood, Florida, United States
- Jacksonville, Florida, United States
- San Juan, Puerto Rico, United States

Other Countries:
Brazil, Colombia, Dominican Republic, Guatemala, Mexico

**Cable 3** **Americas-II**

Owners:
Embratel, AT&T, Verizon, Sprint, CANTV, Tata Communications, Level 3, Telecom Argentina, Orange, Portugal Telecom, C&W Networks, Telecom Italia Sparkle, Entel Chile
Length:
8,373 km
US Landing Points:

- Hollywood, Florida, United States
- Miramar, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Countries:
Brazil, Curaçao, French Guiana, Martinique, Trinidad and Tobago, Venezuela

**Cable 4** **Antillas 1**

Owners:
AT&T, Verizon, Sprint, Tata Communications, Orange, C&W Networks, Telecom Italia Sparkle, Embratel
Length:
650 km
US Landing Points:

- Isla Verde, Puerto Rico, United States
- Miramar, Puerto Rico, United States

Other Country:
Dominican Republic

## Cable 5 Apollo

More info:
http://www.vodafone.com/business/article-cs-apollo-submarine-cable-system
Owners:
Vodafone
Length:
13,000 km
US Landing Points:

- Manasquan, New Jersey, United States
- Shirley, New York, United States

Other Countries:
France, United Kingdom

## Cable 6 ARCOS

More info:
http://www.cwnetworks.com/
Owners:
C&W Networks, CANTV, Codetel, Hondutel, Belize Telemedia, Enitel, AT&T, Alestra, Verizon, RACSA, United Telecommunication Services (UTS), Telecarrier, Tricom USA, Telecomunicaciones Ultramarinas de Puerto Rico, Internexa, Orbinet Overseas, Telepuerto San Isidro, Bahamas Telecommunications Company, Instituto Costarricense de Electricidad, Orbitel
Length:
8,600 km
US Landing Points:

- North Miami Beach, Florida, United States
- Isla Verde, Puerto Rico, United States

Other Countries:
Bahamas, Belize, Colombia, Costa Rica, Curaçao, Dominican Republic, Guatemala, Honduras, Mexico, Nicaragua, Panama, Turks and Caicos Islands, Venezuela

## Cable 7 Asia-America Gateway (AAG) Cable System

More info:
http://www.asia-america-gateway.com
Owners:
Telekom Malaysia, AT&T, Starhub, PLDT, Communications Authority of Thailand, Airtel (Bharti), Telstra, Telkom Indonesia, BT, Eastern Telecom, PT Indonesia Satellite Corp., Spark New Zealand, Viettel Corporation, Saigon Postel Corporation, Vietnam Telecom International, Brunei International Gateway, BayanTel, Ezecom
Length:
20,000 km
US Landing Points:

- Keawaula, Hawaii, United States
- San Luis Obispo, California, United States
- Tanguisson Point, Guam

Other Countries:
Brunei, China, Malaysia, Philippines, Singapore, Thailand, Vietnam

## Cable 8 Atlantic Crossing-1 (AC-1)

More info:
http://www.level3.com
Owners:
Level 3
Length:
14,301 km
US Landing Point:

- Brookhaven, New York, United States

Other Countries:
Germany, Netherlands, United Kingdom

## Cable 9 AURORA

More info:
http://fptelecoms.com/
Owners:
FP Telecommunications
Length:
n.a.
US Landing Point:

- Sarasota, Florida, United States

Other Countries:
Belize, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Honduras, Mexico, Nicaragua, Panama

## Cable 10 Australia-Japan Cable (AJC)

More info:
http://www.ajcable.com
Owners:
Softbank Telecom, Telstra, Verizon, AT&T
Length:
12,700 km
US Landing Points:

- Tanguisson Point, Guam
- Tumon Bay, Guam

Other Countries:
Australia, Japan

## Cable 11 Bahamas 2

Owners:
AT&T, Telefonica, Verizon
Length:
470 km
US Landing Point:

- Vero Beach, Florida, United States

Other Country:
Bahamas

## Cable 12 Bahamas Internet Cable System (BICS)

More info:
http://www.caribbeancrossings.com
Owners:
Caribbean Crossings
Length:
1,100 km
US Landing Points:

- Boca Raton, FL, United States
- Spanish River Park, Florida, United States

Other Country:
Bahamas

## Cable 13 BRUSA

More info:
http://www.telxius.com
Owners:
Telxius
Length:
11,000 km
US Landing Points:

- San Juan, Puerto Rico, United States
- Virginia Beach, Virginia, United States

Other Country:
Brazil

## Cable 14 Challenger Bermuda-1 (CB-1)

More info:
http://cableco.bm
Owners:
Cable Co.
Length:
1,448 km
US Landing Point:

- Charlestown, Rhode Island, United States

Other Country:
Bermuda

## Cable 15 Colombia-Florida Subsea Fiber (CFX-1)

More info:
http://www.cwnetworks.com/
Owners:
C&W Networks
Length:
2,400 km
US Landing Point:

- Boca Raton, FL, United States

Other Countries:
Colombia, Jamaica

## Cable 16 Columbus-III

Owners:
Telecom Italia Sparkle, AT&T, Verizon, Telefonica, Portugal Telecom, Tata Communications, Ukrtelecom, Telkom South Africa, Telecom Argentina, Instituto Costarricense de Electricidad, Embratel, Cyta
Length:
9,833 km
US Landing Point:

- Hollywood, Florida, United States

Other Countries:
Italy, Portugal, Spain

## Cable 17 Crosslake Fibre

More info:
http://www.crosslakefibre.ca
Owners:
Crosslake Fibre
Length:
131 km
US Landing Point:

- Buffalo, New York, United States

Other Country:
Canada

## Cable 18 Deep Blue Cable

More info:
http://www.deepbluecable.com
Owners:
Deep Blue Cable
Length:
12,000 km
US Landing Points:

- Boca Raton, FL, United States
- San Juan, Puerto Rico, United States
- Naples, FL, United States

Other Countries:
Anguilla, Aruba, Bonaire, Sint Eustatius, and Saba, Cayman Islands, Colombia, Curaçao, Dominican Republic, Haiti, Jamaica, Panama, Saint Martin, Trinidad and Tobago, Turks and Caicos Islands

## Cable 19 FASTER

Owners:
Google, KDDI, SingTel, China Telecom, China Mobile, Global Transit
Length:
11,629 km
US Landing Point:

- Bandon, Oregon, United States

Other Countries:
Japan, Taiwan

## Cable 20 FLAG Atlantic-1 (FA-1)

More info:
http://www.globalcloudxchange.com
Owners:
Global Cloud Xchange
Length:
14,500 km
US Landing Points:

- Island Park, New York, United States
- Northport, New York, United States

Other Countries:
France, United Kingdom

## Cable 21 Gemini Bermuda

More info:
http://www.cwnetworks.com
Owners:
C&W Networks
Length:
1,287 km
US Landing Point:

- Manasquan, New Jersey, United States

Other Country:
Bermuda

## Cable 22 Global Caribbean Network (GCN)

More info:
http://www.globalcaribbean.net
Owners:
Leucadia National Corporation, Loret Group
Length:
n.a.
US Landing Points:

- San Juan, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Country:
Guadeloupe

## Cable 23 GlobeNet

More info:
http://www.globenet.net
Owners:
BTG Pactual
Length:
23,500 km
US Landing Points:

- Boca Raton, FL, United States
- Tuckerton, New Jersey, United States

Other Countries:
Bermuda, Brazil, Colombia, Venezuela

## Cable 24 GTT Atlantic

More info:
http://www.gtt.net
Owners:
GTT
Length:
12,200 km
US Landing Point:

- Lynn, Massachusetts, United States

Other Countries:
Canada, Ireland, United Kingdom

## Cable 25

## Guam Okinawa Kyushu Incheon (GOKI)

More info:
http://www.att.com
Owners:
AT&T
Length:
4,244 km
US Landing Point:

- Tumon Bay, Guam

Other Country:
Japan

## Cable 26

## HANTRU1 Cable System

Owners:
Hannon Armstrong, Federated States of Micronesia Telecommunications Company, Marshall Islands Telecommunications Authority
Length:
2,917 km
US Landing Point:

- Piti, Guam

Other Country:
Federated States of Micronesia

## Cable 27 Hawaiki

More info:
http://hawaikicable.co.nz
Owners:
Hawaiki Cable Company
Length:
14,000 km
US Landing Points:

- Kapolei, HI, United States
- Pacific City, OR, United States
- Pago Pago, American Samoa

Other Countries:
Australia, New Zealand

## Cable 28 Hong Kong-Guam (HK-G)

Owners:
RTI Connectivity
Length:
3,900 km
US Landing Point:

- Piti, Guam

Other Country:
China

## Cable 29 Honotua

More info:
http://www.opt.pf
Owners:
OPT French Polynesia
Length:
4,805 km
US Landing Point:

- Kawaihae, Hawaii, United States

Other Country:
French Polynesia

## Cable 30 Japan-U.S. Cable Network (JUS)

Owners:
Verizon, AT&T, BT, Sprint, CenturyLink, KDDI, NTT, Chunghwa Telecom, Tata Communications, SingTel, Telekom Malaysia, Softbank Telecom, Orange, Level 3, SK Broadband, KT, China Telecom, China Unicom, LG Uplus, HKBN Enterprise Solutions, Starhub, PCCW, Telstra, Vodafone, PLDT
Length:
22,682 km
US Landing Points:

- Makaha, Hawaii, United States
- Manchester, California, United States
- Morro Bay, California, United States

Other Country:
Japan

## Cable 31 JUPITER

Owners:
Amazon, Facebook, NTT, PLDT, PCCW, Softbank Telecom
Length:
14,000 km
US Landing Point:

- Hermosa Beach, California, United States

Other Countries:
Japan, Philippines

## Cable 32 MAREA

Owners:
Facebook, Microsoft, Telxius
Length:
6,605 km
US Landing Point:

- Virginia Beach, Virginia, United States

Other Country:
Spain

## Cable 33 Maya-1

More info:
http://www.maya-1.com
Owners:
Verizon, AT&T, Sprint, Hondutel, Telefonica, Orbitel, Telecom Italia Sparkle, C&W Networks, Entel Chile, Embratel, ETB, Axtel, Instituto Costarricense de Electricidad, Proximus, Prepa Networks, Orange, Tricom, RSL Telecom, América Móvil
Length:
4,400 km
US Landing Point:

- Hollywood, Florida, United States

Other Countries:
Cayman Islands, Colombia, Costa Rica, Honduras, Mexico, Panama

## Cable 34 Midgardsormen

More info:
http://midgardsormen.net
Owners:
Midgardsormen
Length:
7,848 km
US Landing Point:

- Virginia Beach, Virginia, United States

Other Country:
Denmark

## Cable 35 Monet

Owners:
Angola Cables, Google, Algar Telecom, Antel Uruguay
Length:
10,556 km
US Landing Point:

- Boca Raton, FL, United States

Other Country:
Brazil

## Cable 36 New Cross Pacific (NCP) Cable System

Owners:
China Telecom, China Unicom, Chunghwa Telecom, KT, China Mobile, Microsoft, Softbank Telecom
Length:
13,618 km
US Landing Point:

- Pacific City, OR, United States

Other Countries:
China, Japan, Taiwan

## Cable 37

## Pacific Caribbean Cable System (PCCS)

Owners:
C&W Networks, Telconet, Setar, United Telecommunication Services (UTS), Telxius
Length:
6,000 km
US Landing Points:

- Jacksonville, Florida, United States
- San Juan, Puerto Rico, United States

Other Countries:
Aruba, Colombia, Curaçao, Ecuador, Panama

## Cable 38

## Pacific Crossing-1 (PC-1)

More info:
http://www.pc1.com
Owners:
NTT
Length:
20,900 km
US Landing Points:

- Grover Beach, California, United States
- Harbour Pointe, Washington, United States

Other Country:
Japan

## Cable 39

## Pacific Light Cable Network (PLCN)

More info:
http://pldc.com.hk
Owners:
Pacific Light Data Communication Co. Ltd., Google, Facebook
Length:
12,871 km
US Landing Point:

- El Segundo, California, United States

Other Countries:
China, Philippines, Taiwan

## Cable 40

## Pan-American Crossing (PAC)

More info:
http://www.level3.com
Owners:
Level 3
Length:
10,000 km
US Landing Point:

- Grover Beach, California, United States

Other Countries:
Costa Rica, Mexico, Panama

## Cable 41 Pan American (PAN-AM)

Owners:
AT&T, Telefonica del Peru, Softbank Telecom, Telecom Italia Sparkle, Sprint, CANTV, Tata Communications, Telefónica de Argentina, Telstra, Verizon, Entel Chile, Telecom Argentina, Telconet, Instituto Costarricense de Electricidad, C&W Networks, Embratel
Length:
7,050 km
US Landing Point:

- St. Croix, Virgin Islands, United States

Other Countries:
Aruba, Chile, Colombia, Ecuador, Panama, Peru, Venezuela

## Cable 42 PIPE Pacific Cable-1 (PPC-1)

More info:
http://www.pipenetworks.com/ppc1
Owners:
TPG
Length:
6,900 km
US Landing Point:

- Piti, Guam

Other Countries:
Australia, Papua New Guinea

## Cable 43 Saint Maarten Puerto Rico Network One (SMPR-1)

Owners:
TelEm Group, Dauphin Telecom
Length:
375 km
US Landing Point:

- Isla Verde, Puerto Rico, United States

Other Countries:
Saint Martin, Sint Maarten

## Cable 44

## Samoa-American Samoa (SAS)

Owners:
American Samoa Government, Elandia
Length:
250 km
US Landing Point:

- Pago Pago, American Samoa

Other Country:
Samoa

## Cable 45

## Seabras-1

More info:
http://www.seabornnetworks.com
Owners:
Seaborn Group
Length:
10,800 km
US Landing Point:

- Wall Township, New Jersey, United States

Other Country:
Brazil

## Cable 46 SEA-US

Owners:
RTI, Inc., Globe Telecom, Hawaiian Telcom, GTA TeleGuam, Telin, Balau Submarine Cable Company, Federated States of Micronesia Telecommunications Company
Length:
14,500 km
US Landing Points:

- Hermosa Beach, California, United States
- Makaha, Hawaii, United States
- Piti, Guam

Other Countries:
Federated States of Micronesia, Indonesia, Palau, Philippines

## Cable 47 South America-1 (SAm-1)

More info:
http://www.telxius.com/
Owners:
Telxius
Length:
25,000 km
US Landing Points:

- Boca Raton, FL, United States
- San Juan, Puerto Rico, United States

Other Countries:
Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, Guatemala, Peru

## Cable 48 South American Crossing (SAC)/Latin American Nautilus (LAN)

More info:
http://www.level3.com
Owners:
Level 3, Telecom Italia Sparkle
Length:
20,000 km
US Landing Point:

- St. Croix, Virgin Islands, United States

Other Countries:
Argentina, Brazil, Chile, Colombia, Panama, Peru, Venezuela

## Cable 49 South America Pacific Link (SAPL)

More info:
http://www.oceannetworks.com
Owners:
Ocean Networks
Length:
17,600 km
US Landing Points:

- Jacksonville, Florida, United States
- Makaha, Hawaii, United States

Other Countries:
Chile, Panama

## Cable 50 Southern Caribbean Fiber

More info:
http://www.southern-caribbean.com
Owners:
Digicel
Length:
n.a.
US Landing Points:

- San Juan, Puerto Rico, United States
- St. Croix, Virgin Islands, United States

Other Countries:
Antigua and Barbuda, Barbados, Dominica, Grenada, Guadeloupe, Martinique, Saint-Barthélemy, Saint Kitts and Nevis, Saint Lucia, Saint Martin, Saint Vincent and the Grenadines, Trinidad and Tobago

## Cable 51 Southern Cross Cable Network (SCCN)

More info:
http://www.southerncrosscables.com
Owners:
Spark New Zealand, SingTel Optus, Verizon
Length:
30,500 km
US Landing Points:

- Hillsboro, Oregon, United States
- Kahe Point, Hawaii, United States
- Morro Bay, California, United States
- Spencer Beach, Hawaii, United States

Other Countries:
Australia, Fiji, New Zealand

## Cable 52 TAT-14

More info:
https://www.tat-14.com
Owners:
BT, Verizon, Deutsche Telekom, Orange, Sprint, TeliaSonera, Level 3, KPN, Telenor, Etisalat, OTEGLOBE, SingTel, KDDI, Softbank Telecom, Zayo Group, Portugal Telecom, Slovak Telekom, TDC, Telus, Tata Communications, Telefonica, AT&T, Proximus, Elisa Corporation, Cyta, Rostelecom, Vodafone
Length:
15,295 km
US Landing Points:

- Manasquan, New Jersey, United States
- Tuckerton, New Jersey, United States

Other Countries:
Denmark, France, Germany, Netherlands, United Kingdom

## Cable 53 Tata TGN-Atlantic

More info:
http://www.tatacommunications.com
Owners:
Tata Communications
Length:
13,000 km
US Landing Point:

- Wall Township, New Jersey, United States

Other Country:
United Kingdom

## Cable 54 Tata TGN-Pacific

More info:
http://www.tatacommunications.com
Owners:
Tata Communications
Length:
22,300 km
US Landing Points:

- Hillsboro, Oregon, United States
- Los Angeles, California, United States
- Piti, Guam

Other Country:
Japan

## Cable 55 Telstra Endeavour

More info:
https://www.telstraglobal.com
Owners:
Telstra
Length:
9,125 km
US Landing Point:

- Keawaula, Hawaii, United States

Other Country:
Australia

## Cable 56 Trans-Pacific Express (TPE) Cable System

More info:
http://tpecable.org
Owners:
China Telecom, China Unicom, Chunghwa Telecom, KT, Verizon, NTT, AT&T
Length:
17,000 km
US Landing Point:

- Nedonna Beach, Oregon, United States

Other Countries:
China, Japan, Taiwan

## Cable 57 Unity/EAC-Pacific

Owners:
Telstra, Google, Global Transit, SingTel, KDDI, Airtel (Bharti)
Length:
9,620 km
US Landing Point:

- Redondo Beach, California, United States

Other Country:
Japan

## Cable 58 Yellow

More info:
http://www.level3.com
Owners:
Level 3
Length:
7,001 km
US Landing Point:

- Bellport, New York, United States

Other Country:
United Kingdom

DECLARATION OF SCOTT BRADNER

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

# Appendix K

This document was also filed as ECF No. 143-3 and can be found in this Joint Appendix at JA0286.

DECLARATION OF SCOTT BRADNER

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

# Appendix L

This document was also filed as ECF No. 168-28 and can be found in this Joint Appendix at JA3145.

DECLARATION OF SCOTT BRADNER

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

# Appendix M

This document was also filed as ECF No. 168-23 and can be found in this Joint Appendix at JA2743.

DECLARATION OF SCOTT BRADNER

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

# Appendix N

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

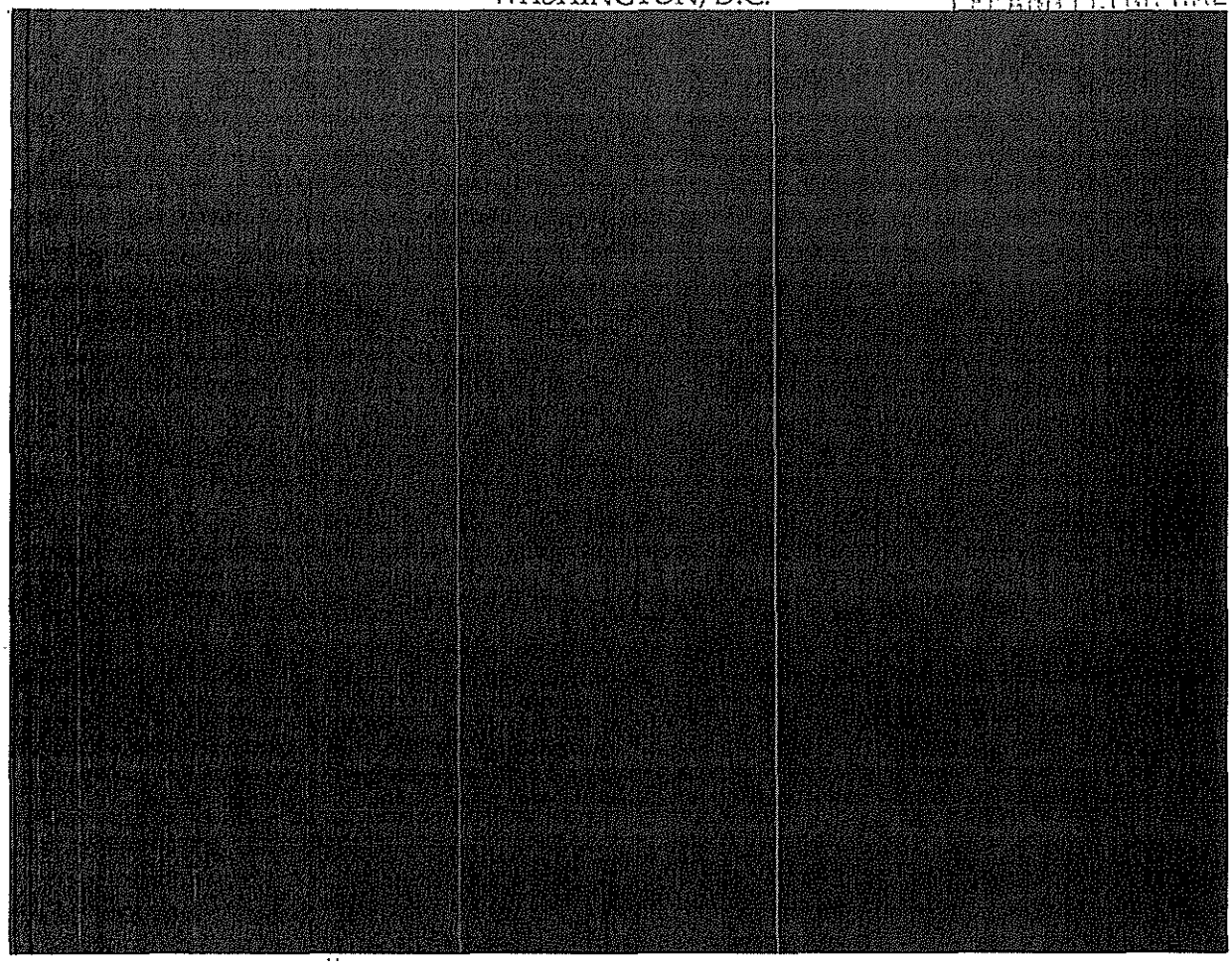
~~SECRET//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

SECRET INTELLIGENCE SURVEILLANCE
2011 AUG 16 PM 2:16
LEEANN FLYNN HALL



NOTICE OF FILING OF GOVERNMENT'S SUPPLEMENT TO ITS SUBMISSIONS OF JUNE 1st AND JUNE 28TH, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits the attached supplement in further support of the

~~SECRET//ORCON,NOFORN~~

Classified by: ~~Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ~~
Reason: 1.4(c)
Declassify on: ~~16 August 2036~~

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



arguments set forth in submissions of June 1st and June 28th, 2011, concerning the above-referenced matters. This supplement explains the methodology behind and sets forth the results of a manual review by the National Security Agency (NSA) of a statistically representative sample of the nature and scope of the Internet communications acquired through NSA's FISA Amendments Act Section 702 upstream collection during a six-month period. The Government respectfully submits that the data provided herein supplements and supports the Government's Responses to the Court's Briefing Order of May 9th, 2011, and supplemental questions of June 17, 2011, and will further assist the Court in concluding that the certifications and procedures submitted in the above-referenced matters satisfy the requirements of the Act and are consistent with the Fourth Amendment to the Constitution of the United States. ~~(S//OC,NF)~~

Given the complex nature of the information provided in this supplement, the United States is prepared to provide any additional information the Court believes would aid it in reviewing these matters. The Government may also seek to supplement and/or clarify the information provided herein as appropriate during any hearing that the Court may hold in the above-captioned matters. ~~(S//OC,NF)~~

Respectfully submitted,

[redacted]

National Security Division
United States Department of Justice



Wikimedia Found. v. NSA DOJ000116

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



## (U//FOUO) NSA Characterization of Upstream Data: Process and Results

### I. (U) Introduction

~~(TS//SI//NF)~~ This report explains the methodology behind and provides the results of a manual review of a statistically representative sample of Internet communications acquired through NSA's FISA Amendments Act (hereinafter "FAA") section 702 upstream collection during a six-month period.[1] The purpose of this review was to assemble data to assist the Court in understanding the nature and scope of the communications acquired through NSA's upstream collection. The data assembled consisted of:

- The volume of transactions containing single, discrete communications to, from, or about a selector used by a person targeted in accordance with NSA's section 702 targeting procedures (hereinafter "tasked selector") versus transactions containing multiple communications (hereinafter "Multi-communication Transactions" or "MCT") not all of which may be to, from, or about a tasked selector;[2]
- The types of discrete communications contained within MCTs [redacted]; and

[1] ~~(TS//SI//NF)~~ Additionally, as described on pages 8-9 of the Government's June 1, 2011 Response to the Court's Briefing Order of May 9, 2011, NSA conducted two tests of FAA 702 upstream collection in May 2011 using information from NSA's technical databases in an attempt to determine the likelihood of collecting an Internet transaction between a user in the United States and [redacted] NSA also attempted to further determine the extent to which those tests might be statistically representative of NSA's 702 upstream collection and repeated these tests in July 2011 using alternative data sets. Because of the technical limitations for automatically identifying transactions containing multiple communications, NSA assesses that the results of these tests are not comparable to each other or with the results of the separate manual analysis discussed herein. Furthermore, for the same reason of technical limitation, the results do not express as high a degree of granularity and accuracy as the manual analysis discussed herein, which took more than one month of careful review by experienced analysts to complete. None of the results discussed herein and in the Government's June 1 Response, however, are inconsistent.

[2] ~~(TS//SI//NF)~~ As described on pages 27-28 of the Government's June 1, 2011 Response to the Court's Briefing Order of May 9, 2011, NSA's inability to separate out individual pieces of information from Internet communications acquired by NSA's upstream collection systems does not extend to all forms of transactions. NSA has developed the capability to [redacted] identify transactions which [redacted] and, in certain other limited instances, transactions where an "active user" (as described more fully below) is a tasked selector. Based on a test of this capability from July 16th-29th 2011, NSA estimates that approximately only [redacted] of NSA's current upstream collection under FAA section 702 could be identified through [redacted] processes as communications to, from or about NSA's tasked selector. As reflected by the results of this manual review, this figure is significantly under-representative of the total proportion of NSA's upstream collection assessed to be communications to, from or about a tasked selector.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360701

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


- The volume of MCTs that NSA assesses contain a wholly domestic communication not to, from, or about a tasked selector.[3]

II. (U) How the Statistically Representative Sample Was Assembled

~~(TS//SI//NF)~~ NSA assembled the sample of communications acquired through its upstream collection by first identifying all Internet communications acquired under section 702 – i.e., both from NSA upstream collection and collection from Internet service providers either by or with the assistance of the Federal Bureau of Investigation (hereinafter "PRISM collection") -- during a six-month period from January 1st through June 30th, 2011, and present within [redacted] as of July 14, 2011. As of that date, 140,974,921 Internet communications were present within [redacted] Of these, 127,718,854 (or approximately 91%) were acquired from PRISM collection, and 13,256,067 (or approximately 9%) were acquired through NSA's upstream collection.[6]

~~(TS//SI//NF)~~ The approximately 13.25 million Internet communications acquired through NSA's upstream collection (hereinafter "transactions") were then "shuffled" by NSA statisticians to ensure a random sample (i.e., any sample drawn would be statistically representative of the total 13.25 million transactions). NSA statisticians estimated that a manual review of a sample of approximately 50,000 of these randomized transactions would enable characterization of all 13.25 million transactions with a statistically high level of confidence and precision.[7]

III. (U) How the Manual Review Was Conducted and the Results of the Review

~~(TS//SI//NF)~~ Under the leadership of NSA's Deputy Director, an experienced interdisciplinary team consisting of experienced intelligence analysts, attorneys from NSA's Office of General Counsel, representatives from NSA's Office of the Director of Compliance, NSA statisticians, representatives from NSA's Network Analysis Center, and representatives from NSA's Office of Oversight and Compliance was assembled to conduct the review described herein and compile this report. A team of experienced NSA

[3] ~~(TS//SI//NF)~~ This aspect of the review required analysts to perform intensive analysis on discrete communications which did not contain the target's selector within MCTs, to determine if the sender and all intended recipients of those discrete communications were located in the United States. Such in-depth analysis is not typically conducted by analysts in their daily foreign intelligence analysis. Instead, an analyst would tend to focus his or her attention on those discrete communications within the MCT that are to, from, or about their assigned target, and would only perform a deeper inspection of those communications to confirm they were not wholly domestic if they were in-fact pertinent to the analyst's evaluation of foreign intelligence information and therefore worth further analysis for potential use.

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

[5] ~~(TS//SI//NF)~~ This figure does not include Internet communications that were acquired during this six-month period but were purged prior to July 14, 2011.

[6] ~~(TS//SI//NF)~~ *See* Figure A of Appendix A, attached hereto.

[7] ~~(TS//SI//NF)~~ Details for the basis for NSA's statistical assertions are set forth in Appendix B, attached hereto.

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


intelligence analysts was assigned to conduct a manual review of the transactions. Ultimately, that team of NSA intelligence analysts collectively reviewed a total of 50,440 individual transactions.

~~(TS//SI//NF)~~ In order to ensure consistency among the analysts in their review, before beginning the manual review, the team members were trained to recognize MCTs and how to characterize the discrete communications contained within them. The team members were given training materials created specifically for this effort, which included screenshots depicting typical examples of the types of transactions acquired through NSA's upstream collection. NSA's Office of General Counsel, Office of Oversight and Compliance, and Office of the Director for Compliance reviewed all training materials and provided guidance throughout the manual review.

~~(TS//SI//NF)~~ For quality assurance, some transactions (approximately 10 out of every 5,000) underwent independent reviews by more than one analyst. In addition, the team lead performed spot reviews of transactions that had already undergone review (approximately 1 out of every 100). The team lead also personally reviewed any transaction that team members were unable to immediately characterize as clearly being a discrete communication or an MCT; as well as any MCT identified as potentially concerning a person located in the United States. Both the quality assurance overlap and the reviews performed by the team lead revealed no discrepancies among how analysts characterized any of the transactions subjected to these overlapping reviews.

~~(TS//SI//NF)~~ In conducting the manual review, NSA analysts took the following steps and made the following findings:

1. **Determined if the transaction was a single, discrete communication or an MCT.**[8] If the transaction was determined to be a single, discrete communication, no further analysis was done. Transactions determined to be MCTs were further analyzed, as described below.

   - Of the 50,440 transactions reviewed, 45,359 (approximately 90%) were determined to be single, discrete communications. The remaining 5,081 transactions (approximately 10%) were determined to be MCTs.[9]

2. **Characterized the discrete communications within the 5,081 MCTs as being** [redacted]

   - Of the 5,081 MCTs reviewed, [redacted]

[8] ~~(TS//SI//NF)~~ For any objects that the initial reviewer was uncertain about how to characterize (e.g., if the transaction contained data requiring further processing to render it intelligible to the analyst), the team lead performed a second review. As a result, each of 50,440 transactions reviewed were able to be characterized as being either a single, discrete communication or an MCT.

[9] ~~(TS//SI//NF)~~ *See* Figure B of Appendix A.

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

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


[redacted][12]

3. **Determined whether the 5,081 MCTs contained any discrete communications as to which the sender and all intended recipients were located in the United States.** As discussed in more detail below, in many cases NSA analysts were able to make these determinations based on the location of the "active user" of the MCT.[13] In other cases, NSA had to rely on content analysis because the MCT did not contain technical information sufficient to identify the active user or to determine the active user's location. There were, however, instances where the MCT did not contain sufficient technical information or content for NSA to assess whether the MCT contained any wholly domestic communications.

   - Of the 5,081 MCTs, 713 (approximately 14%) had a tasked selector as the active user [redacted]. No further analysis of these MCTs was done to determine whether they contained wholly domestic communications. That is because the user of the tasked selector, who by operation of the NSA targeting procedures is a person reasonably believed to be located outside the United States, would be either the sender or an intended recipient of each of the discrete communications contained within the MCT.[14] Accordingly, all of the discrete communications within those MCTs would have at least one communicant reasonably believed to be located outside the United States (i.e., the target) and thus would not be wholly domestic.
   - Of the 5,081 MCTs, 2,668 (approximately 52%) had an active user that was not a tasked selector but was nonetheless an electronic communications account/address/identifier

[11] ~~(TS//SI//NF)~~ *See* Figure C of Appendix A.

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

[13] ~~(TS//SI//NF)~~ When NSA acquires an Internet transaction between an individual using an electronic communications account/address/identifier and his/her service provider, that individual is the "active user" for that transaction. Such transactions can have, at most, one "active user."

[14] ~~(TS//SI//NF)~~ In this context, a communication to or from the target includes communications to or from the tasked selector itself (e.g., an e-mail sent to a tasked e-mail account), as well as communications where the tasked selector appears in other communications attributable to the target [redacted] *See In re DNI/AG Certificatio* [redacted] Docket No. 702(i)-08-01, Mem. Op. at 17 n.14 (USFISC Sept. 4, 2008).

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



reasonably believed to be used by a person located outside the United States.[15] No further analysis of these MCTs was done to determine whether they contained wholly domestic communications. That is because the foreign-based active user would be either a sender or intended recipient of each of the discrete communications within the transaction. Accordingly, all of the discrete communications within those MCTs would have at least one communicant reasonably believed to be located outside the United States (i.e., the foreign-based active user) and thus would not be wholly domestic.

- Of the 5,081 MCTs, 8 (approximately 0.16%) contained an electronic communication account/address/identifier of a non-targeted active user who appeared to be located in the United States, but none of the discrete communications within the MCT were determined to be wholly domestic because at least one of the communicants to each discrete communication was reasonably believed to be located outside the United States. Specifically, the 8 MCTs were determined to concern six non-targeted active users (i.e., two of the MCTs were duplicates):
  - Four MCTs (including both duplicates) [redacted] contained at least one e-mail message from a tasked selector as well as other e-mail messages from accounts/addresses/identifiers reasonably believed to be used by a person located outside the United States.[16] [redacted].
  - Three MCTs [redacted] with the users of accounts/addresses/identifiers who were reasonably believed to be located outside the United States.[17]
  - One MCT [redacted] where further technical analysis revealed that the active user was reasonably believed to be located outside the United States.
- Of the 5,081 MCTs, 10 (approximately 0.2%) contained an electronic communication account/address/identifier of a non-targeted active user who was located in the United States, and the MCTs contained at least one discrete communication that was wholly

[15] ~~(TS//SI//NF)~~ To determine the location of the non-targeted active user, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

[16] ~~(TS//SI//NF)~~ To determine the location of the senders of each of these discrete e-mail messages, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

[17] ~~(TS//SI//NF)~~ To determine the location of [redacted] NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

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



domestic. Specifically, all 10 of these MCTs were [redacted] and all 10 involved U.S.-based persons using [redacted].[18] For all 10 of these MCTs, only [redacted] was present. The [redacted] did not include [redacted]

- 9 of the 10 [redacted] were attributed to a single U.S.-based user. Each of these 9 [redacted] 10 total e-mail messages. The 9 [redacted] were not completely duplicative, but many of the 10 e-mail messages [redacted] were duplicative.
  - Two of the messages [redacted] in each of the 9 [redacted] contained a tasked selector and thus were not assessed to be wholly domestic.
  - Three of the messages [redacted] in each of the 9 [redacted] were [redacted] which is located in the United States) and thus were assessed to be wholly domestic.
  - The remaining e-mail messages [redacted] were between the U.S.-based user and persons reasonably believed to be located outside the United States (and thus not assessed to be wholly domestic) or whose location was unknown.[19]
- The other [redacted] was attributed to a different U.S.-based user. This [redacted] 15 total e-mail messages:
  - One of the [redacted] e-mail messages was from a tasked selector and thus was not assessed to be wholly domestic.
  - One of the [redacted] e-mail messages appeared to be a message that the U.S.-based user sent to himself [redacted] and thus was assessed to be wholly domestic.
  - One of the [redacted] e-mail messages appeared to be a message sent by an associate [redacted] account and thus was assessed to be wholly domestic.
  - The remaining e-mail messages [redacted] were between the U.S.-based user and persons reasonably believed to be

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

[19] ~~(TS//SI//NF)~~ To determine the location of the other communicants, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

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



located outside the United States and thus were not assessed to be wholly domestic.[20]

- Of the 5,081 MCTs, 1,682 (approximately 33%) required further, in-depth [redacted] analysis because they lacked information sufficient for NSA to readily identify the active user or determine the active user's location. In most of these cases, the transactions did not contain enough information for NSA to readily determine which electronic communication account/address/identifier appearing in the transaction was that of the active user. In other cases, NSA was able to determine which electronic communication account/address/identifier appearing in the transaction was that of the "active user," but NSA was unable to determine the active user's location. NSA's further [redacted] analysis of these 1,682 MCTs revealed:
  - For 1,220 of these 1,682 MCTs, NSA analysis of [redacted] data indicated that they were characteristic of a foreign use [redacted]
  - For 152 of these 1,682 MCTs, NSA analysis of [redacted] data indicated that they were [redacted]
  - For 86 of these 1,682 MCTs, NSA analysis of a combination of technical data and content revealed that they appeared to contain communications of persons located outside the United States (e.g., through further content analysis, NSA analysts were able to identify the active users of some MCTs and information indicative of those users' locations).
- Of the 5,081 MCTs, NSA cannot determine whether 224 MCTs contained wholly domestic communications, because these MCTs lack information sufficient for NSA to identify the active user or determine the active user's location. Nevertheless, NSA has no basis to believe any of these MCTs contain wholly domestic communications.
  - For 182 of these 224 MCTs, NSA technical analysis indicates that they were characteristic of [redacted]
  - For 1 of these 224 MCTs, NSA initially determined that it contained an electronic communication account/address/identifier of a non-targeted active user who appeared to be located in the United States, but whose location could not be determined upon further technical analysis. Specifically, [redacted]

[20] ~~(TS//SI//NF)~~ To determine the location of the other communicants, NSA performed the same sort of [redacted] analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its FAA Section 702 targeting procedures.

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



[redacted].

- 23 of these 224 MCTs were not further analyzed because, although they were present in [redacted] as of the date the sample was assembled, they were subsequently purged and/or placed on NSA's Master Purge List.
- 18 of these 224 MCTs could not be further characterized by NSA analysts.

IV. (U) Conclusions Drawn from the Random Sample

~~(TS//SI//NF)~~ Based on a random sample of the approximately 13.25 million total Internet communications acquired by NSA through "upstream" techniques pursuant to FAA section 702 for the six-month period discussed, NSA assesses that the volume of transactions containing multiple communications not all of which may be to, from, or about a tasked selector is approximately between 1.29 and 1.39 million (9.70%-10.45%).[21] With respect to the types of discrete communications contained within multi-communication transactions manually reviewed by NSA analysts, [redacted]

~~(TS//SI//NF)~~ As described in Appendix B, which details NSA's Statistical Methodology for this review, the data compiled during the above-discussed manual review of a random sample of Internet communications acquired during a six-month period can be used to characterize with a statistically high degree of confidence (i.e., a simultaneous confidence level of 95% for these intervals collectively) the nature and scope of the entirety of the approximately 13.25 million Internet communications from

[21] ~~(TS//SI//NF)~~ As calculated in the attached Appendix detailing NSA's Statistical Methodology for this review, these figures are based on the 45,359 of the 50,440 transactions (89.93%) manually reviewed by NSA analysts as containing single, discrete communications and the 5,081 transactions (10.07%) manually reviewed by NSA analysts as containing multiple communications. *See also* Step 1, *supra* page 3.

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

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

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



Wikimedia Found. v. NSA DOJ000124

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



which the random sample was drawn. Specifically, NSA assesses that of these approximately 13.25 million Internet communications acquired through NSA upstream collection:

- between approximately 11.87 and 11.97 million (89.55%-90.30%) are transactions that contain only single, discrete communications to, from, or about a tasked selector;
- between 168,853 and 206,922 (1.27%-1.56%)[25] are transactions that contain multiple communications, all of which are either to or from a tasked selector;
- between 1,042,838 and 1,113,947 (7.87%-8.53%)[26] are transactions that contain multiple communications, at least one of which is to, from, or about NSA's tasked selector, but all of which are believed to either be to or from non-targeted persons reasonably believed to be located outside the United States;
- between 48,609 and 70,168 (0.37%-0.53%)[27] are transactions that contain multiple communications, at least one of which is to, from, or about NSA's tasked selector, and at least one of which is a communication between non-targeted persons (i.e., not to, from or about a tasked selector) that lacks sufficient information for NSA to identify the location of the sender and all intended recipients of that communication; and
- between 996 and 4,965 (0.0075%-0.0375%) contain a wholly domestic communication not to, from, or about a tasked selector.

~~(TS//SI//NF)~~ In sum, while there was insufficient information present for 224 multi-communication transactions for NSA analysts to characterize the likelihood that they may contain wholly domestic communications (the majority of which were attributable to [redacted], for the reasons explained in detail

---

[25] ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 713 of the 5,081 MCTs (14.03%) and 50,440 total transactions (1.41%) reviewed by NSA analysts as containing a tasked selector as the active user [redacted]. See also Step 3, *supra* page 4.

[26] ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 4,134 of the 5,081 MCTs (81.36%) and 50,440 total transactions (8.19%) reviewed by NSA analysts as containing discrete communications believed to be to or from non-targeted persons located outside the United States. More specifically, this total includes the following MCTs manually reviewed by NSA analysts: 2,668 that had an active user reasonably believed to be a person located outside the United States; 8 that included at least one communicant reasonably believed to be located outside the United States for each communication therein; 1,220 that are characteristic o[redacted] 152 that are indicative of [redacted] and 86 that all communications contained therein were to or from persons located outside the United States. *See* Step 3, *supra* pages 4-6.

[27] ~~(TS//SI//NF)~~ As calculated in the attached Appendix, these figures are based on 224 of the 5,081 MCTs (4.41%) and 50,440 total transactions (0.44%%) reviewed by NSA analysts that lacked sufficient information to identify the active user or the active user's location. *See* Step 3, *supra* page 6.

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


above, NSA has no basis to believe any of the remaining Internet communications reviewed in the 50,440 sample are wholly domestic beyond those 10 discussed above.[28] Moreover, each of those 10 Internet communications has been placed on NSA's Master Purge List.

----- *The remainder of this page intentionally left blank.* -----

[28] ~~(TS//SI//NF)~~ *See* Figure D of Appendix A.



Wikimedia Found. v. NSA DOJ000126

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

~~TOP SECRET//COMINT//NOFORN~~

## (U) VERIFICATION

(U) I declare under penalty of perjury that the facts set forth in the foregoing "NSA Characterization of Upstream Data: Process and Results" are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 16th day of August, 2011.

[redacted]

Signals Intelligence Directorate Compliance Architect
National Security Agency



Wikimedia Found. v. NSA DOJ000127

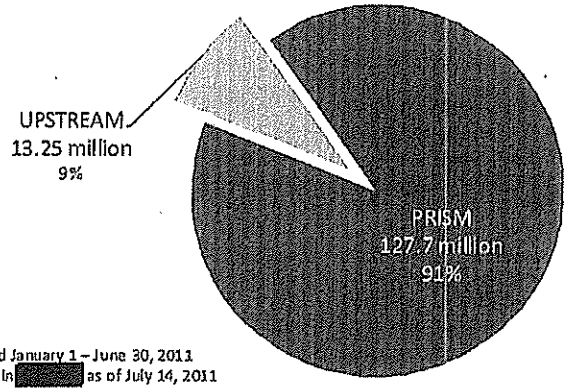
Approved for public release. All withheld information exempt under b(1) and b(3) except as otherwise noted.

~~TOP SECRET//COMINT//NOFORN~~

# Appendix A

## Fig. A Total FAA 702

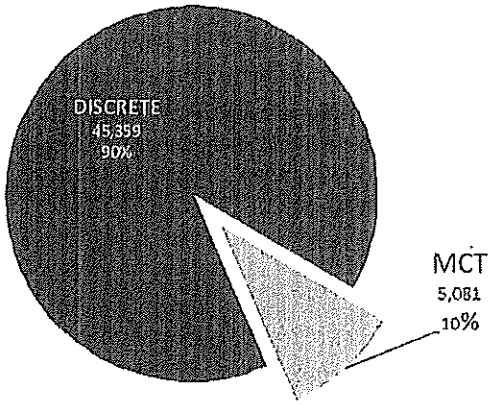
140,974,921 Internet Communications




Acquired January 1 – June 30, 2011
Present in [redacted] as of July 14, 2011

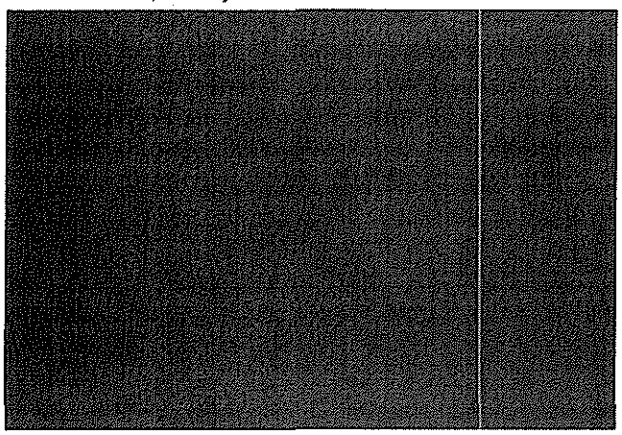
## Fig. B Total Upstream Sample

50,440 objects manually reviewed



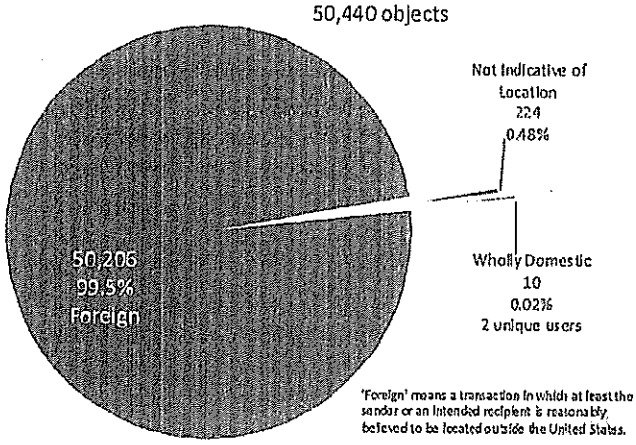

## Fig. C MCT Type

5,081 objects



## Fig. D Summary

50,440 objects




'Foreign' means a transaction in which at least the sender or an intended recipient is reasonably believed to be located outside the United States.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360801

~~TOP SECRET//COMINT//NOFORN~~

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



## Appendix B: Statistical Methodology – FAA Section 702 Upstream Manual Review

~~(TS//SI//NF)~~ Using statistical analysis NSA determined the proportions of transactions satisfying certain criteria (e.g., proportion of FAA Section 702 upstream Internet transactions that are Multi-communication Transactions (MCT) versus transactions containing single, discrete communications). As further described below, transactions were categorized in various ways. The categorization process can be complex; to minimize categorization error, NSA used a statistical approach involving actual examination of an appropriate sample of transactions by experienced intelligence analysts. (The use of only a sample is a concession to the large volume of transactions and the labor-intensive nature of the categorization process.) That is, NSA traded "categorization error" for "statistical error"; the latter refers to the fact that by considering only a randomly sampled portion of the universe of transactions, NSA estimated the true proportions (as they exist in the universe) -- with error bounds and levels of confidence that can be stated justifiably.

~~(TS//SI//NF)~~ **THE SAMPLE.** As discussed more fully in the "NSA Characterization of Upstream Data: Process and Results," NSA identified 13,256,067 transactions acquired through NSA's FAA 702 upstream collection during a six-month period from January 1st through June 30th, 2011. Of those approximately 13.25 million transactions, a team of experienced intelligence analysts carefully examined 50,440 over a nearly one-month time period. The transactions were presented to the analysts in a randomized order, ensuring that a simple random sample would serve as the basis for conclusions -- supported by statistical theory – about the true proportions of the 13.25 million-transaction universe.

~~(TS//SI//NF)~~ **ESTIMATES AND CONFIDENCE INTERVALS.** The proportions formed from the sampled transactions serve as unbiased estimates of the corresponding proportions of the 13,256,067-transaction universe. Further, for (six) selected proportions, NSA states a confidence interval for each. Collectively, these intervals have a simultaneous confidence level of 95%. This means that the intervals were produced by a procedure calibrated to produce, for at least 95% of the sample sets NSA could have drawn, intervals which all cover the corresponding true (i.e., universal) proportions. Individually, each interval has a higher level of confidence associated with it; component confidence levels are quoted below.

~~(TS//SI//NF)~~ For each of the six categories, NSA also states a confidence interval for the actual number of that category's transactions within the 13,256,067-transaction (January-June, 2011 upstream) universe. Such an interval is simply an equivalent representation of the corresponding proportion-interval (it is obtained by multiplying the endpoints of the proportion-interval by 13,256,067), and so the inclusion of such intervals does not affect the (95%) level of simultaneous confidence.

~~(TS//SI//NF)~~ Specifically: By sampling a subset of the universe (or *population*) of upstream transactions, NSA estimated the following six proportions. (Hereinafter, $N$ denotes 13,256,067 – the size of that universe; $M$ denotes the (unknown) actual number of MCTs in that universe).

- $M / N$: the proportion of the population comprising MCTs;

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20360801

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


- 1-($M/N$): the proportion of the population comprising discrete transactions;
- the proportion of the population comprising MCTs in which all communications are either to or from NSA's tasked selector (hereinafter labeled "Target" MCTs);
- the proportion of the population comprising MCTs in which all communications are believed to either be to or from non-targeted persons located outside the United States (hereinafter labeled "Foreign" MCTs);
- the proportion of the population comprising MCTs in which the nature of one or more communications between non-targeted persons lacked sufficient information for NSA analysts to identify the location of the sender and all intended recipients (hereinafter labeled "Unknownable" MCTs);
- the proportion of the population comprising MCTs that NSA analysts assessed contain a wholly domestic not to, from, or about a tasked selector (hereinafter labeled "Confirmed Wholly Domestic").

~~(TS//SI//NF)~~ (The first of these proportions equals the total of the last four.) In the following, lower-case letters denote transaction counts as realized in the sample, in categories corresponding to their upper-case counterparts. That is, $n$ is the number of transactions sampled (this turned out to be 50,440), and $m$ is the number of MCTs in the sample.

~~(TS//SI//NF)~~ **OUTLINE OF PROCEDURE.** NSA designed a procedure that accepts a size-$n$ *simple random sample*[1] of the population, and produced from it estimates and confidence intervals for the six "true"[2] proportions NSA sought. The estimates NSA produced are simply the corresponding proportions as found in the sample – e.g., the sample proportion $m/n$ was NSA's estimate of the population proportion $M/N$; such a sample proportion is unbiased[3] for its population counterpart, meaning that were a sample proportion to be computed for each of the possible size-$n$ samples that could be drawn, the average of these sample proportions would equal the "true" (population) proportion.

---

[1] ~~(TS//SI//NF)~~ A simple random sample is one that is drawn in a way that ensures that all possible size-$n$ subsets of the (size-$N$) population have an equal chance of being selected; this sampling technique enables statistically justifiable claims by avoiding potential (known or unknown) sources of bias in the population (e.g., a periodic trend in the population over time).

[2] ~~(TS//SI//NF)~~ "True" refers to proportions that relate to the entire population, which cannot be determined for certain, as $n$ is smaller than $N$.

[3] ~~(TS//SI//NF)~~ Unbiasedness means that the estimate is aiming for the right "target"; however, it indicates nothing about the precision of the estimate. An estimation procedure can be unbiased whether it is based on a small or large sample size $n$.

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


~~(TS//SI//NF)~~ To express precision appropriately, NSA designed its procedure to produce confidence intervals – one for each of the (six) population proportions of interest – having a simultaneous confidence level of 95%. This means that:

- Based on a sample, the procedure will produce a collection of intervals, each asserted to contain the true (population) proportion it targets.

- Because the procedure operates on a random sample, the interval endpoints are *random variables*; the particular collection of intervals a particular sample yields may fail to cover one or more of the population proportions it targets. But the procedure is designed so that this failure probability – *whatever* the true proportions are – is no more than 5%; that is, for at least 95% of the (size-$n$) simple random samples it might process, the procedure will produce intervals which *all* cover their targeted population proportions.

- In order to achieve this level of confidence about a collection of intervals simultaneously, the procedure is designed so that the respective failure probabilities associated with the component intervals total no more than 5%. In particular, this 5% was allocated as follows:

  - 2.5% to the proportion of "Confirmed Wholly Domestic";
  - 0.67% to each of the "Target," "Foreign," "Unknown" proportions;
  - 0.5% to the proportion of MCT (i.e., $M/N$). As the proportions of discrete and MCT transactions are complementary (i.e., they total 1), the confidence interval for the proportion of discrete transactions is obtained by subtracting each of the endpoints for the MCT-interval from 1 – and it is the case that one of these intervals will cover its population target if and only if the other does. Therefore, there is no need to separately allocate "failure probability" to the proportion-of-discrete.

~~(TS//SI//NF)~~ The probability of drawing a sample resulting in one or more "failing" intervals is no more than the sum of the failure probabilities of the respective component intervals, hence the claim of 95% confidence for the procedure outlined here. The "no more" qualification makes this technique conservative: relationships (complicated and left unanalyzed) between the random variables involved may make the practical confidence level higher; 95% represents a worst-case claim. To achieve simultaneous 95% confidence, the 5% failure probability could have been allocated in any way. (Broadly: the lower the confidence level (i.e., the higher the failure probability), the narrower the intervals the procedure will produce. An extreme example: a procedure for 100% confidence intervals would produce uselessly wide intervals, as it would have to be able to claim that its intervals cover truth for *every* possible size-$n$ sample it could have received.) This procedure for simultaneous intervals is conservative in a further way: Just as the sum of the discrete and MCT proportions equals 1, so does the sum of the discrete, "Target," "Foreign," "Unknown," and "Confirmed Wholly Domestic" proportions. It is difficult to exploit this latter constraint properly; NSA utilized the conservative method described here to ensure that its assertions about the procedure's performance are valid.



Wikimedia Found. v. NSA DOJ000131

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


~~(TS//SI//NF)~~ **CONFIDENCE-INTERVAL PROCEDURE FOR A SINGLE PROPORTION.** As outlined above, the procedure for (95%) simultaneous confidence intervals was achieved by producing component confidence intervals based on (individually higher) levels of confidence (e.g., 99.5% for $M/N$). The construction of component confidence intervals can be understood via the following example, using the $M/N$ target. For the sample of size $n$ to be observed, $m$ represents the (random) number of MCTs to be realized in the sample. Formally, $m$ has a *hypergeometric* distribution (arising from sampling transactions "without replacement"); to make the mathematical computations tractable, NSA approximated this distribution by a *binomial* distribution corresponding to sampling *with* replacement (in which each sampled transaction would be replaced after it is drawn, and hence would be eligible to be drawn multiple times). This approximation is uniformly conservative; i.e., it will result in wider intervals. The proportion to be estimated, $M/N$, appears as the (unknown) parameter (now denoted $p$) of this binomial distribution. Treating $m$ as a binomial random variable based on $n$ *trials*, NSA used an accepted method (the *Clopper-Pearson* method) as the basis to devise its confidence-interval procedure for $p$. (Below, the notation $B(n,q)$ refers to an $n$-trial binomial random variable having parameter $q$.) Upon observing $m$, NSA:

- Determines, for each of various proportions $x$ between 0 and 0.5%, parameters $q$ and $r$ such that
  - $x$ is the probability that a $B(n,q)$ random variable takes a value of at least $m$ (but if $m$=0, take $q$ to be 0);
  - (0.5% - $x$) is the probability that a $B(n,r)$ random variable takes a value no larger than $m$ (but if $m$=$n$, take $r$ to be 1).

  $r$ exceeds $q$; the pair $[q,r]$ determines an interval.

- Determines the narrowest of all such intervals $[q,r]$ and reports it as the (99.5%) confidence interval for $p = M/N$.

~~(TS//SI//NF)~~ Practically, the $q$'s and $r$'s can be computed using *inverse Beta functions*, and computer software can find the narrowest interval efficiently.

*Remainder of this page intentionally left blank.*



Wikimedia Found. v. NSA DOJ000132

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


RESULTS:

| | # of transactions in sample | Sample proportion (of 702 upstream) | Confidence interval for corresponding universal proportion | Confidence interval for the actual number (of the 13.25 million) |
|---|---|---|---|---|
| **Discrete** | 45,359 | 0.8993 | 0.8955 – 0.9030 | 11,870,284 – 11,970,275 |
| **MCT** | 5,081 | 0.1007 | 0.0970 – 0.1045 | 1,285,792 – 1,385,783 |

| | # of transactions in sample | Sample proportion (of MCT) | Confidence interval for corresponding universal (MCT) proportion | Confidence interval for the actual number (of the 13.25 million) |
|---|---|---|---|---|
| **TARGET** | 713 | 0.01414 | 0.01274 – 0.01561 | 168,853 – 206,922 |
| **FOREIGN** | 4,134 | 0.08196 | 0.07867 – 0.08532 | 1,042,838 – 1,130,947 |
| **UNKNOWABLE** | 224 | 0.004441 | 0.003667 – 0.005293 | 48,609 – 70,168 |
| **CONFIRMED WHOLLY DOMESTIC** | 10 | 0.0001983 | 0.00007508 – 0.0003746 | 996 – 4,965 |

[redacted]

*Remainder of this page intentionally left blank.*

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



VERIFICATION

I declare under penalty of perjury that the facts set forth in this Appendix are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, Section 1746, on this 11th day of August, 2011.



[Statistician]
National Security Agency

DECLARATION OF SCOTT BRADNER

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

# Appendix O

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

**JOINT STATEMENT OF**

**LISA O. MONACO**
**ASSISTANT ATTORNEY GENERAL**
**FOR NATIONAL SECURITY**
**U.S. DEPARTMENT OF JUSTICE**

**JOHN C. (CHRIS) INGLIS**
**DEPUTY DIRECTOR**
**NATIONAL SECURITY AGENCY**

**ROBERT S. LITT**
**GENERAL COUNSEL**
**OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE**

**BEFORE THE**
**PERMANENT SELECT COMMITTEE ON INTELLIGENCE**
**UNITED STATES HOUSE OF REPRESENTATIVES**

**AT A HEARING CONCERNING**
**"FISA AMENDMENTS ACT REAUTHORIZATION"**

**PRESENTED ON**
**DECEMBER 8, 2011**

[redacted]

**Joint Statement of**

**Lisa O. Monaco**
**Assistant Attorney General**
**for National Security**
**U.S. Department of Justice**

**John C. (Chris) Inglis**
**Deputy Director**
**National Security Agency**

**Robert S. Litt**
**General Counsel**
**Office of Director of National Intelligence**

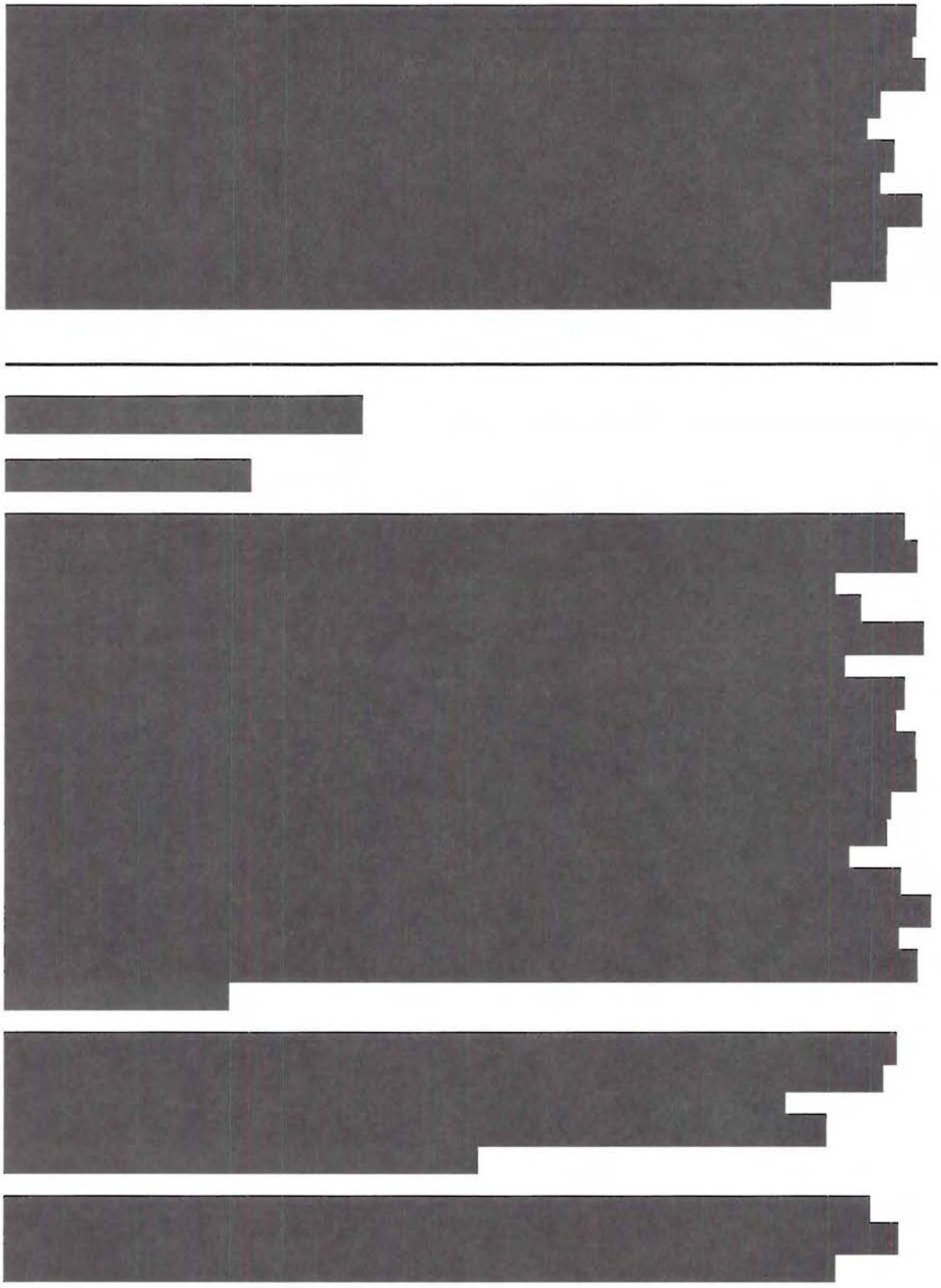
**Before the**
**Permanent Select Committee on Intelligence**
**United States House of Representatives**

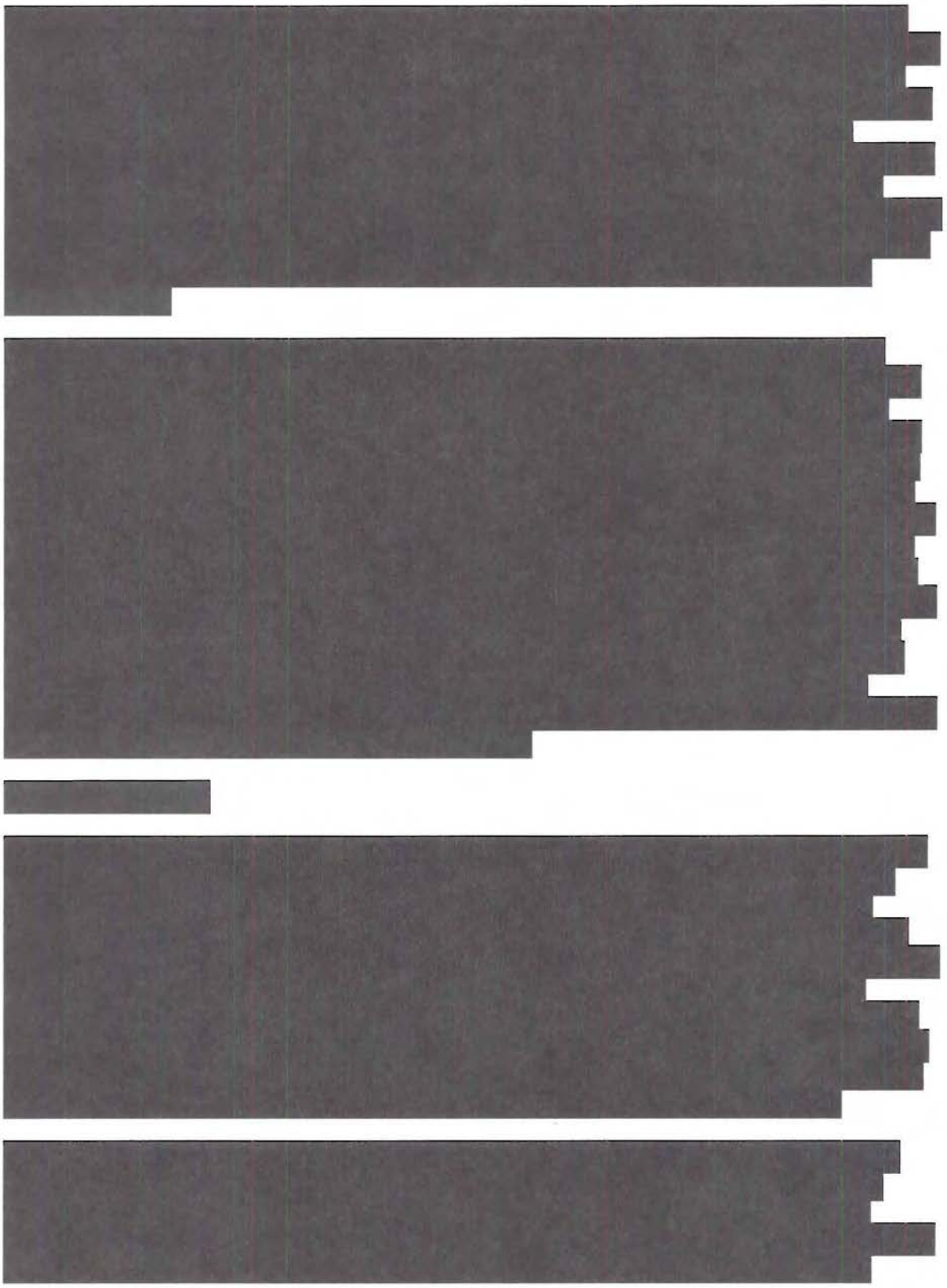
**At a Hearing Concerning**
**"FISA Amendments Act Reauthorization"**

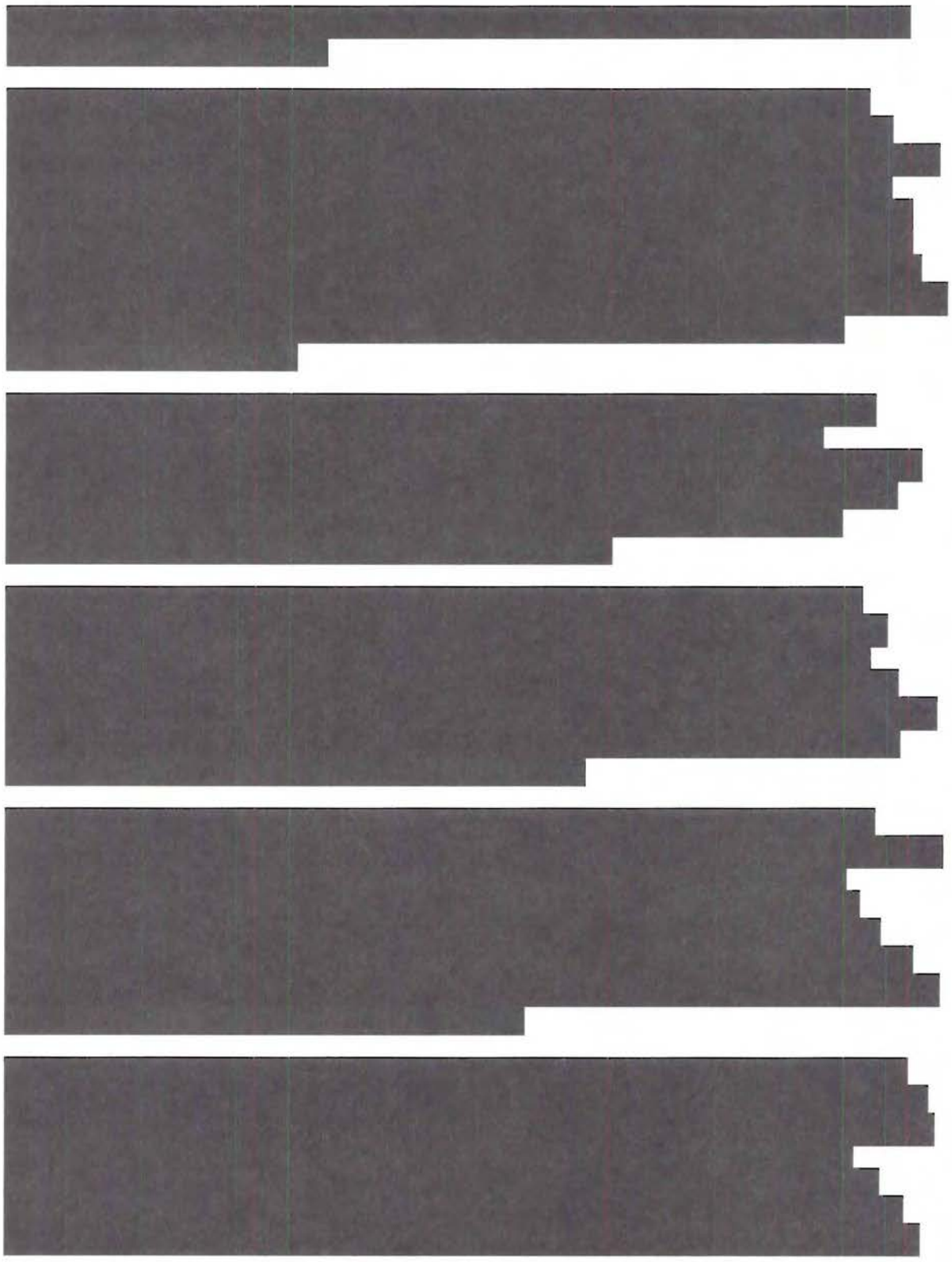
**Presented on**
**December 8, 2011**

---

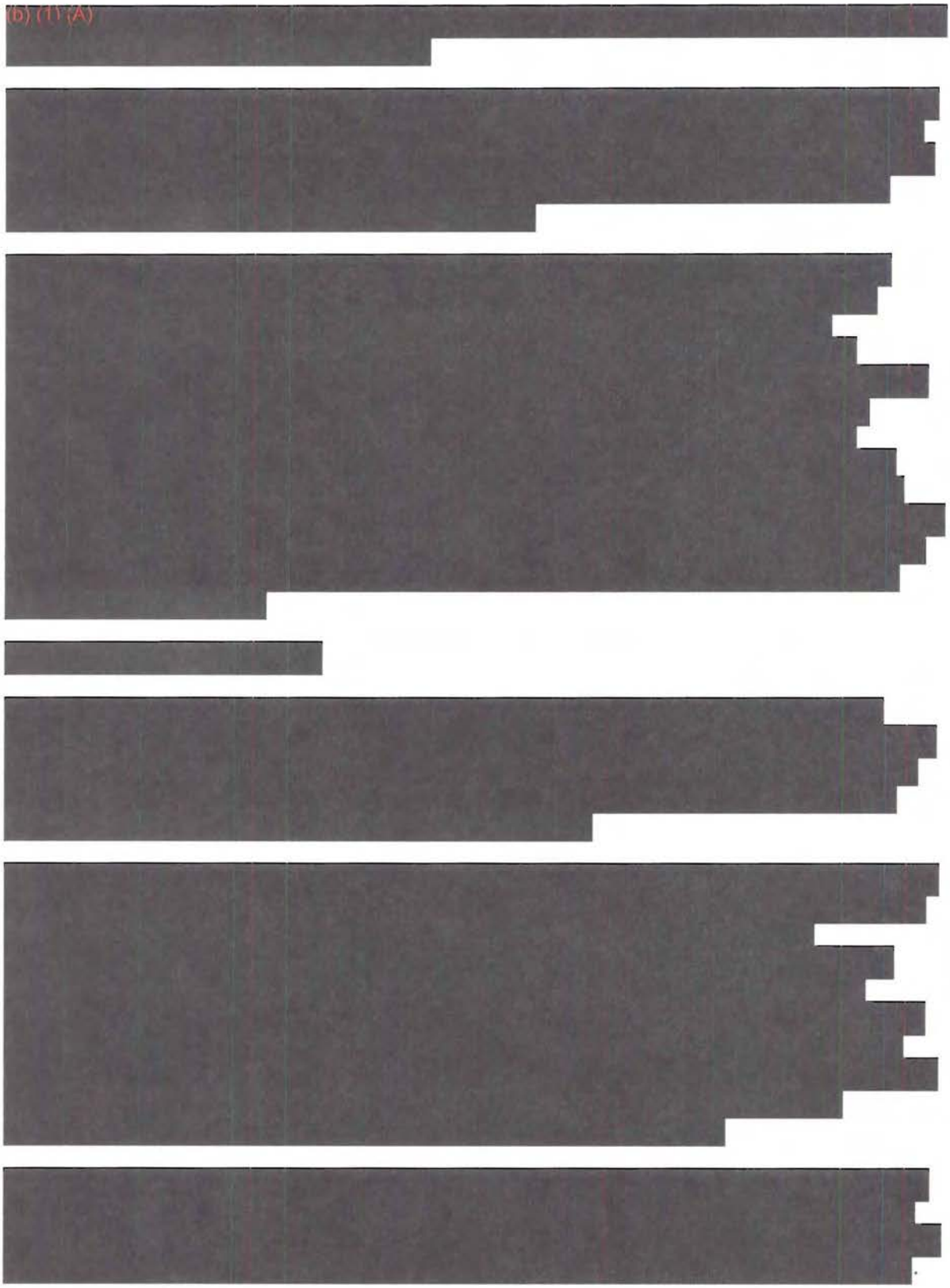
[redacted]

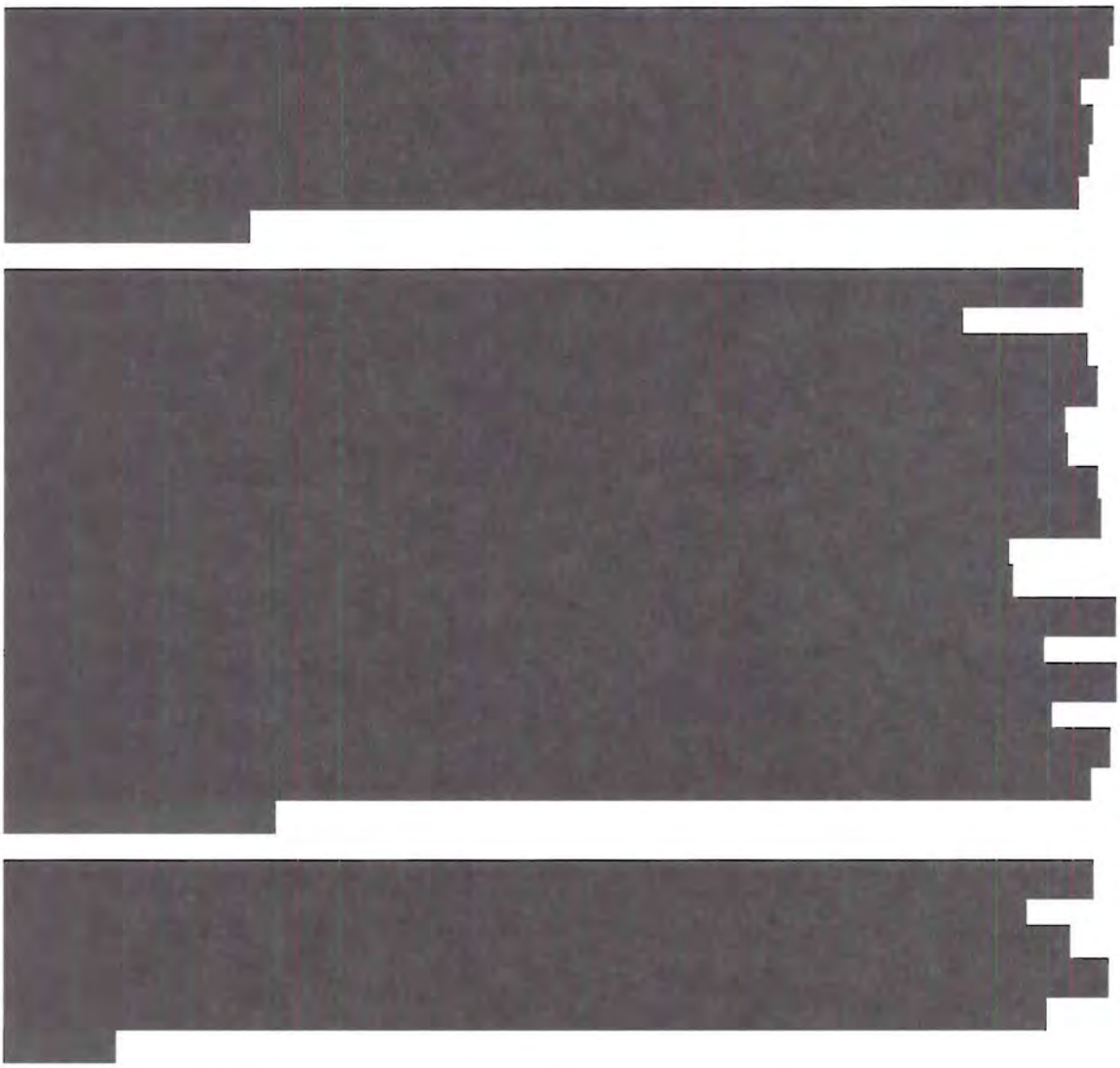






(b) (1) (A)





(U) **Recent FISC Opinion**

~~(TS//SI//NF)~~ On October 3, 2011, the FISC issued an opinion addressing the Government's submission of replacement certifications under section 702. *In re DNI/AG Certification 2009-C, et. al.,* [redacted], Mem. Op. The FISC approved most of the Government's submission. It upheld NSA's and FBI's targeting procedures, CIA's and FBI's minimization procedures, and most of NSA's minimization procedures. Nevertheless, the FISC denied in part the Government's requests because of its concerns about the rules governing the retention of certain non-targeted Internet communications acquired through NSA's upstream collection. The FISC's exhaustive analysis of the Government's submission, like its other decisions, refutes any argument that the court is a "rubber stamp," and demonstrates the rigorous nature of the oversight it conducts.

~~(TS//SI//NF)~~ As described above, upstream collection allows NSA to acquire, among other things, communications about a target where the target is not itself a communicant. In doing so, NSA uses [redacted] that are reasonably designed to screen out communications that are wholly domestic in nature, in accordance with section 702's requirements. Although reasonably designed to accomplish this result, [redacted] are not perfect. In addition, upstream collection devices acquire Internet "transactions" that include tasked selectors. Such a transaction may consist of a single communication (a "single-communication transaction," or SCT) or multiple communications sent in a single transaction (a "multi-communication transaction," or MCT) [redacted] In such instances, upstream collection acquires the entire MCT, which in all cases will include a communication to, from, or about a tasked selector but in some cases may also include communications that are not about a tasked selector and may have no relationship, or no more than an incidental relationship, to the targeted selector. Thus although upstream collection only targets Internet communications that are not between individuals located in the United States and are to, from, or about a tasked account, there is some inevitable incidental collection of wholly domestic communications or communications not to, from, or about a tasked account that could contain U.S. person information. Based on a sample reviewed by NSA, the percentage of such communications is very small (about .02%), but given the volume of the upstream collection, the FISC concluded that the actual number of such communications may be in the tens of thousands annually.

~~(TS//SI//NF)~~ The FISC upheld NSA's continued upstream acquisition of Internet communications under section 702 even though it includes the unintentional acquisition of wholly domestic communications and the incidental acquisition of MCTs that may contain one or more individual communications that are not to, from, or about the tasked selector. *See id.* at 74, 78-79. The FISC also reaffirmed that the acquisition of foreign intelligence information under section 702 falls within the foreign intelligence exception to the warrant requirement of the Fourth Amendment, and confirmed that nothing had disturbed its "prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA's targeting and minimization procedures." *Id.* at 69.

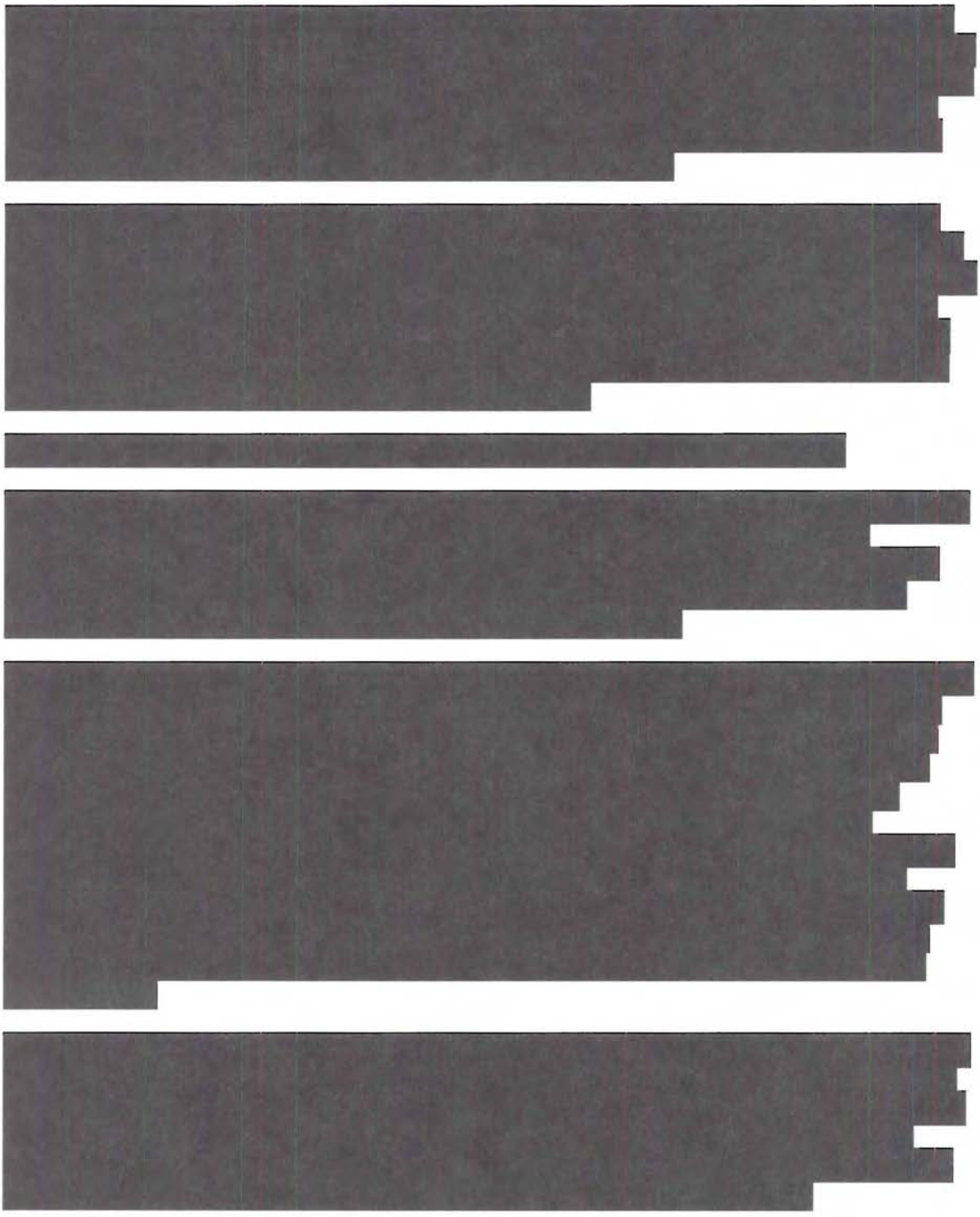
~~(TS//SI//NF)~~ The FISC determined, however, that the minimization procedures governing *retention* of MCTs were inconsistent with the requirements of section 702. The FISC found that the Government had not fully explored options regarding data retention that would be more protective of U.S. persons, and that the FISC thus could not determine that the Government's minimization procedures satisfied FISA's requirement that such procedures be "reasonably designed" to minimize the retention of protected U.S. person information. The FISC further held that, although the Fourth Amendment's warrant requirement was not implicated, in light of NSA's proposed procedures for handling MCTs, NSA's proposed acquisition and minimization procedures did not satisfy the Fourth Amendment's reasonableness requirement. The FISC recognized, however, that the Government may be able to "tailor the scope of NSA's upstream collection, or adopt more stringent post-acquisition safeguards, in a manner that would satisfy the reasonableness requirement of the Fourth Amendment," and suggested a number of possibilities as to how this might be done. *Id.* at 61-63, 78-80.

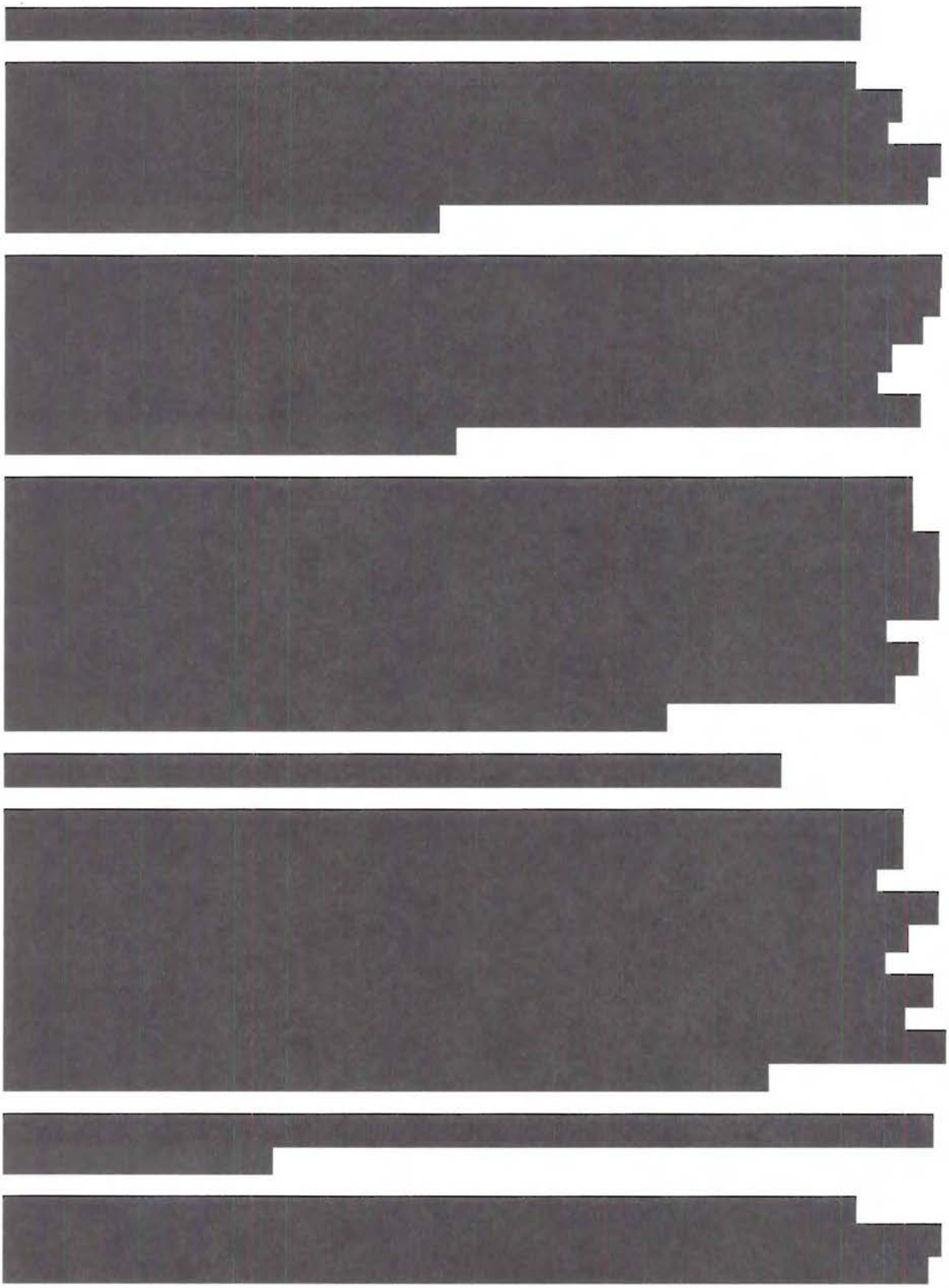
~~(TS//SI//NF)~~ On October 31, 2011, after extensive consultations among the Department, ODNI, and NSA, the Attorney General submitted amended minimization procedures to the FISC addressing the deficiencies noted by the court. These amended procedures continue to allow for the upstream collection of MCTs; however, they also create more rigorous rules governing the retention of MCTs as well as NSA analysts' exposure to, and use of, non-targeted communications. On balance, NSA believes that the impact of these procedures on operations is acceptable as a necessary requirement in order to continue upstream collection, and that these procedures will allow for continued useful intelligence collection and analysis. On November 30, the FISC granted the Government's request for approval of the amended procedures, stating that, with regard to information acquired pursuant to 2011 certifications, "the government has adequately corrected the deficiencies identified in the October 3 Opinion," and that the amended procedures, when "viewed as a whole, meet the applicable statutory and constitutional requirements."

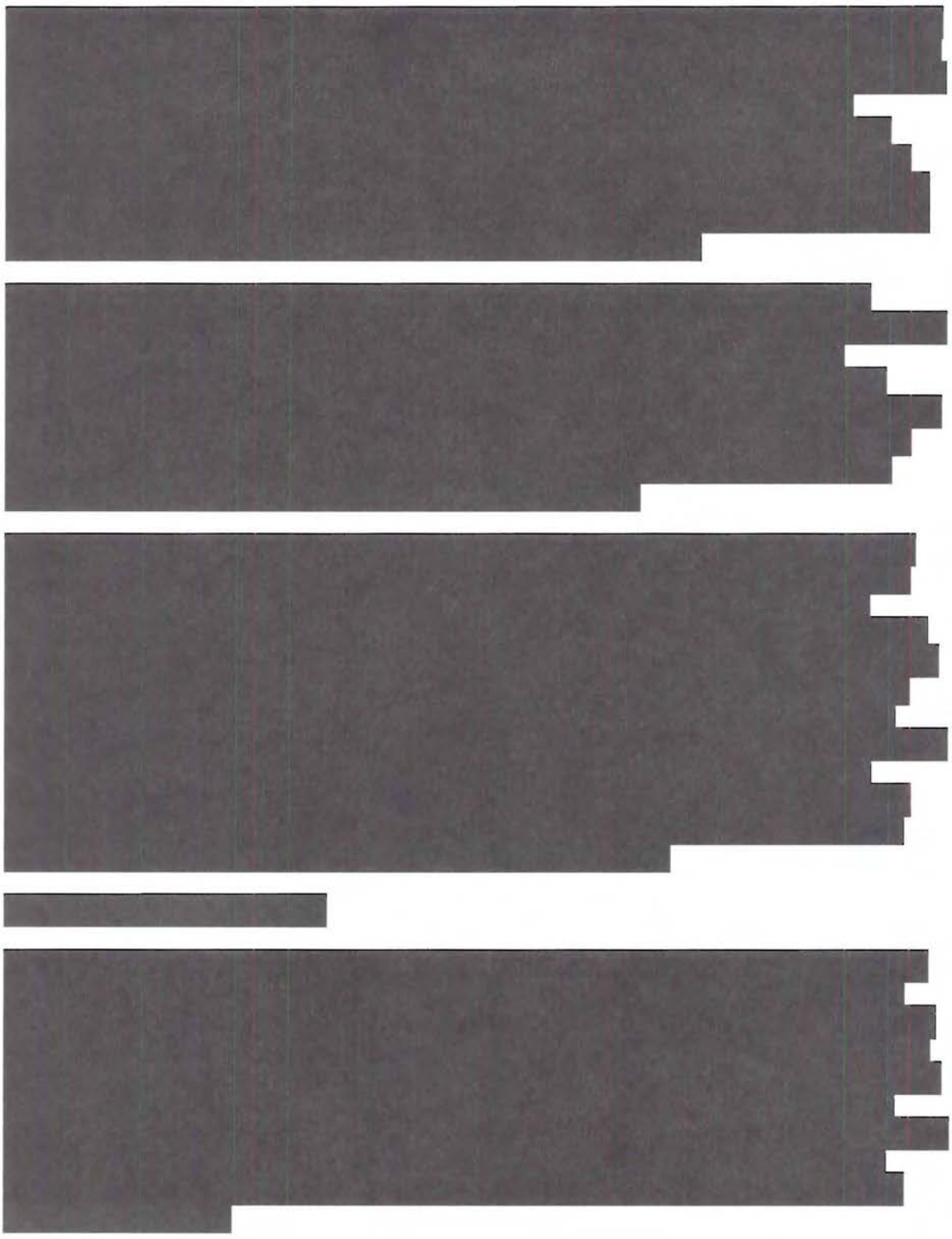
(U) The Government has provided copies of the opinions and the filings by the Government to this Committee, and the Government will continue to inform the Committee about developments in this matter.

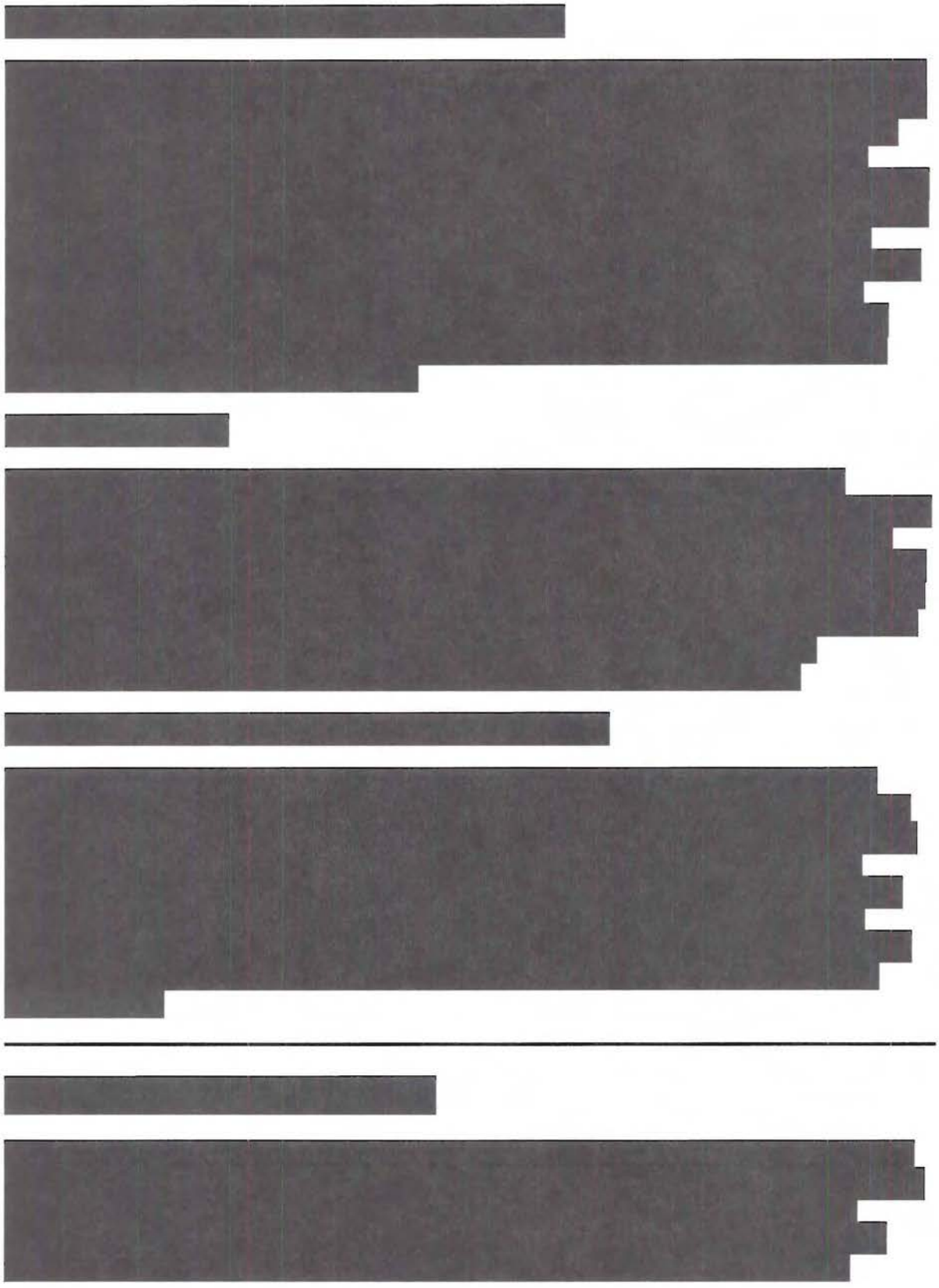
---

[redacted]

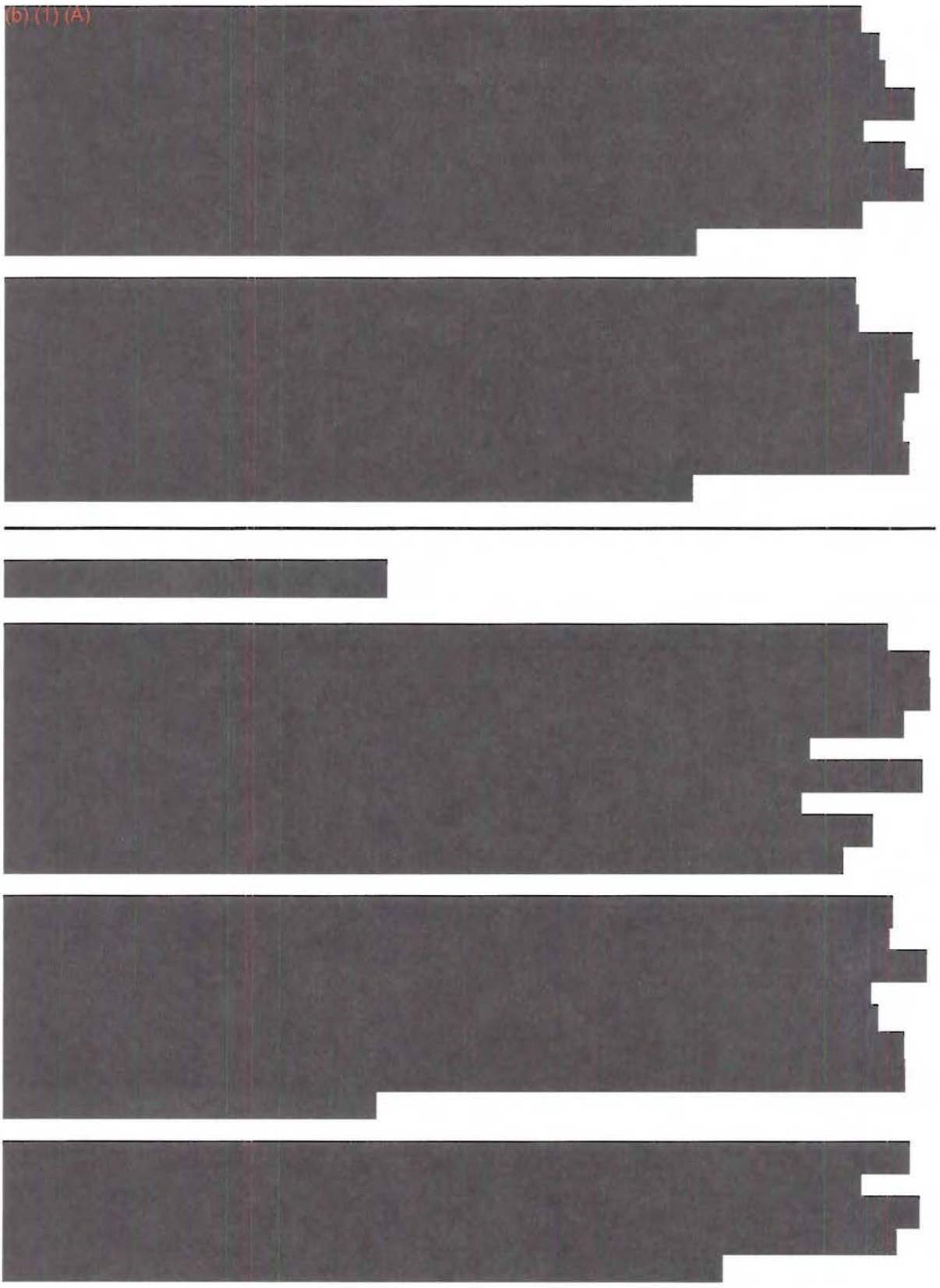


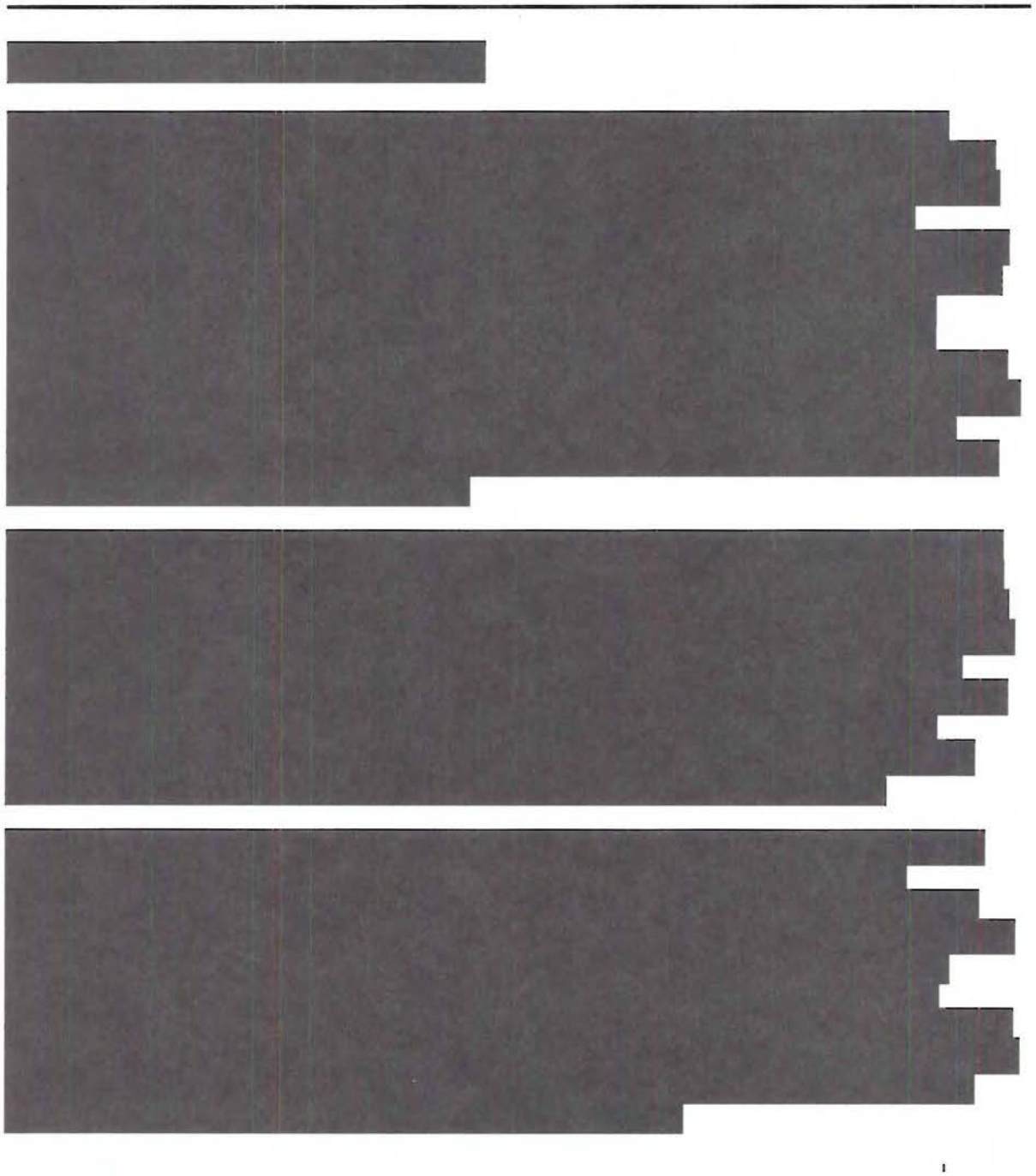






(b) (1) (A)





DECLARATION OF SCOTT BRADNER

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

# Appendix P

This document was also filed as ECF No. 168-20 and can be found in this Joint Appendix at JA2631.

DECLARATION OF SCOTT BRADNER

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

# Appendix Q

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

The public hearing was held at the Renaissance Mayflower Hotel, 1127 Connecticut Avenue NW, Washington, D.C. 20036 commencing at 9:00 a.m.

Reported by: Lynne Livingston

BOARD MEMBERS

David Medine, Chairman
Rachel Brand
Patricia Wald
James Dempsey
Elizabeth Collins Cook

PANEL I

Government Perspective on Section 702 Foreign Intelligence Surveillance Act

James A. Baker, General Counsel, Federal Bureau of Investigations
Rajesh De, General Counsel, National Security Agency
Robert Litt, General Counsel, Office of the Director of National Intelligence
Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, Department of Justice

PANEL II

Legal Issues with 702

Foreign Intelligence Surveillance Act

Laura Donohue, Professor of Law, Georgetown University Law School

Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union

Julian Ku, Professor of Law, Hofstra University

Rachel Levinson-Waldman, Counsel, Liberty and National Security Program, Brennan Center for Justice

PANEL III

Transnational and Policy Issues

John Bellinger, Partner, Arnold and Porter

Dean C. Garfield, President and CEO, Information Technology Industry Council

Laura Pitter, Senior National Security Researcher, Human Rights Watch

Ulrich Sieber, Director, Max Planck Institute for Foreign and International Criminal Law, Germany

Christopher Wolf, Partner, Hogan Lovells

PROCEEDINGS

MR. MEDINE: Good morning. Welcome to the Privacy and Civil Liberties Oversight Board's hearing on the 702 Program.

I'm David Medine, PCLOB's chairman. It's 9:05 a.m. on March 19th, 2014 and we are in the grand ballroom of the Mayflower Hotel located at 1127 Connecticut Avenue, NW, Washington, D.C.

This hearing was announced in the Federal Register on March 10th, 2014. As chairman, I will be the presiding officer.

All five Board members are present and there is a quorum. The Board members are Rachel Brand, Elisebeth Collins Cook, James Dempsey, and Patricia Wald.

I will now call the hearing to order. All in favor of opening the hearing please say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous consent to proceed, we will now proceed.

I want to thank the many panelists who

will be participating in today's hearing for agreeing to share their views with the Board.

I also wanted to thank the Board's staff, Sharon Bradford Franklin, Sue Reingold, Peter Winn, Diane Janosek, Brian Frazelle, and Simone Awang for their efforts in making this event possible.

Last year PCLOB agreed to provide the President and Congress a public report on two federal counterterrorism programs, the Section 215 program under the USA PATRIOT Act and the 702 program under the FISA Amendments Act. The report on the 215 program was issued on January 23rd, 2014.

Our focus today will be on the Section 702 program under the FISA Amendments Act. The purpose of this hearing is to foster a public discussion of legal, constitutional, and policy issues relating to this program.

A few ground rules for today, we expect that the discussion will be based on unclassified or declassified information, however some of the

discussion will inevitably touch on leaked classified documents or media reports of classified information.

In order to promote a robust discussion speakers may choose to reference these documents or information, but they should keep in mind that in some cases they remain classified. Therefore, while discussing them, neither the Board members nor speakers in a position to do so will confirm the validity of the documents or information.

There will be three panels today. The first will consist of government officials whose agencies have varying degrees of responsibility for the surveillance programs that will be the subject of our report.

The second panel with consist of academics and advocates who will focus on legal issues, including statutory and constitutional issues. After the first two panels we will be taking a lunch break.

The final panel will consist of a mix of academics, advocates, and private sector

representatives and will focus on transnational and policy issues.

Board members will each pose questions during each panel with questions in rounds for each Board member. Panelists are urged to keep their responses brief and to permit the greatest exchange of views.

The program is being recorded and a transcript will be posted on PCLOB.gov. Written comments from members of the public are welcome and may be submitted online at regulations.gov or by mail until March 28th.

Today's hearing will focus on the government's collection of foreign intelligence information from electronic communication service providers under court supervision pursuant to Section 702 of the Foreign Intelligence Surveillance Act.

Information is obtained with FISA court approval based on written directives from the Attorney General and the Director of National Intelligence to acquire foreign intelligence

information. This law permits the government to target non-U.S. persons, someone who is not a citizen or a permanent resident alien, located outside the United States for foreign intelligence purposes without obtaining a specific warrant for each target.

We will now turn to our first panel, and I understand that Bob Litt will be making an opening statement for the panel.

MR. LITT: Thank you, and thank you for the opportunity to appear on behalf of the whole group here and talk about Section 702.

I would like to give a brief overview of Section 702 to set the stage, and we'll be glad to fill out some of the points I make here in response to questions.

Section 702, as you noted, enables us to collect intelligence against foreign targets who are outside of the United States while robustly protecting privacy rights.

Under Section 702 the FISA court approves annual certifications submitted by the

Attorney General and the Director of National Intelligence that identify categories of foreign intelligence that may be collected. We then target selectors such as telephone numbers or email addresses that will produce foreign intelligence falling within the scope of the certifications.

The FISA court also has to review and approve targeting and minimization procedures. The targeting procedures ensure that we target only non-U.S. persons who are reasonably believed to be outside of the United States, that we do not intentionally intercept totally domestic communications, and that we do not target any person outside of the United States as a subterfuge to actually target someone inside the U.S.

The minimization procedures ensure that consistent with foreign intelligence needs, we minimize the acquisition and retention of non-public information available about U.S. persons and that we prohibit the dissemination of

such information.

I want to make a couple of important overview points about Section 702. First, there is either a misconception or a mischaracterization commonly repeated that Section 702 is a form of bulk collection. It is not bulk collection. It is targeted collection based on selectors such as telephone numbers or email addresses where there's reason to believe that the selector is relevant to a foreign intelligence purpose.

I just want to repeat that Section 702 is not a bulk collection program.

Second, from a legal point of view persons who are not U.S. persons and who are outside of the United States do not have rights under the Fourth Amendment and so the Constitution doesn't require individualized warrants to target them.

In fact, the type of intelligence that is covered by Section 702 targeting foreigners outside of the United States has historically been viewed as part of the President's inherent

constitutional authority and I'm not aware of any other country that brings this kind of collection under this sort of judicial process.

Third, collection under 702 is subject to extensive oversight by all three branches of government. We can explain the oversight in more detail later, but it includes extensive review of collection activities under Section 702 by inspectors general, by the Department of Justice, and the Office of the Director of National Intelligence. It includes reporting of all compliance incidents to the Foreign Intelligence Surveillance Court, and it includes periodic reports both to Congress and to the court.

As the documents that we've declassified and released make clear, the Foreign Intelligence Surveillance Court carefully scrutinizes our activities under this section. And while there have been a number of compliance incidents over the years, the court has never found any intentional efforts to violate the requirements of Section 702.

Fourth, the fact that the communications of U.S. persons may be incidentally intercepted when we target valid foreign intelligence targets is neither unexpected nor unique to Section 702 collection.

Both the statute itself with its required minimization procedures and the legislative history make completely clear that Congress knew full well when it passed Section 702 that incidental collection of communications of U.S. persons would occur when they're in communication with valid foreign targets.

And it's important to note that this kind of incidental collection occurs all the time in other contexts. When we conduct a criminal wiretap or a wiretap pursuant to Title I of FISA we will likely intercept communications of persons who are not targets. When we seize someone's computer we may find communications with persons who are not targets.

The minimization rules under Section 702 which the FISA court approves is consistent

with both the statute and the Fourth Amendment are designed to protect the privacy of persons whose communications are incidentally collected, while still allowing the use of information that is lawfully collected for valid foreign intelligence and law enforcement purposes.

Finally, I want to close by just emphasizing that Section 702 is one of the most valuable collection tools that we have. Many of the specific achievements of Section 702 have to remain classified so that we aren't revealing exactly who we're targeting and what we're collecting. But it is one of our most important sources of information, not only about terrorism but about a wide variety of other threats to our nation.

And unless one of my colleagues has something to add, I think we're ready to address your questions.

MR. MEDINE: Great, thank you very much for that statement.

I wanted to start off and pick up with

your discussion of incidental collection, and again just to make clear that under this program, even though the target may be a non-U.S. person there will be times when the conversations, either by email or telephone, the person on the other end will be a U.S. person.

And so my question to the panel is whether because you're gathering communications of U.S. persons if that implicates Fourth Amendment concerns? And if so, do you believe there's a foreign intelligence exception to the Fourth Amendment? And if not, how is warrantless collection of information of U.S. persons permissible?

And then to follow up on Mr. Litt's comment analogizing this to a traditional wiretap, is there a distinction here where on a traditional wiretap the court has, there's been a judicial determination with particularity of a particular collection, whereas here there's only broad programmatic court approval and not approval of the specific collection?

So I guess broadly speaking, can you address the Fourth Amendment concerns regarding incidental collection?

MR. WIEGMANN: Sure, I'll take that. So this is, as Bob said, collection that is targeting non-U.S. persons overseas who don't enjoy Fourth Amendment rights under controlling Supreme Court precedent. So that affects the Fourth Amendment analysis.

That's not to say that U.S. persons whose information is or whose communications are collected incidentally doesn't trigger a Fourth Amendment review. It does. Those people still have Fourth Amendment rights, but what the courts have said is that, what the FISA court has said is that the minimization procedures that are in place render that collection reasonable from a Fourth Amendment perspective.

We think there's an exception to the warrant requirement. Before FISA was enacted in the 1970s a number of courts held in a number of different circuits that there is a foreign

intelligence exception to the warrant requirement under the Fourth Amendment, in light of the special needs of the government to collect foreign intelligence, weighed against the privacy interests of U.S. persons concluded that you don't need a warrant when you're engaged in foreign intelligence collection.

So then the only remaining question is, is it reasonable under the Fourth Amendment to collect information on U.S. persons incidentally when you're targeting non-U.S. persons. And what the FISA court has held is that it is reasonable in light of the minimization targeting procedures that we have in place. So I don't know if that answers your question, but.

So the way you look at it is the warrant requirements not applicable to foreign intelligence collection still have a reasonableness requirement with respect to incidentally collected U.S. persons, and that in fact, it is reasonable in light of the procedures that we have that are designed to ensure that we

are targeting only non-U.S. persons.

MR. MEDINE: And could you address why the minimization procedures make it a reasonable form of collection under the Fourth Amendment?

MR. WIEGMANN: Yes, so the minimization procedures address, and the targeting procedures address the acquisition, retention, and dissemination of U.S. person information.

And so those procedures all are designed to protect those U.S. persons whose information might be incidentally collected.

So for example, you can only disseminate information about a U.S. person if it is foreign intelligence, or necessary to understand foreign intelligence, or is evidence of a crime.

You have retention rules. I believe in some cases, for NSA for example, you have a five year retention limit on how long the information can be retained. And so these are procedures that the courts have found protect U.S. privacy and make the collection reasonable for Fourth

Amendment purposes.

MR. MEDINE: And under the minimization procedures I understand that the agency, the NSA, FBI, the CIA have their own minimization procedures and they're not the same with each other?

MR. WIEGMANN: That's right.

MR. MEDINE: Can you address why that shouldn't be a concern that this information is not being subjected to the same minimization standards?

MR. WIEGMANN: So each of them have their own minimization procedures based on their unique mission, and the court reviews each of those for CIA, FBI, NSA, and it's found them all reasonable for each different agency. They're slightly different based on the operational needs, but they're similar.

MR. MEDINE: Would it make more sense then if the same set of minimization procedures apply across the board for this kind of information?

MR. WIEGMANN: I don't think. Again, just to contrast, for example, FBI and NSA that are using information in different ways. The FBI has a little more latitude with respect to U.S. person information in terms of criminal activity and evidence of a crime than NSA, which doesn't have that law enforcement mission. So I think it is important to have some differences between the agencies in terms of how they handle the information.

MR. MEDINE: And is it the practice that all information that's collected under 702 is subject to the minimization procedures?

Some questions I think have been raised in some of the comments that were submitted as to whether address books or other information would be considered communications that would be subject to minimization, or is it the approach that all information collected under 702 is subject to minimization?

MR. WIEGMANN: All U.S. person information is subject to minimization procedures.

MR. MEDINE: I think my time is up.

MS. BRAND: First of all, thanks to all of you for being here this morning. We appreciate your taking the time and making yourselves available.

I want to continue on the Fourth Amendment discussion. Could one of you explain the process both inside the executive branch and then with the court of conducting the Fourth Amendment analysis and seeking the court's approval of the Fourth Amendment analysis and what kinds of opinions on the Fourth Amendment you've had from the court, to the extent that you can talk about it. Help us to understand how that works.

MR. WIEGMANN: So, you know, the FISA court operates a little bit differently than a regular court in the sense that it's ex parte, but. So that means only the government is there. There's not a party on the other side.

But other than that, we are briefing the legal issues in much the same way as we would

in a regular proceeding where there is a party on the other side. So we have an obligation to persuade the court that the collection under 702 is lawful, that it complies with the Fourth Amendment, and as I just explained to the chair, that minimization procedures comply with the Fourth Amendment.

So we would brief that issue explaining the Fourth Amendment procedures, and the court issues opinions and has issued opinions going through the Fourth Amendment analysis and finding that 702 collection, including the minimization targeting procedures meets the Fourth Amendment standards. So it's a full-up kind of regular legal briefing on that.

MR. LITT: And if I could just add something to that, it is typical in matters that involve the collection of evidence for these proceedings to be conducted ex parte. Wiretap or search warrant applications are also all done ex parte, even if they happen to present significant legal issues. So this is nothing novel in terms

of the approach that's taken there.

MR. DE: And if I could have one point. So in addition to what Brad was articulating, the court reviews this at least annually, the Fourth Amendment analysis.

As you all know, the 702 process requires annual certification. As part of that certification process every year the minimization and targeting procedures for the various agencies are submitted to the FISC, which by statute has to conduct a Fourth Amendment analysis on those procedures as part of that annual review process.

MS. BRAND: So the Fourth Amendment analysis is once a year of the program overall?

MR. DE: Well, the court has consistent jurisdiction over the program all year. The point I was making is that as part of the annual certification process, by statute the court is required to do a Fourth Amendment analysis of the annual, of the procedures that are submitted annually.

MR. BAKER: It gets evaluated at least

once a year.

MS. BRAND: Can you elaborate on that? What would there be in addition to that once a year analysis?

MR. DE: There could be a variety of factors. There could be a need to change procedures in the year, so that would prompt another analysis. I don't believe we've done that but that could be one circumstance.

There could be a variety of compliance matters that raise particular concerns to the court, in which case the court may want to do a review off-cycle.

So I think we wouldn't presume and say it only had to be once a year, but at a minimum by statute it needs to be once a year.

MS. BRAND: Okay. Bob, you talked about 702 not being bulk collection. I'd like to delve into that a little bit more, it's not bulk collection. You talked about selectors. We need to elaborate on that a little bit, I think. What is it? It's not bulk you say, but what is it?

MR. LITT: Sure. Well, I think it's probably helpful to talk about what bulk collection is first of all.

And if you look at the President's policy directive there's a definition. I don't have it in front of me, but it's essentially bulk collection is collection of communications without relying on some sort of discriminant to ensure that you're targeting particular collection.

It's sort of viewed sort of more informally, it's getting a whole bunch of communications, hanging onto them and then figuring out later what you want.

This is not that. This is a situation where we figure out what we want and we get that specifically. And so that's why it is targeted collection rather than bulk collection. Is that helpful?

MS. BRAND: But I'd like to get a little bit more into what is it that you're getting. So you have a selector, I mean.

MR. LITT: Sure. So Raj probably can

talk to this a little better than I can.

MR. DE: So if I could, I'd step back and just talk about the different types of collection under Section 702, which I think is a necessary predicate to understand how collection occurs.

So there's two types of collection under Section 702. Both are targeted, as Bob was saying, which means they are both selector-based, and I'll get into some more detail about what that means. Selectors are things like phone numbers and email addresses.

Both are affected by compulsory legal process, both types are conducted with the assistance of electronic communication service providers, and both types of collection under 702 are subject to the same statutory standards, so just as a predicate.

The first type is what's now been come to be known as PRISM collection, so just using that shorthand for a moment. And under this type of collection, communications to or from specific

selectors, again, things like phone numbers or emails, are provided with the assistance of ISPs pursuant to directives.

The second type of collection is the shorthand referred to as upstream collection. Upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers.

It is also however selector-based, i.e. based on particular phone numbers or emails, things like phone numbers or emails. This is collection to, from, or about selectors, the same selectors that are used in PRISM selection. This is not collection based on key words, for example.

This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.

But given the unique nature of upstream collection there are different minimization procedures that apply, to get to the chair's question earlier.

The reason procedures aren't always the same for different types of collection, as Brad articulated, is that there are both different mission interests and different privacy interests at stake.

MS. BRAND: I see my time is up, so.

MS. COLLINS COOK: Thank you for coming here this morning. We really appreciate your time on this and happy to be a part of this dialogue here.

I wanted to follow up on a couple of points that have already been raised, but first, we've talked about the Fourth Amendment implications of the collection. We've also talked about the fact that, or it is known that the information that's collected can subsequently be queried.

Do you consider that subsequent query a search for the purposes of the Fourth Amendment? And if not, why not?

MR. WIEGMANN: No, I would say that the search occurs at the time that the collection

occurs. So when the information, as Raj just explained, from a particular selector is acquired by NSA, then that's the time at which the search occurs.

Once you've lawfully collected that information, subsequently querying that information isn't a search under the Fourth Amendment, it's information already in the government's custody. And so I don't think there are any other contexts really in general in which a warrant is required to search information already in your custody.

MS. COLLINS COOK: Following up on that, I think some have suggested that whether as a matter of Fourth Amendment necessity or as a policy, as a matter of policy that you should seek court approval before doing a query of a U.S. person identifier.

Can you talk a little bit about what the operational impact of such a requirement might be?

MR. WIEGMANN: Sure, and this is

something I guess some of my colleagues could talk about the operational impact. But as I said, in general with other types of collection, whether it's collection under Title I of FISA, which is your regular collection under which you've gone to the FISA court and already gotten approval to target a particular agent of a foreign power in the United States, or moving over to the criminal side if it's information collected under the Wiretap Act, commonly known as Title III, under which you're conducting surveillance, let's say of an organized crime figure or in a drug case of an individual, in all of these contexts we collect information.

We don't, once we've collected it, we've gotten the necessary court approvals to obtain the information, we don't then have to go back to court to query the same information that we've already collected lawfully a second time to say is it okay to look at it. We've already gotten the conclusion that it's legal to collect it.

And if you have to go back to court every time you look at the information in your custody you can imagine that that would be quite burdensome and difficult, to have to go back every time to look at information that's already in your custody. But I can let the FBI and NSA address it a little bit.

MR. DE: If I could add a couple of points and then I'll turn it to my colleague from the bureau.

Just one basic point, we've been talking about U.S. person queries and I just articulated two types of collection. Just to clarify, U.S. person queries are not allowed under what I described as upstream collection. So as I articulated, there may be different reasons to have tailored procedures, minimization procedures for different types of collections. So such queries are not allowed for upstream.

Adding to Brad's point about lawfully collected information, so once information is collected pursuant to 702, the government can and

often will review what it needs to in that information.

Querying that lawfully collected information, one way to think about that is a way to more efficiently review that which the government already has in its possession and can review all of.

And so to get to your question about policy limits on querying that data, one also needs to understand that that information is at the government's disposal to review in the first instance, and querying it is just a way to organize it.

Secondly -- thirdly, if I could add there are standards in place for querying that information, at least for NSA. Such a query, and we're talking about PRISM collection, must be reasonably likely to return foreign intelligence information.

And then finally, in order to disseminate any U.S. person information that may result from such a query it has to be necessary to

understand the foreign intelligence or evidence of a crime is apparent from our publicly available procedures.

But on the operational element, let me turn that to Jim.

MR. BAKER: So just at a high level I think let me make a couple of comments. So first I think you have to think about the fact that you're creating a new and special category of information, as Brad was saying, right. So this would be information that had already been acquired pursuant to lawful process.

We normally will query that. We'll look through that. When something comes in, we'll look through our collected materials to try to find -- a threat comes in, let's say for example. We look at our collected materials, we try to figure out what we have, and then, you know, move forward as expeditiously as possible.

So you would be creating a new category of information that sort of would be off-limits from the normal type of collection that we do.

And I don't pretend to fully understand all the implications that that would have.

But a couple that come to mind, first of all, obviously would be delay. So you would have some additional process that you would have to go through, and I'm sure there would be some kind of emergency carve out and so on, but you'd have to think about and factor in the reality that you would be introducing delay into the system.

You would also then as a result potentially create a gap. There are several types of gaps, I guess. But you would have, there would be a disinclination for people, because either they don't have the facts, or it's just too hard or whatever, to actually go and pursue that extra pot of information.

So there might be some type of connection between what we can look at normally, this material, and then other types of material. And having that type of gap might, you know, actually create a blind spot for us in terms of intelligence collection.

You'd also have to think about, I think, the technical complexity of what it is that you're suggesting. So this is going to have to be segregated in some way, treated differently. And we'd just have to think about that. That could lead to, you know, training issues, technical costs, things like that.

So it's, you just have to actually do it in a way that would be different than from other types of data that we handle, so that's sort of at a high level some of the things that come to mind.

MR. LITT: Beth, can I add one brief point to this which is that over the last decade, decade and a half, there have been a number of commissions that have been set up to investigate after a variety of terrorism incidents, 9/11, Fort Hood, the underwear bomber and so on. Consistently every one of those commissions has found that we need to eliminate barriers to making use of the information that's lawfully in our possession in order to better protect the nation.

And this, requiring some kind of additional process before we can query this information runs directly contrary to the recommendations of all those commissions.

MS. COLLINS COOK: Thank you. I see that my time is up.

MR. MEDINE: By the way, I should say in the excitement of getting into the questioning I never had actually a chance to introduce the panelists. And so I just wanted for the benefit of the audience, you're familiar to us, but for the benefit of the audience we have Jim Baker, who's the General Counsel of the FBI, Raj De, who's the General Counsel at NSA, Bob Litt is the General Counsel at the Director of National Intelligence, and Brad Wiegmann, who is the Deputy Assistant Attorney General at the National Security Division of the Justice Department.

Again, thank you all for being here.

MR. DEMPSEY: Thanks, and thanks to the witnesses for being here. They are very well-known to us. I think everybody should

realize that we've now spent many, many days with these gentlemen and with many, many of their colleagues at all their agencies going through this information, and delving deeply into this.

And there's been a huge amount of dedication of time on the part of the agencies to make sure that we have everything that we ask for and to make sure that all of our questions are answered. And so, you know, all the Board members really appreciate the amount of time that you've dedicated to talking with us.

And I think it is very important here to be one hundred percent clear, and I think there has been a lot of misunderstanding about the 702 program, and I think I do see issues with the program and things we're talking about, but I think it's very important to narrow the subjects of controversy, or discussion, or concern.

And I'm afraid that Raj may have partly reinserted a problem here when you said that U.S. person selectors were not used for upstream collection, or for upstream searches they're not

used at all, period, at the collection stage.

You were saying that U.S. person identifiers or selectors are not used to search the acquired database of communications that were otherwise acquired on a particularized basis under the upstream program, correct?

MR. DE: Correct. I definitely would prefer not to introduce more ambiguities. Let me be absolutely clear, Section 702 collection of any flavor, upstream or PRISM, is only targeting non-U.S. persons reasonably believed to be located abroad.

The topic I was discussing was, is in the realm of that lawfully collected targets information, once it's in the government's possession a secondary issue arises as to how one can search through that data. And the issue that we were discussing was whether those searches can be conducted using U.S. person identifiers within that lawfully data. And the answer to that question is no with respect to upstream collection.

MR. DEMPSEY: And here when you're talking about search and collect and acquire, all of those terms you're using to mean in a colloquial sense when the government collects, obtains, puts into its database, acquires, you're not parsing those words for 702 purposes. There's not a distinction between the search, the collection, the acquisition, right? It's all, you're using those things all that refer to the same activity.

MR. DE: There's no parsing between acquisition or collection.

So there are some theories out there that when the government receives the data it doesn't count as collection or acquisition. That is incorrect. Acquisition and collection for these purposes are the same thing.

But the term search is a different term. Search, as we were just discussing, means searching information that has already been lawfully acquired or collected.

MR. DEMPSEY: Although the first --

okay, so now we have two meanings of search. It's so hard to be clear on this. Brad was explaining a search occurs when you first collect or acquire. That is the Fourth Amendment search.

MR. DE: I think he was speaking to the use of the term in the Fourth Amendment, not the use of the term for purposes of this.

MR. DEMPSEY: And then querying, then there's a second use of search meaning query. So you query your database?

MR. DE: Correct.

MR. LITT: That's the term that we typically use rather than search in that context.

MR. DEMPSEY: Right. In that case a query is not a search for Fourth Amendment purposes.

MR. LITT: Right.

MR. DEMPSEY: Briefly talk a little bit about this 51 percent theory. So persons reasonably believed to be outside the United States, and there's been some talk about, well, so there may have been some slide somewhere, I don't

know where this came from, but some notion that, oh, if it's a 51 percent likelihood, therefore 49 percent of the time we might be wrong, that the person's not outside the United States and that's permitted under 702. Can you comment on that.

MR. DE: Sure. So I think the bigger picture question that that gets to how a determination is made for purposes of the statute that you are in fact targeting a non-U.S. person reasonably believed to be located abroad.

So as Bob articulated, and I'm sorry for repeating this but just for clarity, the statute does not allow us to target U.S. persons, it does not allow the government to target anybody within the U.S., it does not allow for reverse targeting, it does not allow for the intentional collection of wholly domestic communications.

So as to how we establish a reasonable belief that the target is in fact a non-U.S. person reasonably believed to be located abroad, there is no 51 percent rule that if you are 51 percent sure it is a non-U.S. person located

abroad that is sufficient. That is not the rule, and I don't honestly know where that misconception has come from.

The foreignness determination, which is shorthand for referring to the determination that it is a non-U.S. person reasonably located to be abroad, is based on a totality of the circumstances.

So what does that mean? That means that an analyst must take into account all available information. It means that an analyst cannot ignore any contrary information to suggest that that is not the correct status of the person. And it also means naturally that any such determination is very fact-specific to the particular facts at hand.

I did a little checking and it turns out in our internal training materials, at least at NSA, we actually ask our analysts a question along the lines of, if you have four pieces of information that suggests a person is abroad and two pieces of information that suggests a person

is domestic, given that the score is four to two is that sufficient to establish foreignness?

And the correct answer to that is, no, it is not sufficient because it is not a majority test. It is a totality of the circumstances test. One must take into account the strength, credibility, and import of all relevant information.

But just to add on to that, to your bigger point about confidence in that determination, analysts have an affirmative obligation to periodically revisit the foreignness determination. So it is not a once and done system.

Moreover, targeting determinations must be documented ex ante before any collection occurs. That documentation is reviewed, every determination is reviewed in 60 day increments by the Department of Justice and the Office of the Director of National Intelligence to determine if they agree with that determination.

And then finally, the targeting

procedures, as we mentioned, which account for a lot of this are reviewed annually by the Foreign Intelligence Surveillance Court and approved to be consistent with the Fourth Amendment and the statute obviously.

MR. WIEGMANN: And if I could just add from the DOJ perspective, as Raj said, we reviewed all of those foreignness determinations and we found an error rate of less than .1 percent basically. So that equates to essentially less than one in a thousand cases in which we're finding that NSA is making erroneous foreignness determinations.

MR. MEDINE: Judge Wald.

MS. WALD: Thank you again. I think that the NSA has said that in some of its information that if information about U.S. persons is collected incidentally to a 702 search that was targeted on a non-U.S. person and the incidental information about U.S. persons is found not to have any foreign intelligence value it will be, quote, purged.

Can you explain exactly what purging means? Does that mean that it can subsequently not be used at all, or it can be subsequently used or retained for some purposes? And finally, at what point and by whom would this decision of non-intelligence value be made? There's a lot of sub-questions.

MR. DE: Sure. Well, let me step back for a moment. If the information is determined to not have --

MS. WALD: Could you just speak a tiny bit louder because I'm at the tail-end of this table.

MR. DE: Certainly. If information is determined to not have foreign intelligence value then it is required to be purged.

What purging means is removed from NSA systems in a way that it cannot be used, period.

MS. WALD: For any reason at all?

MR. DE: Correct. There are extensive requirements we have gone through with the Foreign Intelligence Surveillance Court to ensure to the

best extent humanly possible that NSA's technical systems can, in fact, purge data as required by both our minimization procedures and the Foreign Intelligence Surveillance Court.

MS. WALD: But just to pursue that a little bit, in your experience is that to purge or not to purge decision made early in the process or is it kept in there until the analyst or whoever has a chance to do some more hunting around and see whether or not maybe other things would suggest that that does have intelligence value?

In other words, if there's such a concern about U.S., as there is in outside groups, about U.S. incidental information that's in the files and later there's a possibility of it being queried, I wonder how extensive this purging operation really is?

MR. DE: To purge or not to purge, that is the question.

MS. WALD: Yes.

MR. DE: So our procedures require that the determination about foreign intelligence value

be made as early as possible in the, what one in the technical sense calls the processing cycle. So it is not something that by default can be ignored.

That being said --

MS. WALD: And who makes that?

MR. DE: An assessment as to foreign intelligence value is made by foreign intelligence analysts.

MS. WALD: By the analysts who are working on it?

MR. DE: Correct, as they would be the ones who have the most relevant information.

But that also goes to a bigger point as to the nature of intelligence analysis. I think you all would appreciate that it's difficult to determine without context the foreign intelligence value of any particular piece of information. In fact, that's why the intelligence community is often encouraged to connect the dots of various pieces of disparate information.

And so I think we would hope and expect

that analysts make that determination about foreign intelligence value within the context of all available information.

But to your point as to if information is not reviewed, what is the default? This is a large reason why we in fact have default retention periods for data. And for example, for NSA the default for PRISM collection is a five year retention period.

But that's also a reason why that retention period is adjustable, or at least is tailored to the specific nature of the collection.

So for example, for upstream collection the retention period is two years, recognizing the nature of, the unique nature of upstream collection and that it may have a greater implication for privacy interests.

MS. WALD: Okay. The President required, I think he required in his January directive that went to 215 that at least temporarily the selectors in 215 for querying the databank of U.S. telephone calls metadata had to

be approved by the FISA court.

Why wouldn't a similar requirement for 702 be appropriate in the case where U.S. person indicators are used to search the PRISM database? I mean what big difference do you see there?

MR. LITT: Well, I think from a theoretical perspective it's the difference between a bulk collection and a targeted collection, which is that the --

MS. WALD: But I would think that, I'm sorry for interrupting, Bob. I would think that message, since 702 has actually got the content.

MR. LITT: Well, and the second point I was going to make is that I think the operational burden in the context of 702 would be far greater than in the context of 215.

If you recall the number of actual telephone numbers as to which a RAS, reasonable articulable suspicion determination was made under Section 215 was very small.

The number of times that we query the 702 database for information is considerably

larger. I suspect that the Foreign Intelligence Surveillance Court would be extremely unhappy if they were required to approve every such query.

MS. WALD: I suppose the ultimate question for us is whether or not the inconvenience to the agencies, or even the unhappiness of the FISA court would be the ultimate criteria.

MR. LITT: Well, I mean I think it's more than a question of inconvenience. I think it's a question of practicability.

MR. DE: And if I could add one point to that. I think one must also look at the underlying nature of the collection program at issue. And so I think we should be clear not to conflate the 215 program with the 702 program, and as you mentioned, one deals with metadata and one deals with content.

But the important point being the latter is directed at content collection targeting non-U.S. persons located abroad, whereas the 215 program, although it deals with metadata, did not

have such a necessary distinction.

MS. WALD: It did have a selective, I mean the 215 program and the original --

MR. MEDINE: I'm going to, your time, the Judge's time has expired, but we'll have an opportunity in another round to continue that discussion.

I want to shift to a different topic, which is about communication, about searches or about queries, which is, and I'm happy to have you explain it, but my understanding basically is that you are looking for other peoples' discussion of a particular selector or email term.

But I'd like to get back to some of the definitions here, which are there are some terms here that would be helpful to understand your view of, which is what is a target? What is a tasking? What is a selector? What's a directive?

If you could explain those terms, because I did want to shift to how those terms might apply in the about context.

MR. WIEGMANN: Okay, I can take a stab

at that. So a target is the -- maybe I should start with selector since that's the operative term that the others build on.

A selector would typically be an email account or a phone number that you are targeting. So this is the, you get, you know, terrorists at Google.com, you know, whatever. That's the address that you have information about that if you have reason to believe that that person is a terrorist and you would like to collect foreign intelligence information, I might be focusing on that person's account.

So when you go up on that selector, we say go up on or target that selector, that means we're collecting information, we're going to the provider and getting information related to that person's account.

So we're intercepting in real time and then collecting the historic communications of that particular account.

Okay, so that's what we mean by targeting a selector. You're using that selector,

you're providing that to the company, the provider, to get information on that account, or if it's a phone number on that phone number.

So that's when we say selector it's really an arcane term that people wouldn't understand, but it's really phone numbers, email addresses, things like that.

And targeting, it means that's the one you're trying to get. They may be in communication with other email addresses or other phone numbers and so forth. Those are not the targeted numbers or accounts, those are others that are incidentally acquired because they're on the other end of these communications. So target is the one you're going after.

And the statute requires that that target be a non-U.S. person located overseas. And so that's the foreignness determinations that we're talking about as we go through at great lengths to make sure that that target is in fact belongs to a non-U.S. person that is located overseas.

The other two questions?

MR. MEDINE: Tasking or task.

MR. WIEGMANN: Tasking is when you're going and saying, okay, I want to task this account means I want to collect information from that account. So that's the collection.

MR. LITT: You task a selector.

MR. WIEGMANN: You task a selector. So you're identifying, that's when you take that selector to the company and say this one's been approved. You've concluded that it is, does belong to a non-U.S. person overseas, a terrorist, or a proliferator, or a cyber person, right, whoever it is, and then we go to the company and get the information.

MR. MEDINE: And directives.

MR. WIEGMANN: So directives are the orders that go to the companies that say they have to comply with the lawful tasking. So that's the kind of more overarching order that goes to a company provider and says, okay, you have a legal obligation to comply with the taskings that are

given to you and here are the rules and everything. And that's all provided to them.

Is that a fair summary? I'll ask my colleagues to see if that is --

MR. DE: Keeping target as the statutory term. A term like selector is just an operational term to refer to something like an email or phone number, directive being the legal process by which that's effectuated, and tasking being the sort of internal government term for how you start the collection on a particular selector.

MR. MEDINE: Okay. So I guess building on that, what's the statutory rationale for about collections, because if the target is the email account or phone number, what is the justification for gathering communications between two persons, it may even be two U.S. persons who are discussing that phone number or that email address, but they are not themselves, there's no to or from that particular email address or particular phone number, why is that targeting that is permissible under the statute?

MR. WIEGMANN: Right. So the conclusion there again in a typical case, you're right, if you're targeting, you know, bad guy at Google.com you're targeting that person's accounts, their communications.

Why abouts collection is different is it's not necessarily communications to or from that bad guy but instead about that selector.

And so what the court has concluded is that when the statute uses the term targeting of a non-U.S. person overseas, targeting that selector qualifies under the statute for targeting that non-U.S. person overseas.

So it doesn't have to be targeting necessarily to or from, but can also target the communications that are about that particular selector.

MR. MEDINE: So that's a different meaning of target than earlier, which is where you're focusing on an account, now you're discussing targeting means discussions about that account.

MR. WIEGMANN: About that selector, correct.

MR. DE: 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.

MR. MEDINE: But does it raise -- oh, I see my time has expired so I'll --

MS. BRAND: I'm glad to see you're following your own rules.

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?

MR. DE: So I would like to --

MS. BRAND: But you could, you could perhaps get it about Rachel Brand at --

MR. DE: Just so that, because I think this is an issue that all of us slip into, clarifying querying for collection.

So we are discussing now the collection of information. Abouts is a type of collection of information.

MS. BRAND: I'm sorry, right. Yes, that's right.

MR. DE: And so all collection of information is based, focused on selectors, not key words, as you just mentioned like terrorist, or like a generic name or things along those lines.

MS. BRAND: Okay.

MR. DE: And it's the same selectors that are used for the PRISM program that are also used for upstream collection. It's just a different way to effectuate the collection.

MS. BRAND: Okay. I think a large part of the function of these hearings is a public

education function and so I thought David's questions were great to explain the meaning of different terms, and I'm glad that you're willing to bear with us asking you some questions that we've already discussed with you in private. But I think it's helpful for everyone to understand what we're talking about.

And along those lines there was some discussion in Pat's questions about purging data that doesn't turn out to be foreign intelligence information.

But can you explain how on the front-end you implement the requirement that, not only that the target be a non-U.S. person reasonably believed to be abroad but that you expect to get foreign intelligence information through the collection, that's a separate statutory requirement. How do you go about ensuring that you're collecting that type of information?

MR. DE: Sure. So in our earlier discussion we skipped right to the foreignness determination, but that's actually a second step.

There has to be a reason one actually wants to collect intelligence from the particular selector in the first place.

And then one has to get to the fact, is this a type of collection permitted under the statute? So there has to be a valid foreign intelligence reason to do that collection.

But beyond that there has to be a valid foreign intelligence reason within the ambit of one of those certifications that the FISC approves annually. Those are certifications on things like counterterrorism, encountering WMDs, for example, weapons of mass destruction.

And so when an analyst needs to make a determination as to the valid foreign intelligence purpose for which they want to effectuate collections, they must also document that.

That is documented in a targeting rationale document in advance, ex ante, and those are always reviewed by the Justice Department and the Director of National Intelligence every 60 days.

MR. WIEGMANN: This is an important point for non-U.S. persons because people think about, okay, well once you've concluded that it's a non-U.S. person overseas then you can collect whatever you want. As Raj said, that's really not the case.

It really is targeted, not only based on the identity of the person and the location of the person, but also that you're trying to get foreign intelligence. And so it's an important protection really in the statute that is designed for non-U.S. persons. It's not blanket collection of any non-U.S. person overseas. It's aimed at only those people who are foreign intelligence targets and you have reason to believe that going up on that account that I mentioned, bad guy at Google.com is going to give you back information, information that is foreign intelligence, like on cyber threats, on terrorists, on proliferation, whatever it might be.

MS. BRAND: What can you tell us in an unclassified setting about the documentation of

foreign intelligence purpose or the oversight to ensure? I mean we've talked a little bit about that in past questions, but can you give us anything more specific?

MR. WIEGMANN: They do have to document that at NSA and every -- it's essentially called a tasking sheet, I think. And on that sheet they are documenting the foreign intelligence purpose that they are trying to pursue in going after a particular target.

And those are all reviewed together with the foreignness determination by the Department of Justice on a regular basis.

MS. BRAND: That's a separate sheet for every selector?

MR. WIEGMANN: For every single one, that's right.

MR. BAKER: And I think, at least with respect to FBI, I think the review that Raj mentioned earlier is done every 30 days on these tasking decisions, I guess you'd say, the foreign intelligence and the foreignness determination.

MR. DE: And if I could put that into the broader context of if the question really is getting at what is the process within which that happens, even before that happens we have training for analysts as to how they should document this material, we have audits of our databases, we have a comprehensive compliance program, we have spot checks, even within NSA prior to the 60 day reviews that are done by the Department of Justice and DNI, for us anyway.

There are also quarterly reports to the FISC on compliance with the program, semiannual reports to the FISC and to Congress, and annual inspectors general assessments, and as I mentioned, the annual certification process by the FISC.

So I think those decisions are, while they're one very granular aspect of the program, are conducted within the context of this broader regime.

MS. BRAND: Okay. And I see that my time just ran out.

MS. COLLINS COOK: I wanted to ask one additional question about abouts. Can you do about collection through PRISM?

MR. DE: No.

MS. COLLINS COOK: So it is limited to upstream collection?

MR. DE: Correct. PRISM is only collection to or from selectors.

MS. COLLINS COOK: I wanted to shift to a separate topic. One of the things that I have found both concerning and frustrating through the process of our evaluation of programs is how to both assess and articulate the efficacy of these programs.

And Mr. Litt, you had begun speaking about this in your prepared remarks. And I'd like to ask a couple of questions. One, how do you assess the efficacy of a particular program? How do you think we should be assessing the efficacy of a particular program?

And three, it's not really a question, it's more of a comment which is, please don't give

me a series of success stories and then say that's how you evaluate the efficacy of the program. Because I think that's an initial response from the government often in response to a question, either from a body like ours or from the media.

But how do you assess the efficacy of the program, how periodically do you do so, and how would you encourage us to assess the efficacy?

MR. LITT: Well, let me start on that, and I want to start by saying that I completely agree with you that sort of individual success stories are not the way to evaluate a collection program and its utility.

The way you evaluate collection programs is going to depend in part on what the particular program is for.

In this case, we have in fact the Office of the Director of National Intelligence has attempted, part of our job is to try to determine that resources are effectively allocated within the intelligence community budget.

And so we have done studies to try to

look at, okay, what are our collection priorities, how much reporting is generated on these priorities, and where do those reports come from, what kind of collection source, to the extent we can identify that. And that's one of the ways that we've determined that Section 702 is relevant.

Another thing is just by looking at the sheer nature of the information that we get and its utility towards a whole variety of national priorities. That's a more impressionistic approach, and yet you can see time and again in important intelligence reports that are provided to policy makers that it's derived from Section 702 collection.

So those are two ways that I would look at estimating the value of a particular collection.

MR. DE: If I could just add on to that. With respect to this program or any program I think intelligence professionals will tell you that any tool must be evaluated in the context of

the other tools in which it is utilized.

All intelligence tools are used in complementary fashion with one another and to isolate one particular tool and evaluate its effectiveness in isolation probably doesn't do us justice as to what's valuable and what's not.

It also depends on the type of tool. Different types of intelligence programs are used for different purposes. A program like Section 702 is used for different purposes, for example, than a program, a metadata program with telephony metadata.

One may be a discovery tool to help pursue more specific collection and others may be used as in fact the specific collection that follows from that.

Third, there may be uses in which the PCLOB has recognized in terms of either directing the government in certain directions or at least helping to shape the focus of the government.

And so I think the absolute wrong question is how many plots did this tool stop.

And you can fill in the blank for what this tool refers to. But that is absolutely the wrong question, and I think it won't do us justice to figure out what we need as a government.

MS. COLLINS COOK: I have time I think for one last question. What is the view of the various agencies as to whether or not 702 is an effective and valuable program for the United States?

MR. BAKER: I think it is an effective and valuable program for the United States.

And if I could just address your last question as well. I mean I think you really, in order to understand whether it's effective and useful you have to think about what your goals are with respect to this particular program.

And the goals for this program, like many other collection programs are to obtain I think timely, accurate, informative foreign intelligence information about the capabilities, plans, intentions of foreign powers, agents, actors, and so on and so forth.

And so I think really what you're talking really is, I think, developing a good metric to understand whether this program is worth all of the costs associated with it. And so I think you'd want to look at the amount of information that you, that we acquire, but also then obviously the quality of it. How good is it? And I think you can slice that a lot of different ways, as my colleagues have suggested.

So I think that's really what I would recommend you be focused on. But you have to, because this is a broad-based foreign intelligence collection program you have to look at not only, I mean you have to look at counterterrorism but you have to look more broadly than that because this program is not limited just to counterterrorism.

MR. DE: I agree it's definitely an effective program. I think the one point I should have added is that the review that Bob mentioned happening within the executive branch is not limited to the executive branch.

Congress also reviews the effectiveness

of this program, as well as the 215 program. And I think that's part of the rationale behind having sunset clauses for various programs is that when those statutory provisions expire, as did the 215 program twice in the last five years and as did 702 in 2012, Congress undertakes, as it should, an evaluation of the effectiveness of the programs.

MR. LITT: So I completely agree that it is an effective and important program and I really want to emphasize the last point that Jim made, which is that this program should not be considered solely as a counterterrorism program. This program has utility, has significant and exceedingly important utility in areas outside of counterterrorism.

MR. DEMPSEY: Trying to clear up another issue in terms of the participation of service providers and the awareness of service providers in the 702 implementation, is 702 implemented, all 702 implementation is done with the full knowledge and assistance of any company that, from which information is obtained, is that

correct?

MR. BAKER: Yes. The answer to that is yes.

MR. DEMPSEY: So early on in the debate there were some statements by companies who may or may not have been involved in the program saying, well, we've never heard of PRISM. But whether they ever heard of PRISM, any company that was, from whom information was being obtained under 702 knew that it was being obtained?

MR. LITT: Correct.

MR. DE: PRISM is just an internal government term that as a result of the leaks became a public term. But collection under this program is done pursuant to compulsory legal process that any recipient company would have received.

MR. DEMPSEY: So they know that their data is being obtained because --

MR. DE: They would have received legal process in order to assist the government, yes.

MR. DEMPSEY: One thing I read in one of the statements is under 702 you could target entire countries or regions, is that correct?

MR. DE: So all collection under 702 is based on specific selectors, things like phone numbers or email addresses. It is not a bulk collection program.

MR. DEMPSEY: And a selector would not be an entire area code, for example?

MR. DE: Correct, correct.

MR. DEMPSEY: Going back to the constitutional -- oh, one other set of questions.

Even I've lost track now of what you've already said here versus what you've said elsewhere. But in terms of where you make a determination that a person is a non-U.S. person outside, reasonably believed to be outside the United States and then you later discover that that was good faith but wrong, the person was in United States, or the person was a U.S. person, do you track that, and what do you do when you discover that, and how often do you discover?

I'm not talking about the roamings, I'm talking just about you thought he was outside the United States and that was just wrong, or you thought he was a non-U.S. person and that was just wrong, how often does that occur?

MR. DE: So I'll defer to Brad on the sort of overarching review, but if I could just make a point about what happens. So yes, we keep track of every time new information comes to our attention to suggest that a prior intelligence evaluation was incorrect, even if it had met the legal standard.

Every such incident is a compliance matter that has to be reported to the FISC and ultimately in semiannual reports reported to the Congress.

And third, that sets in process a purging process by which information that should not have been collected if it had not met the legal standard needs to be purged from NSA systems.

I think Brad can speak to the level of

accuracy of those.

MR. BAKER: Just real quick, it's the same. The item is de-tasked and the information is purged.

MR. WIEGMANN: Right. So just to distinguish again between two different types of compliance issues. One is the roamer example that you mentioned.

So this is, let's say we're up on a cell phone that we believe belongs to a bad guy who's outside the United States, a foreign person, and then that person shows up in Chicago, when that happens we de-task that cell phone. That means we're no longer collecting the communications.

That's a compliance incident that's reported but it's not an erroneous determination. It's based on the movement of the individual.

So putting those cases aside, in cases where we just kind of get it wrong, we think the email account or the phone is located overseas but it turns out that that's wrong, or it turns out

that we think it's a non-U.S. person but it is a U.S. person, we do review every single one to see if that's the case.

And our review at Justice we decided to review, and as I mentioned earlier, we think it's less than one in a thousand cases where they make that determination erroneously.

MR. DE: And this probably bears worth repeating that the initial determination is not a once and done, so there is an affirmative obligation for analysts to reaffirm the foreignness determination on a periodic basis, which contributes to the ability to make sure that determination is in fact fresh and current, which of course contributes to the accuracy of that determination.

MR. DEMPSEY: Going to the constitutional issues, back to those for a second, the FISA court has determined, I mean they must they must determine every year that the program is being implemented consistent with the Fourth Amendment.

The very first time they determined that, there was an opinion that they issued. That one is, am I right, not yet public?

MR. WIEGMANN: I think that's correct.

MR. DEMPSEY: Isn't that a good candidate for declassification?

MR. LITT: We have a lot of good candidates for declassification.

MR. DEMPSEY: Yeah.

MR. LITT: In all seriousness there, we are, there are a lot of documents that we have that we are reviewing for declassification that include not only FISA court opinions but a whole variety of other documents.

MR. DEMPSEY: The FISA court in 2008 when they last considered the constitutionality of a program, the predecessor to 702, the court issued a redacted but largely unclassified opinion conducting a relatively full Fourth Amendment analysis.

And there's been some Fourth Amendment analysis conducted in this situation, and if

you're sort of talking about, you know, the Rosetta Stone kind of Ur document, then the very first court opinion should have been the most fulsome explanation of the constitutionality of the program.

I think that -- I mean I hear Bob saying there's a lot of opinions out there, but to me this one seems to be one that would explicate at least one court's judgement on this because it's been the basis of -- I assume all the rest just said nothing has changed that would merit us to reconsider our very first judgement.

MR. WIEGMANN: So I mean I think it's among the opinions. We're committed to reviewing all the opinions of the FISA court to determine which ones can be declassified in redacted form. So I imagine this will be among those that are reviewed. So absolutely, I don't disagree. It'll be among the opinions that will be reviewed.

MR. DE: I just don't want to leave folks with any mysterious misimpression. I think the Board has access to everything and so one

shouldn't have to assume anything about subsequent opinions. The Board has in fact reviewed everything.

And so I just don't want -- what I think would be an unfortunate consequence would be for folks to take away the impression that there is a mysterious opinion that has some secret analysis, and I don't think that's the case. I don't think you intended to suggest that.

MR. MEDINE: The Board does have access to it but I think the question is whether the public should have access to it as part of the debate. But it's Judge Wald's --

MR. DEMPSEY: The public had access to the 2008 --

MR. MEDINE: It's Judge Wald's turn.

MR. WIEGMANN: So just one other thing I would add on that is that 702 collection has now been challenged by a number of criminal defendants when 702 information is being used against them in their cases. And so we'll be filing public briefs and we can expect some more decisions in that area

as well.

So that's another way that the constitutionality of 702 will now be on the public record, or I mean the opinions on it, and the briefs and everything will now be a matter of public record.

MR. MEDINE: Judge Wald.

MS. WALD: Okay. By whom and under what substantive criteria is the initial decision to use a U.S. person selector for searching the PRISM base made? I mean who decides let's do that? What's the substantive criteria on which they make it?

You don't have to go into the review process. I know the decision will be reviewed up and down. But how does that get made? What's the substantive basis?

MR. DE: So I can speak for NSA in particular.

MS. WALD: So just to clarify, that means if it goes to one of the other agencies, not NSA, CIA or FBI or something, they make their own

substantive decisions for querying?

MR. DE: Yes. The 702 program perhaps as a necessary predicate is one that all agencies operate on their own and have their own minimization procedures which would address topics like searches.

NSA's procedures in this regard, in this element have been made public and so the standard is that such a query needs to be reasonably likely to return foreign intelligence information.

MS. WALD: Be reasonably likely. And who is it made by initially?

MR. DE: It's made by the analyst.

MS. WALD: By the analyst who's working on that particular case, okay.

My other question is that the President did, if I understand his directive correctly, direct that there be some changes in the treatment of non-U.S. persons as to the limits on and retention of the data acquired incidentally to bring them more in line with those of U.S. persons

incidentally where there is no foreign intelligence value apparently.

Can you tell us a little bit more specifically if anything has been done in that regard or is being contemplated vis-a-vis 702?

MR. LITT: So I think first of all it's important to understand the point that somebody made, it may have been Brad made earlier, which is that there are already protections to some degree built into the system there. The protections for non-U.S. persons are not as great as those for U.S. persons because U.S. persons are protected by the Fourth Amendment.

But there is a requirement that we can't target a selector unless we have reason to believe it's of foreign intelligence value. And there's sort of a general principle that the intelligence agencies, their job is to collect, analyze, and disseminate foreign intelligence information, not random information.

I think what the President has directed is that we go back and look at our procedures and

not only with respect to 702, but with respect to signals intelligence in general, assess whether, the extent to which it's possible to provide limitations on collection, retention, and dissemination that more closely track those for U.S. persons.

For example, Executive Order 12333 provides specific categories of personal information about U.S. persons that can appropriately be retained and disseminated.

There's a list of them in Executive Order 12333 and the President has asked that we assess whether we can apply those same sorts of rules to personal identifiable information of non-U.S. persons.

MS. WALD: Right now, just to follow-up, right now if you get incidental information about a foreign person in the course of targeting another foreign person and you look at it, do you use the same criteria and look at the same review and say, well, you know, he was just talking to his grandmother or something, there isn't any

foreign intelligence there, and you purge it?

MR. DE: Any time there is not foreign intelligence value to collection, by definition it would be purged.

But I think an important point to be made as you are articulating, Judge, is incidental collection, just to explain that term a little bit, all communications obviously have two ends. One end is the target and the other is presumably not a target. We don't know. One doesn't know ex ante.

And so by definition there will be incidental collection of non-U.S. persons, as well as U.S. persons. Historically, constitutional protections obviously have only applied to the U.S. person subset.

MS. WALD: I understand.

MR. BAKER: Can I just make a comment about that?

MS. WALD: We don't have time. Okay, quickly on the last time, I found it very provocative when you were answering Beth Cook's

question about if you're going to assess the efficacy of a program you have to look at it in terms of its efficacy and the holistic view of all of the programs.

I guess it's inevitable that I would ask the question, but how can anybody except you people do that, because so many of your programs, I think, are just unknown, even to the FISA court? They're not all FISA supervised, and certainly the outside world doesn't know about many of them. So you know, how in effect can an outside assessment be made?

MR. DE: If I could just address it since it was in response to my comment. Certainly I think I would not suggest that there should be a public evaluation of all intelligence programs. I think, for example, this Board as access to information about counterterrorism programs and so I would expect that any evaluation would be in the context of the other CT programs that you have the jurisdiction to review.

As with Congress, as I mentioned, they

reevaluate programs on a periodic basis. And I think the public record now indicates that there is a fairly robust exchange between the executive branch and the legislative branch on a variety of programs. And so I think that's where traditionally the evaluation has occurred.

MR. LITT: Yeah, I was just going to say that we've managed, we've set the balance between public disclosure and the need for secrecy by empowering the congressional intelligence committees. We're required by statute to keep them fully and currently informed of intelligence activities, and we do. They know about these programs and they have the opportunity to evaluate them, and they do.

In fact, they passed an Intelligence Authorization Act that includes a lengthy classified annex that is very prescriptive with respect both to reports that it requires of us and directions as to what we should, you know, where we should be spending our money.

So that's sort of the external

oversight and the way we've said, okay, well, we need to have oversight of these but they still need to remain classified.

MR. MEDINE: Did you want to finish? I don't know, you wanted to make a point earlier about foreign intelligence.

MR. BAKER: I had several points I wanted to make. But let me just on that real quick, I mean I think the, even the addition of Congress having oversight of it, the courts in certain circumstances, and then also obviously the President and all of the executive branch officials, we have an obligation to make sure that in addition to adherence to the law and taking care that the laws are faithfully executed, to spend our time and spend our money on programs that are effective and not be wasting our time on things that are not.

I mean that flows from the President to the DNI, the Attorney General, Director of the FBI, Director of NSA and so on. We should be focused on things that are useful and collecting

information that produces the kind of intelligence information that I was talking about before.

So the other comment that I just wanted to make was just with respect to FBI, our personnel only have access to the databases when they've received the proper training with appropriate oversight and operating consistent with the court-approved standard minimization procedures when they're doing their query activity.

MR. MEDINE: I wanted to shift to a different subject, which is attorney client privilege. There were some press reports a couple of weeks ago about collection of information that may involve attorney client communications.

But I want to focus particularly on the NSA minimization procedures, which I understand do exclude attorney client communications but only in a very narrow context where the client is under criminal indictment and the United States, basically on a federal criminal indictment.

That seems like a very narrow

interpretation of attorney client privilege. I wanted to see if that is the interpretation you apply in minimizing communications, and if it is what impact there would be if it was expanded to the more normally accepted definition of attorney client privilege, which is basically lawyers and clients consulting with each other?

MR. DE: So we have written a letter to the ABA and commented on it to the Board and to the public, I think it's a public letter now, which explicates in fuller detail than I probably can off the top of my head as to our procedures.

But I think one fundamental premise is that analysts are under an obligation to identify for the Office of General Counsel any time they encounter something that may be potentially privileged.

And I think as all of us who are lawyers, I think that probably encompasses every one up here on the stage, knows just because a communication is with a lawyer does not mean it is in fact a privileged communication. So it's

helpful to have a lawyer involved to determine that.

While I can't speak to any particular incident that may have been written about in the press I think there's a couple of big picture points that are worth making. One is our office has historically provided a range of advice to minimize to the extent possible the collection of attorney privileged material.

MR. MEDINE: That's privilege just where there's a criminal indictment or are you viewing privilege --

MR. DE: Beyond the criminal. So the point I'm trying to make is that while there may be a specific provision in the 702 procedures that addresses the criminal context, there's a reason why we ask analysts to consult counsel, because the advice can often be tailored to the specifics of a circumstance far outside the criminal realm, recognizing the import of attorney client privileged material in context, even outside the criminal context.

MR. MEDINE: I want to talk a little bit about reverse targeting where you target someone overseas potentially with the view of collecting information about a U.S. person in the United States, and that's impermissible.

There seems, again maybe this is a somewhat technical point, but there seems to be somewhat of a quirk in the statute. It says that you can target people reasonably believed to be outside the Unites States, you cannot reverse target someone outside the United States if the purpose is to target a particular known person reasonably believed to be in the United States.

Does that permit targeting a person outside the United States with the intent of gathering information about U.S. persons not in the United States?

MR. WIEGMANN: No.

MR. MEDINE: Why not?

MR. WIEGMANN: There's a separate provision that bars targeting U.S. persons outside the United States and so if you were doing that

and you are trying to target a U.S. person outside the United States, you couldn't do that.

MR. MEDINE: So you wouldn't do the reverse targeting procedure?

MR. WIEGMANN: I don't know if you would call that reverse targeting --

MR. DE: There is another statutory provision that prohibits the targeting of U.S. persons outside the U.S. under 702 --

MR. MEDINE: Even reverse targeting? Again, I'm not talking about -- I agree it's clear that you can't target a U.S. person outside of the United States, but what if I find a non-U.S. person that I know is in communication with a U.S. person who's also outside of the United States, is that permissible?

MR. WIEGMANN: No.

MR. DE: No.

MR. MEDINE: Because?

MR. WIEGMANN: Because you would be targeting, if your real purpose is to target that U.S. person, you're targeting that person.

MR. MEDINE: So reverse targeting in your view is the same as targeting? The prohibition on reverse targeting is co-existent with the prohibition on targeting?

MR. WIEGMANN: Well, I mean again I think of reverse targeting as a geographic issue essentially when you're targeting, let's say you have a legitimate target overseas but you really want the communications of a U.S. person or a non-U.S. person inside the United States, but the statute says you can't do that.

MR. MEDINE: Right, but --

MR. WIEGMANN: But as we were just explaining which is if you have a U.S. person that you're interested in overseas, you can't use 702 to target them either and I don't think --

MR. MEDINE: Or reverse target them?

MR. WIEGMANN: What's that?

MR. MEDINE: If you know that that U.S. person is in communication with a non-U.S. person and both of them are overseas --

MR. WIEGMANN: Right.

MR. MEDINE: Could you target the non-U.S. person to get the U.S. person's communications?

MR. WIEGMANN: You couldn't do it for that purpose but if the non-U.S. person overseas is a valid foreign intelligence target that you're interested in their communications, sure, you can target that person. And the fact that they're incidentally communicating with a U.S. person overseas, that's okay. I wouldn't consider that reverse targeting.

You still have to have that legitimate target. I don't know if that answers your question, but.

MR. MEDINE: It did.

MR. BAKER: I'm not going to read it now and take up your time, but take a look at Section 704 A 2, and that may address the kind of concern that you're focused on perhaps, but perhaps not.

MR. MEDINE: Okay. I wanted to get back to efficacy. As you know, our charge is to

look at the balance between national security and privacy and civil liberties, and I think following up on Ms. Cook's question -- sorry, I'll just hold that until the next round.

MS. BRAND: I wanted to go back to upstream collection a little bit. I've seen some statements in the public domain about the volume of upstream collection vis-a-vis the volume of PRISM collection. What can you tell us in a public setting about that?

MR. DE: I think the best publicly available information is from the October 11th, 2011 opinion that has now been declassified in which there was a rough estimate there, and forgive me for if it's not precise, but that about 10 percent of collection is upstream. On the order of magnitude, I just don't know the exact number.

MS. BRAND: Okay. So you said in an earlier round of questioning that upstream, collection from upstream is retained for a shorter period of time than collection from PRISM and you

said that the reason for that distinction is that there's a potentially greater privacy concern with respect to upstream collection.

Can you elaborate on why, whether the additional privacy concerns that pertain to upstream.

MR. DE: Sure. And a lot of this is laid out in this court opinion that's now public. This is from the fall of 2011. I think because of the nature of abouts collections, which we have discussed, there is potentially a greater likelihood of implicating incidental U.S. person communication or inadvertently collecting wholly domestic communications that therefore must need to be purged.

And for a variety of circumstances the court evaluated the minimization procedures we had in place and as a consequence of that evaluation the government put forth a shorter retention period to be sure that the court could reach comfort with the compliance of those procedures with the Fourth Amendment. And so two years was

one element of the revised procedures that are now public.

MS. BRAND: So from what you just said that if using a legitimately tasked about term a wholly domestic communication is collected, it has to be purged?

MR. DE: If one recognizes it, yes. In fact, there's a --

MS. BRAND: Even if it has foreign intelligence information?

MR. DE: There are specifics. Off the top of my head I can't articulate all the particular exceptions in the minimization procedures but there are an elaborate set of detailed procedures that are now public that discuss how upstream collection must be treated in order to account for this concern.

And it has things like data must be segregated in certain ways where the risk of collecting a wholly domestic communication is higher, there's a shorter retention period.

Wholly domestic communications are not

permitted under the statute, and so therefore as a default rule, yes, it must be purged.

MS. BRAND: Jim, was there something you wanted to add?

Okay. I want to use the word incidental collection there again, and your definition earlier seemed to be that by incidental you mean, by incidental U.S. person collection you mean that the person on the other end of the phone from the non-U.S. person abroad is a U.S. person. That's your definition, right?

Is there another definition that you're aware of? Because you seem to be -- okay.

I think there's been some frustration with the use the term incidental in that context because it's not accidental, it's intentional. It's actually unavoidable. And so I just wanted to make sure that we're all on the same page, that by incidental you mean not accidental, not unintentional, but this is actually what we're doing.

MR. LITT: It is incidental to the

collection on the target. It is not accidental, it is not inadvertent. Incidental is the appropriate term for it.

MS. BRAND: Okay.

MR. DE: And I'd say that term I think has been used far beyond this program and historically, so there's no judgement intended. That is just a term.

MS. BRAND: Okay, okay. I'll hold the other questions for another round.

MS. COLLINS COOK: Just following up on David's question, I think it goes to a broader point which is that there is a perception that this statute is fairly complicated, there's got to be loopholes or idiosyncrasies in there somewhere.

But let me just ask you, would it be the view of the United States government that it is appropriate to use 702 to intentionally target U.S. persons, whether directly or through reverse targeting, whether they are inside the United States or outside the United States?

MR. LITT: No, definitely not.

MR. DE: No.

MR. LITT: That is not permissible.

MS. COLLINS COOK: I wanted to also follow up on a question about the abouts. And I apologize, again just for folks understanding that we spent six and a half hours talking with folks about just the oversight mechanisms in place and were unable to get through that entire conversation. So I apologize if you've said this before today.

The collection methods, procedures that you use with respect to abouts, those procedures, are they approved by the FISA court?

MR. DE: Yes.

MS. COLLINS COOK: Are those transparent to Congress?

MR. DE: Yes.

MS. COLLINS COOK: I think we haven't necessarily, we started to allude to this but can you talk a little bit about your impression of how the intel committees in particular view their obligations with respect to oversight of your

programs and whether you have found in your experience that to be pro forma or in any way lacking?

And let the record reflect a few, not quite eye rolls, but I think the response was, no, they have not found this to be pro forma in any way.

MR. LITT: I've been on this job now for getting on towards five years and I have found nothing about my interactions or our institutional interactions with the intelligence committees to be pro forma.

They have fairly substantial staffs which have a lot of experience. Some of them come from the community. They know, they dig very deeply into what we do. The DNI occasionally uses the term wire-brushing for the interactions that we have with the committees, so it's not a pro forma interaction in any way.

MR. DE: If I could add one point, on programs like 702 that we're talking about today for example, we all lived through the

reauthorization of Section 702 in 2012.

That process was not simply in connection with the intelligence committees, but I can remember numerous briefings where we would go up for a member, for all member briefings that the intelligence committees would host for the Congress.

So I don't want to leave the impression that it's only with the intelligence committees, particularly for a program like 702 that needs to be voted on by all members of Congress on the basis of a sunset clause.

MS. COLLINS COOK: I want to make sure that my colleagues have time for their last round of questions so I'll cede my time.

MR. DEMPSEY: Going back to the minimization procedures question, and specifically the incidental collection question, am I right that the rule is that whether the information is inadvertently collected, that is you were tasking on the wrong selector or some mistake was made and you got something that you didn't intend to get

that's inadvertent, or you were correctly targeting the right account and then you collected communications to or from a U.S. person that's incidental, the procedures say, minimization procedures, rules say that if you never discover that it was inadvertent and never discover that it was incidental, you never realized that it was a U.S. person collection, it's deleted after five years?

The basic rule is you keep it for five years, you keep everything for five years, two years on upstream, five years on PRISM, and then it gets deleted. That's the baseline rule, right?

MR. LITT: Correct.

MR. DEMPSEY: And then you on top of that the rule is that if then you, through analysis, through reviewing it that it was inadvertent or incidental collection on a U.S. person you must immediately purge? Bob's shaking his head.

MR. LITT: There's a difference in the way inadvertent and incidental, as you're using

those terms, are very different concepts.

Inadvertent refers to a collection that was not authorized by law. That is purged.

Incidental --

MR. DEMPSEY: Purged unless?

MR. LITT: Unless, as Raj mentioned, that there are certain exceptions. I'm certainly not able to recite them but they do exist. But they're fairly narrow.

Incidental is collection that is authorized by law. And at that point the rules relating to U.S. persons kick in and if you determine that it has no foreign intelligence value you purge it.

MR. DEMPSEY: Right, but I mean what's your response to the argument, well, fine, that just means that if you think it's valuable you can keep it, if you don't think it's valuable then you purge it?

MR. LITT: But it's lawfully collected.

MR. DEMPSEY: Fair enough. But you do, if it is of interest to you, you do keep it?

MR. LITT: If it's of potential foreign intelligence value --

MR. DEMPSEY: Minimization means --

MR. LITT: If it can be useful to providing the intelligence that policy makers need or to protecting the nation against threats, then yes, we keep it for the required period.

MR. WIEGMANN: So again, to make it more concrete, if it's a terrorist overseas, he is calling a number in the United States that belongs to a U.S. person, we want to keep that information. It is incidental, the fact that we're getting the U.S. person number and we're targeting that non-U.S. person overseas, but he's calling Minneapolis, we want to keep that communication because it's of high interest to us.

MR. DE: One point I would add is just that minimization refers to steps in the process, everything from collection to review to dissemination. And so I think we're talking about one element here, and to retention. And so there are different stages in the process.

To disseminate that information a certain threshold would have to be met and so forth.

MR. DEMPSEY: Yeah, I wish there were some way, I mean I know it's totally now embedded both in law and guideline and practice, but minimization means different things.

Minimization means keep it for five years and then delete it, minimization means don't disseminate identifying information, minimization means delete it unless it's intelligence information. Those are very different.

MR. LITT: Well, they all fall within the statutory definition of minimization essentially. I'm going to mangle it a little bit, but it's procedures that are designed to minimize the acquisition, retention, and dissemination of information about unconsenting United States persons consistent with the need to produce foreign intelligence information.

And so you're going to have different minimization rules based on the particular

missions of the agencies. You're going to have different minimization rules depending on the nature of the activity you're governing. You're going to have different minimization rules depending upon the nature of the information. But minimization is that entire category of rules.

MR. DEMPSEY: But it is a little bit of a circular definition which means different things in different contexts. Sometimes it means you've --

MR. LITT: I'm not sure I'd say circular but I would say it means different things in different contexts.

MR. WIEGMANN: It's a balance.

MR. BAKER: If I could just real quick just to emphasize, you know, as Bob was just alluding to, the FBI does have its own standard minimization procedures with respect to this type of activity. I assume you've had access to those.

So anyway, there's a lot on the table that we just talked about with respect to minimization, but I would direct you to those as

well in terms of understanding the FBI's role.

MR. MEDINE: Judge Wald.

MS. WALD: When a U.S. person information that's been, quote, incidentally acquired and kept for legitimate reasons or whatever in the base is disseminated to foreign governments, as is permitted under certain circumstances, it said that it's usually masked.

I think it would be useful for public consumption to know what the masking process entails, and in what circumstances it isn't masked, and whether or not the different agencies can use different criterias for masking or it's all centralized by Justice or the Attorney General's provision.

MR. DE: Well, I can speak just for masking generally at NSA, and abstracting from the second party issue for a moment, is substituting a generic phrase like U.S. person for the name of the U.S. person that is actually collected.

And that U.S. person is a legal term. Obviously that means an individual or it could

mean a U.S. company or firm.

I don't think there's a centralized process. That's how we do it at NSA. I think that's how other agencies do it as well.

MS. WALD: But different agencies decide how to interpret their own criteria as to what should be masked and what shouldn't?

MR. LITT: It's part of the, in the 702 context it's part of their minimization procedures.

MS. WALD: Well, so what does that tell me? No, I mean specifically as to whether or not in what circumstances it's not masked, that's up to each agency, or not?

MR. LITT: Yeah, it's done on an agency by agency basis.

MR. WIEGMANN: But generally speaking, I think the minimization rules of each agency generally would not permit you to disseminate U.S. person information where that is not either foreign intelligence or necessary to understand that foreign intelligence. So in other words --

MR. DE: Or evidence of a crime.

MR. WIEGMANN: Or evidence of a crime for FBI.

So in other words, if I need to, if it's Joe Smith and his name is necessary if I'm passing it to that foreign government and it's key that they understand that it's Joe Smith because that's relevant to understanding what the threat is, or what the information is, let's say he's a cyber, malicious cyber hacker or whatever, and it was key to know the information, then you might pass Joe Smith's name.

If it was not, if it was incidentally in the communication but was not pertinent to the information you're trying to convey, then that would be deleted. It would just say U.S. person. It would be blocked out.

So they were in communication with, and it would just say U.S. person. So that's essentially how it works I think more or less in all the agencies. Is that a fair description, Raj?

MR. DE: Yeah, the basic parameters for FISA collection are articulated in the statute, the big principles of necessary to understand foreign intelligence or evidence of a crime. And then that's effectuated through the minimization procedures that each agency has. That's for 12333 collection. It's articulated, as Bob mentioned, in 12333.

MS. WALD: With those last subpart, would those, just take NSA as an example, would those mask criteria also include foreigners, non-U.S. person's information?

I mean suppose the government of Romania asks some question which might require a Rumanian non-targeted person who's in your PRISM base, would these masking procedures, etcetera, apply there too or are they just for U.S. persons?

MR. DE: In today's rule, masking procedures are for U.S. persons because they are derivative of the constitutional requirement, the minimization procedures that need to conform with the constitutional parameters for U.S. persons.

MS. WALD: So it would be up to the agency to decide whether they thought it was right or wrong to give that information to a foreign government?

MR. DE: I think there's two points to mention. One is no information would ever be disseminated unless it had foreign intelligence value.

MS. WALD: No, I know.

MR. DE: That's the entire point of disseminating that information.

MS. WALD: But having made that decision in terms --

MR. DE: If I may continue. The second point is that I think what the President has directed the DNI to examine in the PPD is what protections could be extended to non-U.S. persons. That's the study.

MS. WALD: And that's what you're working on?

MR. DE: That's the issue we're evaluating now.

MR. BAKER: One quick comment though. If I'm not mistaken, if you look in 50 USC 1806, which is Title I of FISA but I think also applies to Section 702, it says, and I don't think it restricts it with respect to U.S. person or non-U.S. person, that no federal officer or employee can disclose, can use or disclose information at all except for a lawful purpose.

So the information could only be disclosed for a lawful purpose. And I believe that's across the board.

MS. WALD: I don't have anything more.

MS. COLLINS COOK: I wanted to make sure I understood though both Judge Wald's question and the response.

I understood her to be asking under what circumstances dissemination could be made to a foreign government.

Are there separate agreements and procedures that might govern in that instance or are analysts able to simply decide they would like to provide foreign intelligence information to

foreign governments?

MR. DE: At least our procedures, our publicly available procedures have provisions that address sharing with second party partners. I don't have at my fingertips the details, but I can certainly get back to you on that. But they are now public and articulate the circumstances under which information can be shared with second party partners. Those procedures are approved by the FISC annually.

MR. LITT: I think that the critical point is that these are part of the minimization procedures that have to be approved by the FISA court to the extent we're talking again about Section 702.

MS. WALD: The minimization procedures are only for U.S. persons, aren't they?

MR. LITT: Yes, that's right.

MS. WALD: But I was talking --

MR. LITT: But there are general rules about when we can share FISA information.

MR. MEDINE: All right. Well, I want

to thank the panel very much for spending a fair amount of time with us today and discussing these issues in a public setting and we appreciate it.

And we'll take a short break and then we'll resume at eleven o'clock with our second panel. Thank you.

(Off the record)

MR. MEDINE: We're now ready to begin our second panel, and we are very pleased to be joined by Laura Donohue, who's a Professor of Law at Georgetown University Law School, Jameel Jaffer, for a return engagement, Deputy Legal Director at the ACLU, Julian Ku, who's a Professor of Law at Hofstra University, and Rachel Levinson-Waldman, who is Counsel for Liberty and National Security Program at the Brennan Center for Justice, and each will make a brief set of remarks, if you want to start.

MS. DONOHUE: Sure. Thank you very much for the opportunity to be here today. I'm looking forward to the discussion on 702.

I'd like to confine my remarks to four

central areas, just my initial remarks, and raise statutory and constitutional concerns.

First is with regard to targeting. I'm particularly concerned about four areas here. First is the inclusion of information about targets, and not just to or from targets.

Second is the burden of proof regarding whether somebody is a U.S. person or not.

Third is with regard to the burden of proof regarding the location of the individual. That is, if the NSA in either instance does not confirm, does not actually know where they are, the assumption that is built into the minimization and targeting is that it is neither a U.S. person, nor are they domestically located. And there is no affirmative duty for due diligence on the NSA to actually check their databases to find out if that individual is or is not a U.S. person and is or is not in the United States. And then the implications for the right to privacy.

In the second area on the post-targeting analysis, I'm particularly concerned

about the role of FISC, that it's severely circumscribed and that we're having warrantless searches.

So in the last panel we heard about that moment at which the information is obtained is not a search because it's foreign intelligence and there's an exception for the gathering of the intelligence.

But when information is then used for criminal prosecution, then at that point when the data is searched, if it were a case where if I were, say, speaking with a mobster in the United States and they happened to overhear incidental to my communications that I was engaged in other criminal activity, they would have to go to a court to obtain a warrant to then put a wiretap on my phone and listen to the content of my communications.

In this situation they don't do that and then they find that individuals are implicated in criminal activity and refer it for criminal prosecution.

And I would be happy to address the 2002 Foreign Intelligence Surveillance Court of review opinion that addressed this aspect, but it was with regard to Title I where there was probable cause that had already been established that the target in that case was a foreign power, an agent of a foreign power.

In this particular case, the individual is not themselves the target of any investigation and so the prerequisite Fourth Amendment threshold has not been met.

The third area is the retention and the --

MS. COLLINS COOK: Can you slow down just a bit? I can't keep up. Thank you.

MR. MEDINE: And we also have a court reporter who's probably her fingers are slowing down.

MS. DONOHUE: Sorry, I beg your pardon. I realize we only have a few minutes, and I also have written remarks which I'll be submitting.

MS. COLLINS COOK: I have reviewed

them. Thank you. I've reviewed what you've submitted thus far.

MS. DONOHUE: Right. So I will be submitting on these particular points following the hearing.

On the third area, the retention and the dissemination of data, and this came up with Judge Wald's question on the previous panel, there are a number of exceptions in terms of when the information itself has to be expunged.

The foreign intelligence information exception I would direct your attention to. It's not defined in either Section 702 specifically, or in the minimization or targeting procedures.

It is, however, defined in FISA to include any information that would be helpful for foreign affairs, which would include economic information, it would include political information, it would include a whole range of data.

The retention, dissemination for criminal prosecution, I've raised the Fourth

Amendment concerns. We're starting to see now in courts what's called parallel construction where individuals where information has come from intelligence agencies' programs, is then passed on to law enforcement, who then must create a parallel trail for probable cause, but the actual tip or initial indication of criminal activity came from intelligence.

And it essentially covers the traces that this initially arose within FISA or within Section 702, and I have increasing concerns, certainly as a scholarly matter, about the growth of parallel construction.

The client attorney privilege you had already mentioned in the last panel. That continues to be, I think, an area of some concern, not just because it's, not just in the post-indictment stage but in terms of all communications with attorneys prior to and in the context of the interception of content.

The retention of encrypted communications was not mentioned in the last

panel. All encrypted communications are retained according to NSA documents, as well as the technical barriers. If there are technical barriers they also will simply keep the information.

The other aspects of this have to do with multiple databases and CIA access, which I was surprised you didn't have the General Counsel of the CIA on the last panel. We now understand from NSA documents that the CIA has a separate set of minimization procedures and also uses Section 702. And I think that's important to take a look at what those procedures are, both the targeting and the minimization.

Finally, the fourth area that I'd just like to raise is the First Amendment concerns that I have. As has been well-recognized in the judicial system, First and Fourth Amendments often travel hand in hand, especially in national security when political matters are on the line.

And in this particular instance not only do we have a general First Amendment concern

but we know that if individuals visit IP addresses, for instance, that have been associated with particular targets, then their correspondence, communication, emails, etcetera, and other information is also retained.

What if that IP address is Al Jazeera, let's say? What if that IP address happens to be a media or a news site that's been associated with a particular area of concern? Then I think there are also First Amendment implications that follow from that.

So in conclusion I'd be happy to talk in more detail about each of these areas, the targeting, the post-targeting analysis, the retention and dissemination of data, and the final First Amendment concerns.

MR. MEDINE: Thank you very much. Mr. Jaffer.

MS. DONOHUE: Thanks.

MR. JAFFER: Thanks for the opportunity to appear before the Board.

The ACLU's view, as you already know,

is that Section 702 is unconstitutional. The statute violates the Fourth Amendment because it permits the government to conduct large scale, warrantless surveillance of Americans' international communications, communications in which Americans have a reasonable expectation of privacy.

In our view, the statute would be unconstitutional even if the warrant requirement didn't apply because the surveillance it authorizes is unreasonable.

As I discuss in more length in my written testimony, the statute lacks any of the indicia of reasonableness that the courts have looked to in upholding other surveillance statutes, including Title III and FISA.

But the point that I would like to emphasize today is that even leaving the constitutionality of the statute to the side, the government is claiming and exercising more authority than the statute actually gives it.

I say that for three reasons. First,

while the statute was intended to augment the government's authority to acquire international communications, the NSA's minimization and targeting procedures give the government broad authority to acquire purely domestic communications as well.

That's because the NSA's procedures allow the agency to presume that its targets are foreign, absent specific evidence to the contrary, and because the procedures don't require the government to destroy purely domestic communications obtained inadvertently.

Instead, they permit the agency to retain those communications when they're believed to contain foreign intelligence information, a phrase that is defined very broadly.

Second, while the statute was intended to give the government authority to acquire communications to and from the government's targets, the NSA's procedures also permit the government to obtain communications that are merely about those targets.

And that practice, in my view, finds no support in the language of the statute or in the statute's legislative history. But it's a practice that has profound implications for individual privacy.

In order to identify the communications that are about its targets, the government has to inspect every communication. To endorse the practice of about surveillance is to say that the government can surveil literally everyone, or at the very least that it can surveil every communication in and out of the country.

Finally, while Section 702 prohibits reverse targeting, the NSA's procedures authorize the government to conduct so-called back door searches, searches of communications already acquired under the FAA using selectors associated with particular known Americans.

Given the absence of any meaningful limitation on the NSA's authority to acquire international communications under Section 702, it's likely that the NSA's databases already

include the communications of millions of Americans.

The NSA's procedures allow the NSA to search through those communications and to conduct the kind of targeted investigations that in other contexts would be permitted only after a judicial finding of probable cause.

And if I have thirty more seconds I would like to make just one final point. Today we're focused on Section 702, but it's important to understand that Section 702 is merely one expression of a broader philosophy.

Yesterday the Washington Post reported that the NSA has built a surveillance system called MYSTIC capable of recording all of a country's phone calls, allowing the NSA to rewind and review conversations as long as a month after they take place.

MYSTIC is the logical endpoint of the arguments that the government is making here today. So the stakes and the conversation that we're having today are very high. It's very

difficult to believe that democratic freedom would survive for long in a system in which the government has a permanent record of every citizen's associations, movements, and communications. Thank you.

MR. MEDINE: Thank you. Professor Ku.

MR. KU: Thank you, and thanks also for the opportunity to appear before the Board today.

I just want to remind -- I have a different view I think from most of the panelists, and I apologize for not getting my remarks ahead of time.

I just want to remind the Board of two under-emphasized points of constitutional law that I think should frame our understanding of the U.S. government's surveillance practices under Section 702.

I mean first, it is important to remember that Section 702 and FISA itself need to be interpreted and understood against the history, and tradition, and the background of the President's broad, inherent executive power under

the Constitution to conduct electronic surveillance of foreign governments and foreign agents, especially overseas.

Second, although we often speak loosely of the Fourth Amendment's limitations on this presidential foreign surveillance power, it's worth noting that courts have repeatedly upheld wide-ranging, warrantless U.S. government surveillance overseas, even of U.S. citizens.

So these two constitutional observations should frame any legal assessment of Section 702 and FISA in general.

If you keep in mind the background and where we're coming from rather than where we are, 702 is not an ineffectual attempt to regulate lawless executive conduct, as the critics would have it.

In actuality, Section 702 almost certainly requires more limitations than are actually required by the Constitution and may even, although I'm not taking that position, but could in some circumstances encroach on the

President's foreign affairs powers to conduct foreign intelligence activities.

So let me just briefly elaborate on these two claims about constitutional law, which I'm sure some folks might disagree with, but this is not a dispute that U.S. presidents have long exercised the power under the Constitution to conduct foreign intelligence, and this uncontroversially flows from the President's role as the chief of foreign affairs under the Constitution. And almost every court considering the question has concluded that the President, has agreed that the President possesses an inherent constitutional authority to conduct foreign surveillance. And this is undisputed by any court.

In other words, there does not need to be statutory authorization for the President to engage in foreign surveillance.

Prior to the enactment of FISA in 1978, the executive branch claimed, and the courts did not dispute that it possessed a broad

constitutional power to conduct surveillance for foreign intelligence purposes, even inside the United States and usually without a warrant.

So prior to the enactment of Section 702 and its predecessors, the executive branch claimed a constitutional power to conduct warrantless surveillance in foreign countries for foreign intelligence purposes, whether or not that surveillance included a U.S. citizen who was physically overseas.

So given this history I'd ask the Board to keep in mind that Section 702 and its predecessors placed more constraints on the executive branch's conduct of overseas foreign intelligence gathering than has ever been imposed in prior, in the past.

You might conclude that we need even more constraints, but we should not kid ourselves that existing constraints or even more constraints as proposed by some other folks, are consistent with historical practice and tradition and moves us further toward constraints.

As to my second point, I do not believe the Fourth Amendment imposes limitations on foreign intelligence as strict as those employed, imposed by Section 702. And let me just briefly explain the two reasons why.

First, it is very clear the Fourth Amendment does not apply to non-U.S. citizens and when they are outside the territory of the United States. And the Supreme Court confirmed this in the 1990 decision of The United State versus Verdugo-Urquidez.

So foreign citizens or the surveillance of foreign citizens outside of the United States is completely unconstrained by the Fourth Amendment.

Second, the courts have confirmed that it's highly unlikely the Fourth Amendment's warrant requirement applies to surveillance of U.S. citizens when they're outside of the United States, especially when the surveillance is conducted for foreign intelligence purposes.

No court in the United States has held

that a warrant is required for a search of a U.S. citizen when they are overseas if that search was conducted for foreign intelligence purposes.

Some courts like the second circuit have even held that no warrant is ever required for an overseas search, while others have relied on a broader foreign intelligence exception.

So there is further details here about the reasonableness, and courts have generally interpreted the Fourth Amendment's reasonableness requirement very generously in favor of the government when conducting overseas searches.

Again, in light of this long history and tradition of the United States conducting essentially unsupervised foreign intelligence gathering without any statutory authority, this is actually the tradition in the U.S. system prior to the enactment of FISA, then more recently Section 702.

So just to conclude, if you look at Section 702, the government faces a complete ban on the intentional targeting of any United States

person reasonably believed to be outside of the United States. And there are other procedural mechanisms, as you know about.

But I don't believe that actually the Fourth Amendment would actually require if there was no Section 702, the Fourth Amendment would require that the government could not intentionally target a U.S. citizen overseas and their communications.

So let me just conclude, I believe Section 702 should be understood as a sensible compromise between privacy interests and the continuing need to conduct aggressive foreign intelligence gathering. Congress has given its blessing to broad-based overseas surveillance that was already occurring pursuant to the President's inherent constitutional power.

Congress has now imposed limitations on those activities that go beyond what I believe the Fourth Amendment requires, but I think that's a small price to pay, and many of us agree, to minimize privacy intrusions into Americans'

overseas communications. And the courts are involved to provide oversight.

This is the type of political compromise and cooperation between different parties and different branches of government that we always wish, we always say we want, and so I think we should applaud it rather than condemn it.

MR. MEDINE: Thank you.

Ms. Levinson-Waldman.

MS. LEVINSON-WALDMAN: Thank you, of course, for having me here. I have a few brief comments and then I hope we'll also have a chance at some point potentially to respond to comments that were made during the first panel or during this panel.

So I'm just going to focus briefly on two primary issues that are reflected in my written submission for now.

First, I know of course that the Board is particularly interested in whether this about collection complies with the letter or spirit of Section 702. And based on the structure of the

statute, we believe that it doesn't.

Briefly, there are two main restrictions reflected in Section 702 on the collection of communications. So that would be the first, the acquisition cannot target U.S. persons or persons known to be within the United States. This is a geographic or nationality and residence restriction.

And second, that the purpose of the acquisition must be to acquire foreign intelligence information. And that's basically a content restriction. What that means is that the content of the communications that can be picked up by electronic surveillance is regulated by the foreign intelligence restriction, while the class of people who are subject to electronic surveillance is regulated by the targeting restrictions.

When communications that are about a target are collected, we believe sort of the what and the who of the collection are conflated, and that that's contrary to the clear structure of the

statute.

And we know that the results of the collection, our intention with the foreign intelligence requirement of the statute, that is, if communications that merely mention certain targets are collected then we know that significant quantities of communications that contain no foreign intelligence information whatsoever are acquired, which would appear to undermine the significant purpose requirement in the statute.

And of course this has been confirmed in the 2011 FISC opinion that was referred to that's been declassified. We learn in fact that the NSA does acquire tens of thousands of wholly domestic communication in the course of conducting that about collection.

And so for those reasons we do think that the about collection is contrary to the meaning and the structure of the statute.

And second, let me briefly mention one of the main contributions I think the Board can

make as part of its review, and I think that some of these questions came out in the first panel, which is to shed more light on some of the ways that Section 702 is being used.

It appears that what we don't know about Section 702, certainly for the public, still outweighs or outnumbers what we do know.

Obviously there will always be things that will be properly classified and kept secret, but it seems that there are many unanswered questions that the Board is in a position to help answer, help shed some light on.

So those questions would include certainly questions about how targets, and selectors, and key words are used. Some of those were answered in the first panel, but I think some of those answers also raised more questions.

There has been the suggestion, the strong suggestion from the 2011 minimization procedures that all encrypted communications can be retained by virtue of their being encrypted, and finding out if that, in fact, is true. And if

not, if the PCLOB can obtain and provide additional information about that provision.

And finally, and this is something that Laura mentioned as well, that domestic communications can be shared with law enforcement agencies if they are reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed.

In addition to raising, I think, a host of constitutional issues at the very least, and practical issues, one of the things that we don't know is whether there are minimum standards for how severe, for instance, such a crime has to be in order to share this information, which of course has been collected without a warrant.

So I hope that the answers to some of these questions also will come out during this process. Again, thank you for the opportunity to address the Board.

MR. MEDINE: Great, thank you very much for your opening statements. I'm going to ask you some questions but any panelist should feel free,

I may ask them to a specific person but anyone should feel free to jump in.

Professor Ku, you talked about the limited applicability of the Fourth Amendment to overseas collections, and maybe, and suggesting there's certainly no warrant requirement and a very generous reasonableness standard.

One question I have is the collections that we're talking about under 702 technically are happening in the United States. That is, the electronic communications provider is in the United States while admittedly the target is outside of the United States. Is that a distinction that you think has any constitutional significance?

MR. KU: That's a great question. I mean I think it reflects the difficulty of this, which is the technology is changing our, the way the Fourth Amendment was interpreted in some of these older cases, right.

So in the classic Fourth Amendment overseas case it was the guy searching through the

house or the apartment physically overseas of the U.S. citizen, or of the phone call that occurred on the foreign networks, right, in the foreign country.

Here we have this kind of weird situation where you have phone or communications sort of transiting through the United States. And I do agree that that might raise a harder Fourth Amendment issue, but I do think that the larger thing to keep in mind is that the geography matters because if there's a foreign person on the other side of the line, so to speak, that's I think in part the way the communication is an international communication. It has different implications for that perspective.

But I do agree that the Fourth Amendment, the territorial aspect of the Fourth Amendment would be less significant in that context.

I think the broader point though is that the courts have been very generous, both domestically and internationally about

surveillance conducted for foreign intelligence purposes.

So even, so the territorial distinction was something that FISA created, because prior to that I think FISA, the foreign intelligence gathering occurred both domestically and internationally, and the fact that it was for foreign intelligence was what mattered.

FISA has created this sort of territorial division, which I think is becoming less important with the changes in the types of communication we have.

MS. DONOHUE: If I may add to that. You know, Professor Ku brings up the exception for foreign intelligence gathering for purposes of surveillance. That's very different from the acquisition of information for purposes of prosecution. And here courts have very clearly ruled that even in cases of national security or domestic security, a warrant is required.

This is U.S. vs. U.S. District Court, a case handed down in 1972 in which there were three

individuals conspiring to bomb the CIA. And the court said that the executive branch, quoting Justice Brownell (phonetic) and others said the court -- the executive branch is not a disinterested neutral observer and cannot be put in the position of having to determine whether a search will be reasonable. They have to seek a third opinion on that.

In Katz as well in 1967, some of the justices in that case, Justice Byron White said, went beyond the decision and said basically we should not require a warrant procedure for the magistrate's judgement if the President of the United States, or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.

And other justices responded very angrily to that statement. Justice William Brennan, Justice William O. Douglas, they pointed out that there was a conflict of interest here. They said, look, neither the President nor the

Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court where the magistrate must be.

The Foreign Intelligence Surveillance Court of Review has also considered whether or not information obtained from FISA warrants could be used in the event of a prosecution.

In the case that brought down the wall in 2002, the court looked to Title I of FISA where probable cause had been established that an individual was a target, sorry, that the target was a foreign power or an agent of a foreign power and said in that case you have this review that has gone on specific to that target by the Foreign Intelligence Surveillance Court.

In Section 702, individuals who may be brought up on criminal charges are not themselves the target of any investigation. No probable cause has been established for their involvement as a foreign power or an agent of a foreign power.

Instead, once the content of

conversations are obtained, then the government may go through, analyze the information and look for evidence of criminal activity, which can then bring them into a courtroom to face criminal charges, and at no point is this warrant requirement, which the court has held for domestic security cases. So here you have a U.S. person on U.S. soil and the court has said in U.S. vs. U.S. District Court, you have to have a warrant in that situation.

So to use the veneer of, well, we're just collecting foreign intelligence and the executive branch has the right to do this under Article II, yes, perhaps the executive branch can gather intelligence but if there are criminal penalties associated then you also need to meet the requirements of the Fourth Amendment for U.S. persons.

MR. MEDINE: I'd like to give Professor Ku a chance to respond, although I can do it on my next round.

MR. KU: Okay. Well, I mean I'm not

going to go through all the cases. And I think that the way I understand this is the way you think about this is the foreign intelligence purpose, right. The foreign intelligence purpose has been sort of an important part about whether there's an exception to the warrant requirement, or if there's a foreign intelligence purpose, sometimes a primary purpose, or a purpose, depending on how you define it. And then there's the, whether that gives a question of reasonableness, where there's legitimate government interests that goes to the reasonableness.

The reason I'm emphasizing the significance of the foreign intelligence purpose aspect of this and the territorial aspect of this is because I do think it's relevant to analysis.

This is, in fact, what's going on here is a collision between our law enforcement and intelligence goals here, right. So the U.S. government is gathering a lot of information for foreign intelligence purposes. It's also using

sometimes that information.

Some of that information is, although not I think so far frequently, leaking into criminal prosecutions. But if we start from the perspective of foreign intelligence gathering, right, this is Article II, this is where we start, and this is something that's largely been unregulated.

What's changed is that the nature of communications have changed so that many of the communications that were essentially gathered unsupervised for foreign intelligence purposes are being sort of routed in a different way so that it falls within, technically speaking, what we might consider a different sort of format, which then looks more like a classic Fourth Amendment case.

But I think that the larger point I'm trying to emphasize here is that this is, there are real Fourth Amendment issues here with respect to law enforcement.

But this is also about foreign intelligence gathering. It's not just a total

sham. It's not as if the government is claiming here that this whole thing is a scheme in order just to gather information for criminal prosecution.

Essentially they're both interests here that are part of this analysis. And that legal analysis with respect to foreign intelligence gathering needs to be considered and it should frame our analysis of what's going on here as well.

MS. BRAND: Thank you. So it's a good segue actually what you said, Professor Ku, because I want to understand, Professor Donohue, what you were saying, and I may not have taken the best notes, so forgive me.

But walk me through the argument, because a second ago you said that you were making a distinction between collection for foreign intelligence purposes and I think you said collection that was focused, was for the purpose of prosecution.

So are you, is it your view that 702

collection is for the purpose of prosecution?

MS. DONOHUE: It's one of the two stated purposes for which the information can be retained once it is collected. So it can be --

MS. BRAND: But that's different. But I'm asking about you said collected for the purpose of prosecution, I thought. I mean what is, I guess what I'm trying to get at is, is this distinction between foreign intelligence purpose and criminal purpose relevant at the collection stage only, or at all stages, or what? Help me understand what you're talking about.

MS. DONOHUE: Yeah, so in the previous panel Brad addressed this point. He mentioned that in the context of it's the moment at which the information's obtained that a search occurs, right.

So if we do our Fourth Amendment analysis at that point, then the moment at which you're obtaining the wiretap evidence is the search, at which point you would require a warrant under these.

And I believe Professor Ku's point is, no, you don't need a warrant if it's for foreign intelligence purposes at the moment you acquire the information with the international nexus to it. And he's citing Verdugo-Urquidez where there was no nexus to the United States and a search occurred overseas.

The problem is in the case, and this gets back to my first point, which I apologize if I spoke too quickly at the beginning of the panel, which is with regard to the targeting. If it is not just information to or from the target, or held by the target, but any information about or relating to the target.

And here, it's interesting, I was a little bit confused by the earlier panel because according to the actual documents the NSA has released, the NSA can actually use computer selection terms and other information such as words, or phrases, or discriminators to scan content.

So if it can collect all of the

international communications and then scan the content of those communications, then I would argue that is a search for purposes of the Fourth Amendment at the point of collection.

MS. BRAND: But let me get to this distinction though between foreign intelligence and a criminal purpose, because 702 requires not only that the collection be a non-U.S. person abroad but also that there be a foreign intelligence purpose, that the information be reasonably believed to be, to collect foreign intelligence. I'm not quoting the statute.

But doesn't that statutory requirement suggest that it has to be for a foreign intelligence purpose? And it might also then collect evidence of a crime, which then there are procedures for what to do with that information.

But it seems like you're suggesting that you think that the collection itself is for a criminal purpose, and that's what sort of piqued my interest and I wanted to understand what you were saying there.

MS. DONOHUE: Sure. So to push on this a little bit, under FISA to be a foreign power one is not a U.S. person, right, one is a foreign power or an agent of a foreign power. Not all of the agents of a foreign power require criminal showings, but many of them do.

So to say that this is purely a foreign intelligence purpose when an individual can be targeted based on being either a foreign power or an agent of a foreign power, in which case there is criminal activity involved and there may be the element of criminality from the outset. So it's not as though criminality is not an aspect of the foreign intelligence gathering generally.

MS. BRAND: Professor Ku, do you have -- Jameel, it looks like you wanted to respond.

MR. JAFFER: Well, I was just going to speak to the foreign intelligence exception more generally, if you want to pursue this.

MS. BRAND: Go ahead. Go ahead.

MR. JAFFER: Well, so I just want to caution the Board about starting from the premise

that there is in fact a foreign intelligence exception to the warrant requirement. The cases in which courts have held that there is such an exception predate FISA. There's arguably one exception to that, but the vast majority of them predate FISA.

And so their rationale has been undermined by practice under FISA over the last thirty-five years. The rationale for those cases was in large part that the courts might not be capable of overseeing collection or surveillance for foreign intelligence purposes. But the courts have been doing precisely that now since 1978.

But even if you accept that there is in fact a foreign intelligence exception to the warrant requirement, you have to ask the question of how broad that exception is.

And all of those cases, those pre-FISA cases, involve cases involved situations in which there was probable cause to believe that the target was a foreign agent, the surveillance was approved personally by the President or the

Attorney General, and the primary purpose of the surveillance was to gather foreign intelligence information.

And Section 702 doesn't include any of those requirements. So no court has ever approved a foreign intelligence exception to the warrant requirement that is broad enough to read Section 702. Section 702 is a broader statute than any foreign intelligence exception recognized so far would allow.

I think that it may also be important to emphasize that concluding that the warrant requirement applies doesn't mean that the government has to get a warrant before surveilling legitimate foreign targets. It doesn't mean that in order to surveil, you know, some suspected terrorist outside the United States the government necessarily needs to get a warrant.

But at the very least it means that the government needs to take reasonable measures to avoid acquiring Americans' communications without warrants.

It means it has to not acquire them in the first place where it cannot acquire them.

When it does acquire them, it has to destroy the communications that it acquires relating to U.S. persons.

And when in narrow exceptions it retains those communications, there should be a back-end warrant requirement so the government doesn't access Americans' communications without a warrant. That's what compliance with the warrant clause would mean.

MR. MEDINE: Ms. Cook.

MS. COLLINS COOK: So thank you all for coming. I find these panels to be incredibly helpful and informative.

Ms. Donohue, I would like to -- Professor Donohue, I apologize, I'd like to follow-up on something you mentioned at the very end of your opening remarks, and that's your position that 702 raises First Amendment concerns.

I think it's clear from my previous separate statement on our 215 report that I don't

necessarily approach the First Amendment analysis the same way, but what I would find helpful from you is if you could just describe your approach to when the First Amendment would be implicated, when concerns arise, and when something would be unconstitutional based on First Amendment concerns.

So for example, would a traditional wiretap raise First Amendment concerns, and would it potentially be unconstitutional under First Amendment concerns?

Would a traditional grand jury subpoena for bank records or credit card statements that could reveal payments to lawyers or payments to various charities or associations, would that raise First Amendment concerns? Would it be unconstitutional under the First Amendment?

So if you could just walk me through on the spectrum where you're finding concerns and where you're finding violations.

MS. DONOHUE: Sure. And just to return back to Ms. Brand's point, I agree with Jameel on

the analysis about what point it would kick in for a warrant requirement is the point at which it's either about the information, because I feel like I didn't quite answer what you were asking me and I want to make sure that I do, I answer it.

It's the point at which you're getting information about that particular individual, which is a different target, and then you analyze that information, then at that point I would believe that the Fourth Amendment warrant requirement would apply.

Okay, so in response to the First Amendment question, so the courts have recognized that there is a close link between the First and the Fourth Amendment. And I frequently find whether it's in remote biometric identification systems in view of public space and facial identification, you know, that there is a First Amendment context there as well. So it tends to be in the shadows in the room.

In this particular context, the way that I see it present is with regard to the target

that is in the statute. It's very clear that the target cannot be selected --

MS. COLLINS COOK: I'm sorry, can you actually answer the question that I had posed, which was, for example, starting with a traditional --

MS. DONOHUE: Oh, yeah, so I do not see a traditional wiretap as implicating First Amendment. I do not see --

MS. COLLINS COOK: Why?

MS. DONOHUE: Because --

MS. COLLINS COOK: Even though it could, for example, reveal the fact that I belong to the ACLU, or I have called my attorney, or I'm discussing, you know, private contents and communications. So why not?

MS. DONOHUE: Because there's a balancing that occurs with regard to the element, in this case of probable cause that you have committed, are committing, or are about to commit a crime under Title III, in which case having gone before a neutral, disinterested magistrate, a law

enforcement officer says, oh, no, I suspect that Professor Donohue is engaged in this bad activity. And I think that that balancing test basically takes that situation out of a First Amendment context.

MS. COLLINS COOK: So let's take a grand jury, and then a pen register trap and trace. So a pen register trap trace, there's definitely no determination, no probable cause. So does a traditional pen register trap trace, which would reveal potential phone calls to the ACLU, to my lawyer, very private, the existence of potentially private conversations, does that violate the First Amendment?

MS. DONOHUE: Again, with prior judicial approval and review, no.

MS. COLLINS COOK: Okay. So let's take a grand jury subpoena which can be issued by a prosecutor. So in the absence of beforehand judicial review, does that violate the First Amendment?

MS. DONOHUE: No. I would say --

MS. COLLINS COOK: So what's the factor --

MS. DONOHUE: Well, it's the same for administrative warrants, I would say in the case of administrative warrants. Here's where the tipping point is for me with PRTT, let's take Section 215 as kind of a bulk metadata collection program, or Section, what is it, 402, right, for these bulk collections of pen register trap and trace type information.

When you have the bulk collection of information in a way that changes the political discourse in society, then I think you have a First Amendment question that arises.

MS. COLLINS COOK: Okay. So is if there is a perception that there is a change in political discourse, then you have a concern about a First Amendment? It's not necessarily prior judicial review, particularized probable cause?

I'm just struggling to understand, you know, at what point there's a First Amendment implication and at what point there's a First

Amendment violation, because to me, I think it's a bit of a sea change to look at either traditional or really these FISA authorities as violating the First Amendment. I do think that that's a fairly novel approach.

MR. JAFFER: But to be fair -- to be fair, the distinction between individualized surveillance and bulk surveillance is also a bit of a sea change. And so I think the question is whether the bulk surveillance, the fact that the government is now engaged in bulk surveillance, I mean I understand that there's some dispute over the vocabulary, but the fact that the government is engaged in bulk collection or bulk acquisition of this information makes the First Amendment relevant in a way that it perhaps wasn't relevant in the context of individualized surveillance of the kinds that you were describing.

I mean I think that your question perhaps goes more broadly to the question of incidental overhears, you know. When the government defends Section 702, one of the

government's defenses is that all of this information is, about Americans is overheard incidentally.

You know, I go into this in a little more detail in my written submission, but I don't think it's fair to call this kind of collection incidental in any conventional use of the term. The collection of Americans' information is entirely foreseeable, and in fact, it was the purpose of the statute.

If you look at the statements that administration, then Bush administration officials made to justify the statute or to advocate for the statute, they were quite forthright about the purpose of the statute. And the purpose in their view was to give the government broader authority to collect information, collect communications between people outside the United States, and people inside the United States.

And obviously there's no illegitimacy to the government's interest in collecting those communications. The question is whether there are

sufficient safeguards in place, but that's why I say that incidental is probably the wrong word.

But if the government is relying on the incidental overhear cases from the Fourth Amendment context, those cases were, involved very different contexts. Those were cases in which the surveillance was individualized. It was based on a probable cause warrant.

The scale of the surveillance of the incidental collection was much different. And the fact that there was judicial oversight at the front-end provided a kind of protection for incidentally overheard people that doesn't exist under a statute like 702.

MR. MEDINE: Let's give Jim the chance to ask some questions, then we can come around.

MS. DONOHUE: Okay.

MR. DEMPSEY: Thanks. Thanks to the witnesses.

A question for Jameel and for Rachel on the abouts. What actually is, quoting the words of the statute, what is the strongest textual

argument against about surveillance?

Because the statute says the targeting of persons, never really refers to even the collection of communications or interception, etcetera, so if you're collecting something about somebody, isn't that almost paradigmatically targeting the person? Where's the text?

MS. LEVINSON-WALDMAN: I mean I think one of the -- right, there's obviously ambiguity in the statute in part, and this is one the things that I mentioned in the written submission is that target isn't defined.

And I have to say some of the answers in the first panel, which answered some questions about target and selectors, I think also opened up new questions.

I do think the strongest statutory argument, literally looking at the language, is what the statute talks about.

So it says here, literally just looking at 1881 A, subpart A, Attorney General and Director of National Intelligence may authorize

jointly the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information.

So as I say, you sort of see implicitly, but I think you do see implicitly these two sort of halves of the targeting requirement, the foreign intelligence requirement and this kind of nationality and geographic restriction, and that when what you're doing is collecting about communications, what you're doing is kind of adding together, you're kind of conflating, you're morphing together these different parts of the statute so that the targeting has usually been literally thinking about the facility that's being used --

MR. DEMPSEY: Excuse me. The government has determined that a person is outside the United States and that collecting information about that person will yield foreign intelligence.

MS. LEVINSON-WALDMAN: Well, but I think that may be what's suggested by the about collection, but I think the foreign intelligence

determination is a separate one, right.

The government identifies these targets or selectors which have generally been to or from. And in fact we know, especially from Judge Bates's opinion that thousands, tens of thousands of communications are collected using the about targeting, the about collection, that are wholly domestic, that have no foreign intelligence value, which I think undermines an argument that there has been some determination of foreign intelligence value there, because to some extent the results are sort of speaking for themselves.

MR. DEMPSEY: Because then you would be questioning the legitimacy of the to and froms because they only do abouts about people that they also do to and froms, so you can't say that the foreign intelligence determination of the abouts is illegitimate because then you call into question the to and from.

MS. LEVINSON-WALDMAN: Well, but I think the to and from is pretty clearly contemplated by the statute, right? You target a

person, you are trying to find communications to or from them, understanding that those will have foreign intelligence value.

MR. DEMPSEY: Let me go to Jameel. Jameel, what is the best textual argument against abouts?

MR. JAFFER: Right. Well, let me first I think agree with what I think Rachel was saying at the outset, which is that the statute I don't think explicitly forecloses about surveillance or explicitly authorizes about surveillance.

But I think a fair assessment of the statutory structure and some of the statutory text leads to the conclusion that about surveillance was not contemplated by Congress. And I'll answer your question.

MR. DEMPSEY: The text, yeah.

MR. JAFFER: So here are a few aspects of the statute that I think show that Congress was contemplating, that the target would, himself or herself, be the person whose communications were acquired.

First, a definition of electronic surveillance. It says the acquisition of the contents of any wire --

MR. DEMPSEY: This is not electronic surveillance. 702 explicitly does not cover electronic surveillance.

MR. JAFFER: Well, I think that the point I'm making is relevant nonetheless.

MR. DEMPSEY: Electronic surveillance definition is irrelevant to 702. It is not -- 702 does not regulate electronic surveillance.

MR. JAFFER: I think the point that I'm trying to make is just that the entire statutory scheme, both FISA and the FAA, contemplate that the person who is the target will be the person whose communications are actually acquired.

If you look at the definition of aggrieved person, for example, which does apply in the FAA context, aggrieved person to implicitly contemplates that the person who will be raising the claim as an aggrieved person is a person whose communications are actually acquired.

And in fact, if you conclude otherwise what you are concluding is that the target would be an aggrieved person even if his or her communications weren't acquired, which I think is a nonsensical conclusion and one that the government itself would reject.

But I think it follows from accepting that about surveillance is contemplated by the statute.

And if I could just make a sort of broader point about about surveillance, we have sort of combed through the legislative history for discussions of this kind of surveillance, and it's possible we overlooked something, but we have not found any exchange in the legislative history around the FAA that suggests that Congress was contemplating about surveillance.

To the contrary, when people discuss, when legislators discuss the kind of surveillance that would take place under the statute, they discuss surveillance of the target.

And even on the government panel this

morning one of the panelists used the example, bad guy at Google.com, you know, which again is suggesting that the surveillance that's going on is of the target himself or herself.

And in defending the statute before the Supreme Court, the Solicitor General and the Justice Department more generally characterized the statute as one that allowed the government to collect targets' communications.

So you know, I think that this is an entirely a foreign concept, foreign to the legislative history and foreign to the text of the statute.

MR. MEDINE: Thank you. Judge Wald.

MS. WALD: Let me pick up on the about thing and pose one of those terrible hypotheticals. If you had a to and from, you had a targeted, a legitimately targeted person and in the process of collecting information you got, you came across this email between, I'll be facetious a bit, the grandmother of one of them to the grandmother of somebody else saying something

along the lines of, my grandson was talking to me and he was telling me all about this wonderful service he did by plotting, I'm using an extreme, plotting to blow up a facility kind of thing, I mean how would you take care of that situation where you had it between two people who are not the to and froms? You wouldn't ignore it, would you, or would you? I mean how would you handle that if you had no abouts?

MS. DONOHUE: I'm not sure whom that's directed to.

MS. WALD: I don't care.

MR. MEDINE: Who would you like it directed to?

MS. WALD: What?

MR. MEDINE: Who are you asking?

MS. WALD: Well, the two people who've talked about what about abouts, Mr. Jaffer and Ms. Levinson-Waldman, I think.

MR. JAFFER: Well, I'm not a hundred percent sure I understand the question. The question is, you know, if you were conducting

about surveillance and you come across evidence of a terrorist plot, do you really expect them to ignore it? Then no, I don't, you know.

But that's like asking, you know, if the government breaks into a home unconstitutionally and finds evidence of a terrorist plot, do I expect them to ignore it? I don't.

But we still need to ask the question what are the proper limits on the government's surveillance authority in the first place, and I think that we need to draw those limits in a way that's consistent with the Constitution.

I'm not sure that I'm answering your question.

MS. WALD: Well, you are except that I'm puzzled, too. I'm not sure I know the answer where, as I say, you had -- maybe that's an extreme example about where they have a plot, but where there's actually some foreign intelligence information which even everybody would agree had some relevance to a legitimately targeted

individual, and it's right there, and it's picked up.

MS. LEVINSON-WALDMAN: Then I think I would echo Jameel's points to some extent and sort of elaborate to say that I do think that there are always hypotheticals, presumably for any of these programs, for Section 702, for Section 215, for other collection programs that are going on where there could be some piece of information out there that might be useful that would be collected by a program.

I think it's dangerous to build surveillance programs and to think about the constitutionality and the practicality based on hypotheticals, and especially when we know that there is significant over-collection that occurs and significant collection of Americans' communications.

I think the hypotheticals are, may need to be thought about, but I don't think that they can drive how we think about the constitutionality and the statutory implications of the collection.

MS. WALD: In other words, you or anybody over there wouldn't consider if that happened, some other means that the government might have to take that about information and go to somebody, to some authority and say can we keep this, can we use this, etcetera, etcetera?

MS. DONOHUE: So what I'm a little bit confused about, and I did hear the previous panel say, oh, well, there would be all sorts of procedural implications if we had to return to a judge on the Foreign Intelligence Surveillance Court to get approval to do further monitoring.

What I'm a little bit confused about is if that information was appropriately obtained in the first place and it indicates that other people are implicated, why they wouldn't go back for a Title I electronic search and they would have what they need for that?

MS. WALD: Well, if it's two grandmothers, they're probably not -- they're just chatting. They're probably innocent. All I'm saying is I guess the only reason I raised it is

I'm trying myself to figure out are there not some gray areas here, and wondering if you had any solutions short of about authority which you find is too broad, and completely ignoring it?

But let me not use up my whole five minutes. Thank you.

I did want to ask you about, as you know, the President's review commission said they wanted to see a warrant, an actual, go get a warrant for probable cause before you could search the data using a U.S. person indicator.

My question to you is, and we've heard some reasons why they think that's very onerous, including the fact that the President's review commission's recommendation was it had to be a probable cause warrant that the person was about to commit something, do bodily injury, or about to commit some terrorism crime.

My question to you is if you think there are legitimate, and you do, problems under the Fourth Amendment with using U.S. person indicators to surveil the PRISM data, would

anything short of a probable cause warrant such as they recommended satisfy you, i.e., I'm just throwing this out, you know, having, going back to, say, to the FISA court and having them look at it to see if it, either post or pre, before they used it, approving this so-called, you know, selector, etcetera, that was in fact a reasonable cause to believe that the person had information or didn't have information?

MR. JAFFER: I don't think that would be sufficient. I think that you need a warrant at the back-end and --

MS. WALD: But what kind of a warrant warrants --

MR. JAFFER: A warrant based on probable cause and --

MS. WALD: Probable cause of what?

MR. JAFFER: Well, so I think it could be foreign intelligence probable cause, although I hope that the panel will, that the Board will think about the scope of the definition, the definitions of foreign agent, foreign power, and

foreign intelligence information.

But I think that foreign intelligence probable cause could be sufficient for that particular process, or obviously criminal probable cause.

But I also just want to say that I don't think back-end procedures alone are enough, no matter how strong they are. And I think that, you know, I know that the Board can't talk about the Washington Post report from yesterday, but if you just take it as a kind of hypothetical, you know, if you accept that back-end procedures are enough and that we'll focus solely on the protections on searching, and dissemination, and analysis of information in the government's hands, there's nothing to prevent the government from recording every phone call, copying every email, creating a permanent record of everybody's movements, associations, and communications. And the only question we'll be asking is when can the government access it.

But the creation of that kind of

massive database will have huge implications for the way that ordinary people operate in society, both the way that they interact with one another and the way that they interact with their government.

People who believe that the government is surveilling every movement and every communication, believe justifiably that it's doing it, will act differently. They won't go to controversial websites and they won't engage in controversial communications that are necessary for any democracy.

MS. WALD: I'll save, I know my time is up. I'll wait for the next round. I have another question.

MR. MEDINE: I want to go back to that back-end searching, basically the U.S. person searches, and this really is two questions.

One is the government panel asserts that this is lawfully obtained information and therefore should be permissibly used without any further Fourth Amendment implications. And why

that's not a persuasive argument.

And then two, if it's not persuasive, what is the procedure that you envision? And again, I think it's different from Professor Donohue where you're using that U.S. person information to get more information. You're just saying let's use the information we've already collected under some other, under authority for, say, criminal purposes or foreign intelligence purposes.

So I guess it's two parts. Why isn't is already legally usable? And if it's not, what procedure would you apply to access it? And that's to any panelists.

MS. DONOHUE: So as a statutory matter I would come back to the burden of proof with regard to whether that information that's being collected on targets, they are indeed U.S. persons or non-U.S. persons and located outside the United States.

So here the statute is silent, and I share Mr. Dempsey's textual analysis of the about

question. I think the statute is silent there as well. But in regard that the statute does say where you know that somebody is a U.S. person, you know, you have Sections 703 and 704 that you have to operate under.

MR. MEDINE: Again, we're not targeting the U.S. person, we're targeting a non-U.S. person, and Congress clearly knew that at the other end of that phone call could be a U.S. person and still authorized that kind of collection without a warrant.

And the question is, why isn't that sufficient to then say, okay, this information was lawfully collected, now we can do searches based on it?

MS. DONOHUE: Because it isn't certain that the person on whom you're collecting the information really is a non-U.S. person. So the burden of proof on the NSA is to say, to establish that this individual is a non-U.S. person.

But in fact, so the assumption that all

the collection that's going on currently is of non-U.S. persons I think is an erroneous one. And it's one -- and the reason why I think it's erroneous is because the NSA is under no obligation to check and see and make sure that that individual is not a U.S. person.

To the contrary, they have in their documents they say, well, they may check these databases, they may check these other databases. There's no obligation that they do so.

Mr. De in the previous panel referred to the totality of the circumstances type tests that say they have two strikes against, four strikes for, they look at everything. There is nothing that obliges them to then go back and dig up more information to find out in that particular circumstance.

And not only that, but actually if you look at the requirements for what is required to positively identify, to conclusively determine it in the minimization procedures, the bar is actually significantly high.

It means that you know their name, you know their title, your know their address, you know their personally identifiable information in the context of activities conducted by that person that are related to that particular person. A reference to a brand name, manufacturer's name, Monroe Doctrine, etcetera, that's not sufficient.

So not only are they under no obligation to establish that but in order to establish it, it's a very high bar. So it's not clear to me that that information is lawfully collected in the first place.

MR. MEDINE: Ms. Levinson-Waldman, do you want to weigh in on that?

MS. LEVINSON-WALDMAN: I think the other thing I was going to add, if I'm understanding the question correctly about why is it not okay to do searches on information that's been lawfully collected, I think there's also an element of bootstrapping.

So that it was lawfully collected for a purpose, for a foreign intelligence purpose, and

that you're right, of course Congress knew that U.S. person information was going to be incidentally collected through that process, but then there are these minimization procedures.

And so kind of almost bypassing those procedures and allowing that body of information to be collected without meeting a fairly high bar, some kind of probable cause warrant seems like kind of going back and bootstrapping your way into that information in a way that is very different from searches of, I think, any other, almost any other body of lawfully collected information, because the standard for which it's obtained, that foreign intelligence standard and purpose is so different.

MR. JAFFER: I mean I actually think there are two kinds of bootstrapping. The first is pointing to the fact that foreigners outside the United States lack Fourth Amendment rights in order to collect huge volumes of communications to which Americans are a party.

And then the other is pointing to the

foreign intelligence purpose to gather information which is then later used in criminal prosecutions. So that's to state the problem. It's not a solution to the problem, but I think that's where the concern comes from.

MR. MEDINE: Professor Ku.

MR. KU: If I could just add, I mean I'm not sure that's bootstrapping. I think that's sort of the purpose, right. The purpose is -- it's not that they're not also collecting it for foreign intelligence purposes.

It's also true that if in the old days they came across a letter from an American person to a foreign person, it seems unlikely to me that because an American sent the letter that means they can't -- but they lawfully obtained the letter, it's unclear to me why they couldn't use that letter.

And so I'm a little, possibly it's bootstrapping, but it's, there's a long history of going after foreigners and doing foreign surveillance.

I'm not sure that -- I think the only difference I think is technology does make it easier for it to flip back into the states, but I'm not sure that fundamentally this is a really different thing.

MR. MEDINE: Thank you. Ms. Brand.

MS. BRAND: Thank you. Well, it seems like there are some fundamentally opposing world views about the Fourth Amendment on the panel, and I want to, I mean this Board is not going to move Fourth Amendment law. So I want to get to what you think the law is and what you think the law should be, because I think there might be some conflation of those two things going on here.

First of all, Professor Ku, thank you for submitting your comments this morning, your written comments. I haven't had a chance to read them yet so I just want to ask you a question to make sure I understand where you're coming from.

You talk about inherent executive authority to conduct surveillance abroad or even of non-U.S. persons abroad. In your view, does

that inherent executive power operate alongside the Fourth Amendment, or irrespective of the Fourth Amendment, or does that create an exception to the Fourth Amendment?

MR. KU: Right, no, I don't think it creates an exception to the Fourth Amendment. It operates within the constraints, whatever they might be, of the Fourth Amendment.

But I would like to point out that historically this -- I mean so just to clarify. The reason I raise this, it goes to the point that historically the U.S. government as operated without statutory authority to conduct foreign surveillance. It's been, the power was granted, was thought of as coming from the Constitution.

So the statutory scheme has not been thought of as necessary to authorize the type of intelligence gathering that's going on.

Now the Fourth Amendment does apply, but as I also emphasized, it hasn't always applied. It didn't originally was thought of to apply at all, even to U.S. citizens overseas, but

I think we understand that the courts have come around to view that it does apply to U.S. citizens overseas. But I think it still has a limited impact compared to the way it applies for purely domestic searches. So that's how I would analyze that.

MS. BRAND: And how does it apply to purely domestic searches where there's a purpose of foreign intelligence gathering?

MR. KU: Well, I think that -- well, here I think that, you know, it does. The Fourth Amendment has been interpreted in recent cases to be a much more robust protection for searches domestically, although even in some of those cases, right, a warrant has not been required or the exception to the warrant requirement has been found for foreign intelligence purposes. So it still continues to exist within the domestic sphere.

I would say that for me, at least my understanding is a lot of this has been supplanted by the FISA system. The rise of the FISA system

has to some degree made the Fourth Amendment analysis a little bit less onerous because what's been happening is that everything's been funneled through the FISA system and the challenges to the FISA system has not been sort of as robust.

I think if we hadn't had FISA maybe we'd have had more cases that would have clarified exactly what the Fourth Amendment limits on domestic foreign intelligence searches would be. I do think that it applies more strongly to domestic searches and I think it has more significance.

But I do think that ultimately the foreign intelligence exception to the warrant requirement is a reasonable one that does need to be respected. It has a long tradition in history.

In my view, really FISA is sort of on top of that to add additional privacy protections that I think Congress has judged, and probably rightly so, we need. But I'm not sure the Fourth Amendment itself standing alone would necessarily require all of the sort of procedural limitations

and minimization protections that we have.

MS. BRAND: Okay. And Jameel, can you very briefly, because I have another question for you, you do not think there is any foreign intelligence exception to the Fourth Amendment? Is that what I heard you say earlier?

MR. JAFFER: I don't think that there's any foreign intelligence exception broad enough to justify 702, and no court has --

MS. BRAND: But there is -- I mean I guess what I'm trying to get at is, do you think that the Fourth Amendment applies equally to collection for the purpose of foreign intelligence gathering as it applies to collection when the purpose is to gather evidence of a bank robbery, for example?

MR. JAFFER: I think that there are certainly narrow circumstances in which the courts have held that there is a foreign intelligence exception.

Again, those cases predate FISA, and so you know, you have to evaluate whether those cases

survived the thirty-five years of experience under FISA.

MS. BRAND: Okay. And then you referred earlier to, I think you were referring to, well, you're referring to 702 generally as large scale collection. I'm not sure if you were including both upstream or PRISM in that assessment.

But if you were here for the first panel and if you take the government's facts as they stated them to be true, what about that program strikes you as large scale? What's your justification for that description?

MR. JAFFER: Well, so two responses to that. The first is I think it's important to draw a distinction between statutory restrictions and executive restraint. So there's a question of what the statute allows and then there's a question of how the government is implementing it.

Obviously I know much less about how the government is implementing it than I do about what the statute on its face allows because I can

read the statute and I have access to only a portion of the government's documents.

But then as to, you know, whether it's large scale collection or not, I think that the problem is that everybody is using these words in different ways. The panelists this morning said that they weren't drawing a distinction between acquisition, surveillance, and collection. But their own documents do draw a distinction.

If you look at USD 18, for example, which is the Defense Department's implementation of the executive order on intelligence collection, it draws a distinction between electronic surveillance and acquisition on the one hand and collection on the other.

And collection involves the tasking of that, or tasking of communications, whereas electronic surveillance and acquisition do not.

And so, you know, we have always thought of this, putting the vocabulary to the side for a second, we've always thought of this in two stages. There is a kind of, just to -- there

is a kind of, you might call it scanning, you might call it collection, but there's a kind of large scale acquisition of data, and then there's the government tasking that data, and then there is the government's tasking that data with selectors.

So to be a little more concrete, if the government installs on a switch somewhere installs a device that either diverts all of the communications or a large portion of the communications, or scans a large portion of the communications, we would call that bulk collection.

I'm not sure that anything turns on vocabulary but we should all make sure we're talking about the same concepts.

MR. MEDINE: Ms. Cook.

MS. COLLINS COOK: Actually that was right at the top of the last piece. I think we've used, and in this conversation alone we've used scan, inspect, acquire, collect, access.

And so I guess my question is, if you

have access, so in your hypothetical you've installed something that gives you access to this stream of communications, is that a seizure or a search for the purpose of Fourth Amendment analysis in your view?

MR. JAFFER: Well, I think it would depend what you were accessing. You know, the question would be have you invaded a reasonable expectation of privacy?

But we have taken the position that, for example, the bulk accessing of telephone metadata is an invasion of a reasonable expectation of privacy, and we would certainly take the same position with respect to the bulk acquisition of telephone calls or emails.

The MYSTIC program, again, just discussing it as a kind of hypothetical, that program in my view involves the bulk collection of telephone calls, voicemail messages, and telephone calls, even if the government doesn't access more than a small proportion of them.

MS. DONOHUE: May I add something to

that just very quickly? I was a little bit confused in the earlier panel because on the one hand they were saying this is a very limited program. On the other hand they say that this SIGAD is the most used NSA SIGAD.

The slides that have been released say it draws from Microsoft, Google, Yahoo, Facebook, Paltalk, YouTube, Skype, AOL and Apple, that it gets voice over Internet protocol, email, chats, all this information, and it's hard to square that.

And what they say is the value of the program, with its limited nature --

MS. COLLINS COOK: I'm sorry, can we talk about -- I appreciate your desire to talk about the previous panel but I had a specific question out that I'm really trying to understand the panelists' view on when the Fourth Amendment is implicated and how.

And so if it's under your hypothetical if you have the acquisition of all phone calls from a country with subsequent access, at what

point would the Fourth Amendment attach?

MR. JAFFER: I would say certainly the moment you put it in your databases, by that moment the Fourth Amendment has attached.

MS. COLLINS COOK: So flipping that, if it's access to a wide swath of communications but acquisition into the government's possession or control, when would the Fourth Amendment attach?

MR. JAFFER: I'm sorry, but I've lost track of the difference between access and acquisition.

MS. COLLINS COOK: And this is part of the, I think you've used scanned, but some ability to review a stream of communications and pull, filter, something to that effect.

MR. JAFFER: Right. The scanning or the filtering would implicate the Fourth Amendment in my view.

MS. COLLINS COOK: That's helpful. I wanted to follow up on a different set of questions and just close the loop.

If the determination was made that the

acquisition of the information pursuant to 702 was lawful, it's lawfully acquired information, would you still take the position that a subsequent search, and by that I mean a query using a U.S. person identifier, would need some sort of probable cause determination, that there would be a separate Fourth Amendment analysis?

And can you explain why? I guess is this because there's a view that there's a lack of particularity of the front-end and therefore you have to have subsequent some particularized finding?

MR. JAFFER: Yes.

MS. DONOHUE: That would be my position as well.

MS. COLLINS COOK: Okay. One question for Professor Ku, if I could. We've heard that 702 is silent, I think it's fair to say on the precise question of abouts. There are some structural arguments here and some purpose arguments that you can look to, but it's silent.

In view of the evolution of our

understanding of Article II of FISA, how would you as a constitutional matter assess a silence in 702? Because Title VII is both an authorization and a restriction on Article II authority, so.

MR. KU: Right. So I think, I don't know if I have any sort of grand insights on the purely textual analysis, although I do think that the constitutional background is what can help us here with respect to, if we understand where we're coming from can help us analyze this.

If we understand that constitutionally that the U.S. government was engaged in broad searches prior to the enactment of 702 then you have to sort of think about, well, to what degree.

This is not really about authorizing, this is really about restricting, imposing restrictions on what I think the U.S. government had the authority to do prior to the enactment of the statute.

And so if you look at it from that perspective then, if it doesn't, the silence or the lack of clarity or specificity would then I

think lead me from that perspective to suggest that the President retains that power.

I would analogize this a little bit to the point that was made in the earlier FISA statute, how they excluded radio completely from the original FISA, radio communications, they just said nothing about it.

And there are a lot of people that argue that was on the assumption that most of the foreign intelligence was radio in 1973 and that the President would continue going on gathering as much radio signals intelligence as he could. And then at a certain time, no one used radio anymore.

But the point is that if you add the restriction in the statute it doesn't -- the previous or the other authority the President has to conduct the surveillance should in theory continue, and I think would likely to continue here too, assuming he had the authority prior to the enactment.

MR. MEDINE: Mr. Dempsey.

MR. DEMPSEY: A quick comment and then

a question. Going to the definition of distinctions between collect, acquire, etcetera, my comment is we really have to take yes for yes and no for no and move on. The government has said, to my mind totally clearly, they are not relying upon the USD 18 concepts in implementing 702, so I think that we just have to move on from that. That's my comment.

My question is the following, and this is for Jameel or anybody, Rachel, in terms of the querying of data otherwise lawfully acquired, what is the best case law that would limit the proposition that data lawfully acquired can be subsequently queried without limitation?

MR. JAFFER: Well, so on your comment, I think you're certainly right that the government said on the panel earlier today that they were not relying on the distinction, any distinction between acquisition and collection.

But I think that the government also acknowledged that it was engaged in about surveillance, and to engage in about surveillance,

my understanding is that there is no way to engage in about surveillance without inspecting in some sense every communication within the universe of those that you are monitoring or surveilling. There's no way to do it.

Now you can call that bulk collection or you can call it something else, but that scanning of every communication in a particular universe raises constitutional issues, and if all you're saying, Mr. Dempsey, is we should just address those constitutional issues, then I entirely agree.

MR. DEMPSEY: So now as the querying of otherwise lawfully acquired communications, and let's take, you know, if I steal your computer, I think, and then I give it to the government, the government lawfully acquired it. I may have stolen it. Or certainly in the Title III context the government lawfully acquires, or in the normal search and seizure context, or in the voluntary disclosure context, where is there case law limiting the proposition that lawfully acquired

information cannot subsequently be queried essentially without prior authorization, without meeting any threshold? What is, is there any case law limiting that?

MS. DONOHUE: So we're starting to see cases come out of border security issues where computers -- border security issues, and I'd be happy to send you the names of the cases afterwards, where computers have been lawfully seized under customs laws but then they cannot be searched for all of the information on them because of the privacy implications that are involved and lack of a sufficient nexus to the suspected criminal activity.

So those cases might be one source that you would look to in a new age of data where so much information is available.

MR. JAFFER: You know, I think it's important to ask the question the other way around as well, which is, you know, where is there case law showing that the Constitution is indifferent to the government collecting huge

volumes of communications without any individualized suspicion or particularity, and then sort of bootstrapping its way into free rein or --

MR. DEMPSEY: Again, if we're in a situation, I'm just trying to pose the situation of let us assume, just let us assume that the collection was lawful.

MR. JAFFER: I'm not suggesting for these purposes that the collection was unlawful. What I'm saying is that the collection here is different in kind from the kind of collection that the courts have been concerned with in other cases involving the use of information lawfully acquired. You know, it was important to those cases not just --

MR. DEMPSEY: So then the license plate readers, the information collected by the license plate readers is lawfully acquired and then the government can subsequently query that license plate database. I mean that's standard procedure.

MR. JAFFER: I'm not sure that it's

established with any certainty that the bulk collection, that the querying of a database of bulk collected license plate reader information doesn't raise Fourth Amendment concerns, and I think that that's still an open question.

MR. DEMPSEY: Well, I'm looking for some cases. Professor Donohue has some border cases --

MS. DONOHUE: I'd be happy to send you the border doctrine cases.

MR. DEMPSEY: That may be relevant. I would welcome any other cases limiting that proposition.

MR. MEDINE: Judge Wald.

MS. WALD: This is probably an unfair question but I'll ask it anyway. Given the fact that the grievances about 702 as it operates today have included a whole series of things, one we didn't discuss here but it's been raised in written stuff is the lack of FISA review of particularized targeting designations. I know it's allowed by the statute, but nonetheless the

capture and use of incidental U.S. information to search database, the use and retention of the U.S. information.

But my question is, if you had to focus on one or maybe two important changes that you would like to see made now in 702, what would they be? Very quickly, anybody that wants to answer it.

MS. DONOHUE: I would say limiting the information to, or from, or held by the actual target and inserting a mechanism of judicial review if information is uncovered that would lead to subsequent criminal prosecution prior to analysis of the databases that are held.

MS. WALD: Okay, great. Down the line.

MR. JAFFER: The only thing that I would add to that is destruction of inadvertently acquired communications. Communications that the government itself acknowledges should not have been acquired in the first place should be destroyed immediately.

MS. WALD: Destruction, they say

they're purging them but you mean something --

MR. JAFFER: There are broad exceptions to the --

MS. WALD: I know there are exceptions, but you mean -- okay.

Do you have any, Professor Ku?

MR. KU: Actually, I mean this may be kind of not what you're looking for, but I do think that actually I would prefer the FISA section clarify the default that I've been arguing for, that it doesn't encroach, to clarify further that it doesn't encroach on, Section 702 doesn't encroach on the President's, you know, foreign intelligence authority. That would, I think, help our interpretation of the statute.

MS. LEVINSON-WALDMAN: And I just would mention three things. One is I agree more robust involvement by the FISC.

MS. WALD: I'm sorry, more?

MS. LEVINSON-WALD: More robust involvement by the FISC in terms of review. There's some review now that is sort of a

box-checking procedure, and have that review be more --

MS. WALD: Just the way they do what they do now, but more carefully?

MS. LEVINSON-WALDMAN: Well, I'd say not even, it's not so much that I think that they're not careful with it now, it's that the statute actually limits the scope of some of the review that they do, that they sort of don't get behind the curtain.

MS. WALD: Including the targeting.

MS. LEVINSON-WALDMAN: Right. I guess the second, thinking about, so if you think about Section 702 but having the minimization procedures be a natural part of that statute.

Certainly limiting and potentially eliminating the use of information for law enforcement purposes. And obviously this is something that the NSA, that the President's review group spoke to as well and made that recommendation.

And then the third quite honestly would

be to lift the standard back up to agent of a foreign power from the foreign intelligence requirement. And the foreign intelligence purpose is so loose and that that seems to be --

MS. WALD: For targeting?

MS. LEVINSON-WALDMAN: For targeting, yes, that's correct.

MS. WALD: Okay. I've got maybe one minute left so a quick question. Some of you, I don't remember now, all of you in a prior one, when we were doing 215, talked about the desirability/necessity of having an adversarial element in the FISA proceedings.

A very quick notion of how would you see an adversary, however appointed, in a 702 proceeding? In other words, what function could they serve, he or she serve in a 702?

215 was a little bit more evident. A novel technological case coming up to the court, what would you say, do they have any, would they have any function in a 702?

MS. DONOHUE: So I would imagine them

having a function absolutely, yes. The ACLU tried to do this and was not allowed to intervene on a motion on a First Amendment grounds and it was denied by the court in part on the grounds that they would never succeed on the First Amendment to actually intervene.

I think having an advocate there would allow them to more carefully review minimization procedures, to more carefully review targeting procedures. It would allow them to evaluate the role that they play with regard to targeting.

MS. WALD: In individual cases in 702?

MS. DONOHUE: And in individual cases, yes, but you would have to change to insert some sort of a warrant requirement equivalent for criminal prosecution or further examination of the records.

MR. JAFFER: And I think that our biggest concern is with judicial rulings that have far-reaching implications and not just implications in the individual cases. So I think that when you're talking about the individual

cases, I do think that, you know, in theory an adversarial process would be a useful thing.

On the other hand, I think that the closer you get to an individualized warrant application, or court order application, or surveillance application, the more it looks like traditional Title III or a search warrant context, which is ex parte.

But you know, when you get to judicial opinions that authorize about surveillance at some level of generality, that is something that ought to be argued in open court, you know, with a closed hearing to follow if there is legitimate, if there are legitimate sources and methods to be protected.

But if I can just use the process to add one answer to your previous question, I agree very strongly with what Rachel said that reforming or revising the standard, the targeting standard is crucial.

Right now there is, there's really no limit on who the government can target overseas.

The example that the government panelist kept coming back to is bad guy at Google.com or bad guy at Yahoo.com. But it could as easily be journalist at Yahoo.com, or human rights activist at Yahoo.com. And I think it's crucial that some limits be drawn around the category of people whom the government can legitimately target.

MS. WALD: And by the FISA court?

MR. MEDINE: We only have a couple of minutes. If there's any members of the Board who want to ask any additional questions.

MS. COLLINS COOK: Can I ask just one quick follow-up question on this point actually?

MR. MEDINE: Sure.

MS. COLLINS COOK: And this is to Ms. Levinson-Waldman. You had said lift the standard back to agent of a foreign power or a foreign power. What were you referring to when you said back to?

MS. LEVINSON-WALDMAN: Right, I mean I guess back to, we're sort of envisioning to some extent Section 702 is sui generis and when it came

into being it was a foreign intelligence requirement. But I guess thinking of FISA more broadly, narrowing that foreign intelligence standard in some way to match what is in other sections.

Obviously one option would be matching what's in other sections of FISA, agent of a foreign power, I think that would be our preference, but narrowing that in some way. Back was probably an imprecise way of referring to it.

And if I could add one other brief thing, I think our other, you know, if we have a wish list it would be, and again, I'll say restore, but thinking about other parts of FISA, having the collection be, and you know, these may be one or the other but having the collection, the foreign intelligence be the primary purpose rather than a significant purpose, that that has also allowed, you know, potentially a fair amount of slippage in terms of what the collection is for.

MR. MEDINE: Any other final questions? I want to thank the panelists very much for

joining us today. It was a very enlightening discussion. We're now going to take a lunch break and we will resume with our third panel at 1:45. Thank you.

(Off the record)

MR. MEDINE: Good afternoon, and thanks everyone for rejoining us. And I want to introduce our third panel, which will be on transnational and policy issues.

We are joined by John Bellinger, who is a partner at Arnold & Porter, Dean Garfield, who is the President and CEO of the Information Technology Industry Council, Laura Pitter, who is a Senior National Security Researcher at the Human Rights Watch, Ulrich Sieber, who is the Director at the Max Planck Institute for Foreign and International Criminal Law in Freiburg, Germany, and Chris Wolf, who is a partner at Hogan Lovells.

Each of the panelists will make a brief opening statement and then we will proceed with the Board questioning.

I guess we can start alphabetically

with Mr. Bellinger.

MR. BELLINGER: It's me first then. Well, thank you all very much for having me in, the members of the Board. I'm going to focus my comments on whether international law places any restrictions on electronic surveillance of foreign nationals outside the United States.

I think you know I served as the legal advisor for the Department of State from 2005 to 2009, as the legal advisor for the National Security Council from 2001 to 2005, and then I was the national security advisor to the head of the Criminal Division at Justice Department before that, so I have extensive experience, both in intelligence activities and international law.

So in recent months I think you know many scholars and human rights advocates have argued that NSA surveillance of foreign nationals violates a so-called universal right to privacy recognized in international law.

They base their argument on Article 17 of a human rights treaty called the International

Covenant on Civil and Political Rights, which the U.S. ratified in 1992.

Article 17 provides, and I quote, no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, end quote.

The argument that NSA surveillance violates Article 17 of the ICCPR is incorrect for several reasons. And I will say in my view international law, neither the ICCPR or any other part of international law placed international legal restrictions on the NSA, any of the NSA programs.

With respect to the ICCPR, first, for the last sixty-four years the United States government has taken the consistent position that it does not apply outside the borders of the United States. The U.S. took this position when we negotiated the treaty in 1950, and we re-articulated it in 1995, when the Clinton administration submitted its first report to the U.N. Human Rights Committee, which is the group

that oversees compliance with the ICCPR.

My predecessor at the time, the then legal advisor Conrad Harper, explained to the committee that the ICCPR imposes obligations on the United States only inside the United States. And that's because Article 2 of the ICCPR, which defines its scope, says that a state party is bound to respect and ensure the rights in the ICCPR only to all individuals within its territory and subject to its jurisdiction.

And as my predecessor, Conrad Harper said at the time, this is a dual requirement that establishes that treaty obligations apply only if both conditions are satisfied. An individual must be under United States jurisdiction and within United States territory.

And now the negotiating position of the United States of the treaty confirms that interpretation. The phrase, within its territory, was added at the request of the head of the U.S. delegation, Eleanor Roosevelt at the time in 1950. And she explained that, quote, the purpose of the

proposed addition is to make it clear that the draft covenant would apply only to persons within the territory and subject to the jurisdiction of the contracting states.

There was a vote held on that addition and that addition was adopted 8 to 2 in 1950. Subsequent efforts to change that have failed.

And again, in his statement to the Human Rights Committee in 1995, Conrad Harper explained that the words were added, quote, with the clear understanding that such wording would limit the obligations to within a party's territory.

Now it's true, and I know that Laura Pitter is going to talk about this, that the Human Rights Committee and a lot of human rights groups in other countries don't agree with the long-standing U.S. interpretation, but the Human Rights Committee's statements don't have binding legal effect on the United States or to any other country. We give respect to them but they're not binding on us.

Both the Bush and the Obama administrations have confirmed the Clinton administration's position that the ICCPR does not apply extra-territorially.

In fact, just five days ago in Geneva we were making our periodic report to the Human Rights Committee and the acting legal advisor, Mary McLeod, told the committee, quote, the United States continues to believe that its interpretation that covenant applies only to individuals both within its territory and within its jurisdiction is the most consistent with the covenant's language and negotiating history.

So we really have fifty years of U.S. practice on this point recently reaffirmed by the Obama administration.

But even if the ICCPR did apply extra-territorially, the treaty would still not place limits on NSA surveillance because persons in other countries are not subject to U.S. jurisdiction.

The Human Rights Committee itself has

defined the phrase subject to a party's jurisdiction to include people within the power or effective control, or effective control of the forces of a state party acting outside its territory. So not even the Human Rights Committee is suggesting that everybody who may be subject to NSA surveillance is actually within the power or effective control of the United States.

And I would want to hear more from my colleague who I've met before, Professor Sieber, but even if they're unhappy with NSA surveillance, I am not aware of any foreign government that believes that the ICCPR or any other provision of international law imposes an obligation to respect the privacy rights of non-citizens.

In fact, candidly, most foreign governments spend lots of time spying on foreign citizens. So they may be unhappy with what we're doing as a policy matter, human rights groups may suggest that there are binding legal norms, but I'm actually not aware that foreign governments are suggesting that there is an actual violation

of international law.

And finally, just to close on my analysis of the ICCPR, and then I'll wind up, even if the ICCPR did impose certain obligations on United States extraterritorial conduct, even if people outside the United States were considered to be within the jurisdiction of the United States, Article 17 of the ICCPR still only bans, quote, arbitrary and unlawful interference with privacy.

Now we can certainly argue about constitutes arbitrary and unlawful interference but there is no international norm on that point. I'm sure lots of people can suggest that the NSA program is arbitrary, that it's unlawful, but when we're talking about international law there has to be actually a specific norm that people have agreed to, and there is no generally accepted framework under international law that defines what kind of surveillance is unlawful or arbitrary.

So the bottom line, despite statements

that we are violating the Article 17 of the ICCPR, it just simply does not apply, nor does any other provision of international law.

And so let me close by saying that just because international law doesn't actually create a universal right of privacy that's binding on the United States, I'm by no means saying that we ought to be insensitive to the rights of non-citizens. Certainly if I were still in the White House I would be saying, you know, we need to be respectful of concerns both of individuals or of leaders. That's why we make these policy decisions.

President Obama's recent presidential policy directive states that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.

So it's perfectly appropriate to take

into account privacy interests, but international law does not place binding legal obligations on us. Thank you.

MR. MEDINE: Thank you. Mr. Garfield.

MR. GARFIELD: Thank you. Thank you members of PCLOB on behalf of fifty-six of the most dynamic and innovative companies in the world, thank you for inviting us to testify today. And thank you as well for your efforts to advance both national security and civil liberties.

From our perspective we have the firm view that those two concepts are mutually reinforcing and in fact are not mutually exclusive and so we want to do whatever we can to support your efforts.

I'd like to focus my testimony on two areas. One, what we're experiencing in the marketplace as a result of the NSA disclosures and, then share some solutions that may help remediate some of the challenges that we're facing.

On the first, the economic impact from

the NSA disclosures are significant and ongoing. The folks in this room are very familiar with Section 215 and the distinction between that and Section 702, but for folks outside of this room much of what they experience and what we're experiencing is diminishing trust, particularly diminishing trust in U.S.-based technologies. So rather than made in the U.S.A. being a badge of honor, it's increasingly becoming a basis to question the integrity and security of technologies.

That has a real world economic impact. In fact, there are a number of analyses out there that put the numbers of the impact in the tens of billions of dollars.

As significant, perhaps even more significant than the economic loss is the broader societal impact and the implications for the Internet more generally. We're celebrating this year the 25th anniversary of the commercialization of the Internet and are all very familiar with the benefits and the way it's transformed all of our

lives.

Increasingly, what we're seeing though are policies aimed at changing the open, ubiquitous, globally-integrated Internet into one of walled silos. And so the legislation that's actually being debated today in Brazil would create walled gardens around their data.

And it's not simply limited to Brazil. We're seeing the same in Europe, as you all know, where the parliament is questioning the continuing viability of the safe harbor, or in particular territories within Europe where they're calling for country-specific clouds that would again create these islands of walled silos rather than an open, integrated Internet, which we all know the implications of that.

And so what do we do about it? I'll offer up three sets of solutions that build on global principles that we released earlier this year after working with our members to forge consensus on it.

And I place the emphasis on global

because we firmly believe that in order to address these issues and to address them effectively, high level, global communication and engagement around surveillance is critically important.

The first aspect or screed of solutions is around transparency. This body, the PCLOB in its January report made the point that transparency is the foundation for democratic principles. We firmly agree. We also think it's the foundation for separating fact from fable.

And so to the extent that there's a greater awareness, particularly around 702 where there are protections in place already, for there to be greater awareness about that would be quite helpful.

As it relates to our companies, the ability to share with the public more about 702 and 215 and the requests that come in pursuant to those, as well as the accounts, particularly the numbers, would be incredibly helpful. And so greater transparency is one element of what we would recommend.

The second relates to oversight. And as I've said in other places, including my testimony on the hill, our solutions are offered with a great deal of humility because we don't know what we don't know. I don't pretend to be able to offer the exact framework for making sure that there is a civil libertarian advocate or a civil liberties advocate within the FISA or FISC court process. But developing a framework for enabling that, we think is very important.

Finally, the last set of solutions are based on working to rebuild the trust that has been eroded, and there, a few unequivocal statements from our government would be quite helpful.

By way of example, there has been a lot of reporting around steps that may or may not have been taken to undermine encryption standards. NIST has been very firm in taking steps to make sure that they bolster the encryption standards that are being developed.

But a statement from our government

that they don't, do not intend to take steps to undermine the integrity of our cyber -- to undermine the integrity of those standards would be incredibly important.

Similarly, taking steps to affirm that data acquisition pursuant to 702 is not being done in an indiscriminate manner, I think would also be incredibly helpful. With that, I'll pause.

MR. MEDINE: Thank you. Ms. Pitter.

MS. PITTER: First, thank you very much for this opportunity. Thank you for having me. We've filed a more lengthy statement with the Board so I'm just going to be a little bit more brief here.

I was asked to talk about U.S. obligations under the International Covenant for Civil and Political Rights so I'll start with that.

And obviously, I'm going to disagree with Mr. Bellinger on this issue, as did Harold Koh's recently released memo where he disagreed as well and tried to get the Obama administration to

take a different position, arguing that it was not actually in the U.S. interests to continue to not apply the ICCPR in an extraterritorial manner.

There has been debate about whether or not this treaty applies outside of U.S. borders and it stems from, as Mr. Bellinger said, the operative jurisdictional clause in the covenant which says that states have an obligation to respect and ensure that those within its territory and subject to its jurisdiction, the rights under the covenant.

So the word jurisdiction in that clause has been interpreted to mean power and effective control. But the U.S. does not accept that. It takes a strictly territorial stance. And this essentially means that a state has to abide by the covenant within its territory but then it can willfully violate the covenant outside its territory, killing and pillaging at will outside its borders, which doesn't really make any sense.

Treaty law requires that the language of the treaty be interpreted in accordance with

its context, as well as its object and purpose. And the context in this case was post-World War Two when the treaty drafters were aiming at empowering people with rights universally and not diminishing them, and responding effectively to Nazi atrocities.

To interpret the treaty in that limited way would allow, for example, Nazi Germany to run a concentration camp in Poland, as Marco Milanovic, a prominent scholar on this issue has pointed out.

And the U.S. is the clear outlier on this. Only the U.S. and Israel take such a strict interpretation of the treaty.

So how does this apply to surveillance and the right to privacy? Some have argued that even if the ICCPR applies extra-territorially it should only be in the case where the government has physical control over the individual, like in the context of detention or torture. And that doesn't apply to surveillance simply because the individual is not within a state's effective

control.

But the problem is that their communications are. And so to not recognize even a duty to respect the right to privacy in this context creates a kind of absurd situation where the U.S. would be barred from going into someone's house in Germany and taking letters out of someone's drawer but not barred from reaching into their computer and doing the very same thing remotely.

These are novel questions, and I won't deny that. The Human Rights Committee, which is the main interpretive body of the ICCPR, has not adjudicated this matter.

And though there is a body of case law in other jurisdictions, particularly in the European Court of Human Rights, that have the issue and they do provide some guidance on a framework for how to analyze surveillance laws.

That said, those decisions, they came out before the Snowden revelations so they're not informed by a lot of the information that's come

in the public domain about the vastness of the collection that's going on.

But these issues are novel in the U.S. too. Just because there may not be necessarily a case en point does not mean the obligations or the rights don't exist. They are in the treaty.

Just as like many in the U.S. have argued that U.S. law has to catch up with technology and recognize a reasonable expectation of privacy in metadata, international law has to acknowledge that when it comes to surveillance, though an individual may not necessarily be in a state's physical control, their communications are, and the right to privacy can be violated remotely through technical means.

But just because the obligation applies extra-territorially does not mean that the surveillance has to stop. There is a framework within which surveillance can take place, but also be in accordance with human rights obligations. The surveillance has to be lawful and non-arbitrary and necessary to a legitimate cause

that's proportional to that legitimate aim.

By all accounts, that's not what 702 is. 702 may all be for the purpose of protecting U.S. national security, which would be a legitimate aim, but are there more narrowly tailored ways to achieve that aim?

And if the answer to that question is no, and I'm going to quote from the review group here, the question is not whether granting the government authority makes us incrementally safer but whether the additional safety is worth the sacrifice in terms of individual privacy, personal liberty, and public trust. And also, is it really worth the other harms that will result?

We're in a situation now in which countries are rushing to enact laws that would localize data collection and companies are rushing to offer alternatives to customer data being stored in the U.S.

And from a technological standpoint data flows are not necessarily based on geography but travel the cheapest, most efficient route.

This means a transfer to someone in the same country can mean data passing through many countries without the sender even knowing it. So a failure to respect the right to privacy extra-territorially imposes, exposes U.S. data to vulnerability when it's situated in other states.

The President has already essentially recognized all this. His presidential policy directive purports to bring the rules on retention and dissemination of data collection on foreigners closer to those that govern data on U.S. persons.

But it did not end bulk collection and specifically exempted data temporarily acquired to facilitate targeted collection.

Also, this was through an executive order not legislation, so it could be changed by future administrations.

The bottom line is that the U.S. is in a unique position because most of the world's data flows through its borders. And this confers an obligation to respect the privacy rights of those individuals whose communications fall within the

U.S. jurisdiction, but also to refrain from interfering with the ability of other countries to protect data, protect their own citizens' data. And a failure to recognize the value of this undermines U.S. business and long term national security interests.

The administration says it will make some changes but the law remains the same and that too has to change.

MR. MEDINE: Thank you. Mr. Sieber, Professor Sieber.

MR. SIEBER: Thank you very much for your kind invitation. It's a pleasure to be here.

International legal obligations for U.S. surveillance programs for which you are asking can be based on two different sources, interests of states and interests of persons. The two are interrelated since the protection of a state's territory also has effectual protective functions for its citizens.

Let me start therefore with a few remarks on this broader approach before turning to

specific human rights, which have been addressed here.

General international law and Article 2 of the U.N. Charter protects the sovereign equality and territorial integrity of all states.

A state therefore violates territorial sovereignty if it accesses, copies, or manipulates non-public data in computer systems located in a foreign state because such acts initiate in data processing on the servers located in a foreign territory.

There are no norms in public international law that permit violating other states' sovereignty by across the board world-wide surveillance.

There is also no customary rule of international law that permits the infringement of sovereignty resulting from acts of espionage.

In addition, espionage committed from the premises of embassies violates the obligations under Article 3 of the Vienna Convention on Diplomatic Relations.

These infringements of the territorial integrity of many states by large scale surveillance programs have two impacts for our topic. First, with respect to policy considerations, infringements of the territorial integrity of foreign states violate international law, plus in addition also national cyber crime statutes that are globally agreed upon in the Budapest Convention.

These violations pose serious threat to the continuing trust and the integrity of the U.S. and its IT industry. This infringement may be more serious than the violations of privacy rights, the scope of which are controversially in dispute in most countries.

Secondly, transnational surveillance programs on foreign territory take over the security functions of the affected states. This transnational control deprives citizens of protection by their own state and any other legal protective systems in these security measures, since their home state cannot protect them against

unknown foreign violations of their privacy and the intercepting foreign state often does not recognize any aliens' rights outside its territory where the interception is taking place.

In such a global system the citizens, including U.S. citizens, are deprived of any protection, especially if authorities of different countries exchange certain data.

Thus we are all losing a protective system which mankind has won in a long historical battle dating back to the Enlightenment. Thus, if we are engaging in transnational surveillance programs we must at least recognize certain basic human rights apply to all humans, regardless of nationality and place of residence. And if we want to create an effective global solution this must be supported by international human rights, to which I will now turn.

In the field of international human rights I will also concentrate on Article 17 of the International Covenant of Civil and Political Rights. The International Court of Justice, the

U.N. Human Rights Committee, both in its case law and in its General Comment 31, as well as many national courts and governments acknowledge the extraterritorial applicability of the ICCPR.

I also simply refer to the well-founded memorandum presented by Harold Koh, former legal advisor at the U.S. State Department in 2010 and 2013, with respect to the ICCPR. Koh is convincingly for the extraterritorial applicability of the conventions.

According to the prevailing opinion, the ICCPR is extra-territorially applicable to anybody within the power or effective control of the acting state party or its agents.

In the physical world, extraterritorial applicability of the ICCPR is thus limited to situations in which the government has total or special control, spatial control over a territory.

Since communications and privacy rights are by their very nature exercised in the virtual world and are prominently infringed upon there, the control of this virtual world by highly

extensive surveillance programs should be a decisive factor.

If we do not accept these conclusions we still must deal with an argument of the German Constitutional Court, which also might be relevant for the American discussion. The court argues that telecommunication interception not only infringes upon privacy rights by the first act of recording the telecommunication, it also infringes on these rights by the following data transmission to their home country, the analysis, the linking, the long-lasting storing, and by further transmissions to other recipients.

All these acts are repeating and deepening the infringements of privacy rights and they are undoubtedly committed on the territory of the surveilling states. Thus, even in cases of foreign intelligence gathering, we are not dealing only with actions outside the national territory.

Accepting the arguments for the transnational applicability of specific international human rights would promote then a

deeper discussion on the substantive scope of international human rights protection of privacy.

A first attempt to define the contours of the international concept of privacy can be seen in the already mentioned U.N. General Assembly Resolution 68167 of last December on the right to privacy in the digital age.

When this discussion proceeds, it will be most important to recognize that threats from abroad are different from internal threats. Thus the principle of proportionality as developed by international and national courts will lead to very different results in different circumstances, such as for data collection to homeland, in Afghanistan, or today in the Ukraine.

These necessary differentiations under the principle of proportionality can recognize many U.S. security concerns. Thus applying certain transnational privacy rights would not prevent a reasonable security policy, especially also since the ICCPR is self-executing in the U.S.A. and national foreign citizens could not

initiate judicial proceedings against the U.S.

In sum, I would advocate for an international solution and discussion in order to maintain or regain the leading role of the U.S. as an advocate for the rule of law and human rights in democratic societies, as well as for the trust in its IT industry and its clouds.

If time is not yet ripe for an international human rights solution, then more emphasis should be placed on national efforts to provide more guarantees for non-U.S. persons.

For that reason I welcome the respective U.S. Presidential Directive 28 of last January to applying certain safeguards for all individuals, regardless of the nationality of the individuals to whom the information pertains or where that individual resides.

This policy is also the position of the German constitutional law. In case of your interest it would be a pleasure for me to provide you with more details on these comparative legal aspects later on in the discussion. Thank you.

MR. MEDINE: Thank you. Mr. Wolf.

MR. WOLF: Thank you, Mr. Chairman. As Chairman Medine said at the outset, I'm the partner in the law firm of Hogan Lovells, where I lead the firm's global privacy practice.

And in 2013 Hogan Lovells published a white paper examining the similarities and differences among various legal regimes that authorize and limit governmental access to data.

And our work began before the Snowden NSA disclosures in response to the claims of certain EU cloud service providers that storage of data in the EU made it safer from surveillance than storage with a U.S.-based cloud provider.

Obviously following the Snowden revelations the argument in support of allegedly secure from surveillance regional clouds has been renewed loudly.

A previous white paper we did on governmental access to data internationally noted the availability of mutual legal assistance treaties and other forms of cross-border

governmental sharing addressing faulty claims of regional cloud service providers about the invulnerability to foreign government access that local cloud storage might provide.

Our 2013 white paper specifically looked at Section 702 surveillance and the frameworks in Australia, Canada, France, Germany, and the United Kingdom. My written and oral testimony today synthesizes the findings from this white paper and includes additional information on similar laws in Brazil, Italy, and Spain that we intend to publish soon.

I will note that our white paper foreshadowed last week's report of the European Parliament criticizing the practices of certain EU member states for the lack of transparency and controls on their surveillance activities.

My principle point today following our white paper is straightforward. While the policies and practices of the United States addressing surveillance and related privacy concerns obviously need to be and are being

reassessed, the U.S. has on its books greater due process and independent oversight of surveillance activities than many of our fellow democracies.

As you know, Section 702 surveillance requires court approval, surveillance is limited to foreign intelligence information, and oversight mechanisms exist for 702 surveillance.

As our white paper revealed those same limitations are not always found in the law of many of our counterparts. Australia, Canada, France, Germany, Italy, and the United Kingdom do not require court approval for national security surveillance.

In France, the intelligence agency is allowed to conduct surveillance to protect economic and scientific assets, even when national security interests are not at stake.

On the issue of intelligence agencies secretly and without any process at all asking companies for data, we have found that Australia, Canada, France, Germany, and the U.K. allow their governments to ask private entities voluntarily to

disclose data to the government.

In the U.S. the government is not allowed to seek voluntary transfers. A neutral judicial body must approve the government's request for data.

Last week's resolution by the European Parliament recognized extensive surveillance systems in EU member states, and the lack of control and effective oversight that some EU member states have over their intelligence community.

The resolution also questioned the compatibility of some member state's massive economic espionage activities within the EU, with the EU internal market and competition laws. The parliament did not go into the detail of our white paper, but its resolution reflected the baseline findings of our research, that there are substantial deficiencies in transparency about and controls over national security access to data in countries outside the U.S.

Thus when also considering the cross-

border sharing arrangements available to governments for information they collect through surveillance, it is misleading in the extreme to contend that so-called regional clouds provide individuals with security from government surveillance.

I commend this Board for engaging in an assessment of U.S. surveillance practices and looking at how these practices relate to our counterparts. There are no guarantees in the U.S. or elsewhere that agencies will abide by the laws restricting national security surveillance, but the degree of authorization required and the kind of review that occurs is obviously relevant to a determination of how well personal privacy and personal liberty are protected.

Thank you again for the opportunity to present the findings of our white paper and I'll look forward to your questions.

MR. MEDINE: Thank you very much.

I want to turn to the ICCPR for a moment, and as I understand it there are really

two issues here. One is the jurisdictional test, and if you pass that then the substantive test with regard to evaluating whether the 702 program affords appropriate protections or is arbitrary in some fashion.

I want to start with the jurisdictional issues, and that is, I guess there are three interpretations of the applicability of the treaty. One is that there has to be both territorial presence and jurisdiction. The other is there could be one or the other. And I guess the co-approach, which is they sort of split it, and that is there is a respect requirement across the board and an ensure requirement only subject to the territorial and jurisdictional issues.

I want to ask about the jurisdictional side. As we know from discussion earlier today and what's been made public is the information that's being collected under the 702 program is being collected in the United States, albeit about non-U.S. persons.

I guess my question is for the

panelists, how should we, how should one interpret jurisdiction? It's not going to be up to us to interpret it, but in terms of understanding jurisdiction, is it jurisdiction over the information, which may be here, is it jurisdiction over the person, who may be elsewhere? And how would that apply, both in sort of friendly and unfriendly countries, in terms of the scope of our responsibilities?

MR. BELLINGER: I'll take a stab at that. Let me say a couple of things. One, just to reiterate that the U.S. has in fact reaffirmed its position again that the ICCPR does not apply extra-territorially and the point that the individuals have to be under the power and control.

You know, I get sort of the novel suggestion that anybody who is subject to electronic surveillance is therefore under U.S. power and control. But I don't think that's actually a credible argument.

Even the Human Rights Committee I think

would not go so far as to say that if one can touch a foreign national through surveillance that that is someone who is under U.S. power and control.

The fact that the surveillance may be then collected ultimately inside the United States I think does not change the fact that the collection is being done of persons who are outside the United States. And so I think that does not change the, either the essential jurisdictional element that it does not apply extra-territorially outside the United States, and that those individuals are within the power and control of the United States.

Again, these are things that one might wish were so, and I'm not sure that there's as much of a disagreement between me and Laura Pitter as she suggests.

If one were writing a new treaty and could get people to agree to certain things one might agree that there might be, you know, policy limitations that one might accept.

But the way this particular treaty is written now, certainly the view of the United States government, and I frankly think I am not aware of any single government in the world, and I mean this is what I mean, governments who believe that their right to conduct electronic surveillance of people outside their territory is controlled by the ICCPR. I would be very surprised if we found any European government, as upset as they might be with electronic surveillance by the United States, who would say the Article 17 of the ICCPR limits our ability to collect outside our borders.

And in fact, the German government in a submission made to the European Court of Human Rights interpreting the European Convention on Human Rights argued that that convention did not limit its electronic surveillance of Uruguayans outside of Germany.

So again, the view of governments is that this does not have jurisdictional control over people who are outside their territory.

MR. MEDINE: I just wanted to follow up. What is the scenario where someone would be in our territory and not within our jurisdiction? Because the statute, the treaty says both territory and jurisdiction. Are there other situations where one would apply but not the other?

MR. BELLINGER: Well, certainly there would be people who would be, theoretically there could be people who are not in our territory and who could be subject to our jurisdiction. That was the problem that Eleanor Roosevelt was trying to solve at the time, to think about what the converse might create.

MR. MEDINE: Okay, thanks. Ms. Pitter.

MS. PITTER: Well, first of all, the German position was taken in 2008 before these revelations came forward and they've since sponsored a U.N. resolution which underscores the importance of respecting the right to privacy.

So I would say that, you know, Koh's interpretation is that there's on the one hand a

duty to ensure the rights in the covenant to those within a state's territory and jurisdiction, and then there's also a duty to respect the rights of individuals outside of the territory, the actual territory of the United States.

So there's the duty to respect is what's important here, and so there is an obligation under the ICCPR, even with the jurisdictional clause, to respect the rights to privacy of those outside the United States.

But this all, as you said, is happening in the United States. I mean the data is flowing through U.S. borders, although I'm not sure about the backbone upstream collection, where exactly that's taking place. So absolutely, yeah, absolutely, I mean I think that it would be the duty to respect the right to privacy is what's implicated here.

MR. MEDINE: Thank you. Judge Wald.

MS. WALD: I've got two questions I think for Mr. Bellinger. First is I think we recognize that the government has now reaffirmed

its earlier position about what the ICCPR means in relation to people abroad. But I wondered if you'd just say a word about how they dealt with the question of Article 31 of the Vienna Convention on the interpretation of treaties insofar as, as I remember it, you know, deference should be given to the official interpreters of the -- which in this case I believe, you know, have taken a much broader interpretation of that.

And I think a couple of our Supreme Court justices have said in several cases that when you're interpreting, when they're interpreting a treaty one should look to the interpretations, maybe for guidance, maybe not controlling, of other parties to the same treaty. Just a word or two on those two aspects of the reasoning which led to what is, is the reaffirmance of it.

MR. BELLINGER: Right, and I think what you're talking about is the General Comment 31 of the Human Rights Committee.

MS. WALD: Yeah, yeah.

MR. BELLINGER: Which certainly in the view of the United States, and again, I'm not aware of any government in the world who believes that the views of the Human Rights Committee actually are legally binding.

The Human Rights Committee was set up to monitor compliance and it makes statements which governments, including the United States, give respect to but we certainly don't, neither we nor other countries believe that that is the definitive interpretation of the treaty, nor do we believe that it's legally binding.

MS. WALD: Okay. My second question --

MS. PITTER: I was just going to add, sorry.

MS. WALD: Go ahead.

MS. PITTER: That it is, the Human Rights Committee is a very authoritative source regarding the interpretation of the covenant. And I mean the U.S. is under an obligation to give effect to the rights in the treaty in good faith. So what the Human Rights Committee has said in

that regard is very important.

MR. BELLINGER: And if I could just say, because these are important points right now, including for treaties, frankly the Human Rights Watch is extremely interested and having gotten through the senate the U.N. Convention on Disabilities.

So you know, Human Rights Watch can speak for itself, but certainly the view of the U.S. government and of most human rights organizations is that the statements made by these treaty compliance groups, while due great respect, are not binding on the United States.

If they were in fact considered to be binding on the United States, those would in fact fundamentally change U.S. obligations under the treaties and we would never get any treaties through the senate, including the treaty that both Laura and I would very much like to get through the senate, the U.N. Disabilities Convention.

MS. WALD: Okay. My second question very quickly is that acknowledging what

everybody's about, that this big debate in the international world will continue probably despite the most recent position we've taken, and given, you know, all of the people allied with it, the official interpreters, whatever they're called, Harold Koh, Sara Cleveland, Manfred Nowak, who's the U.N.'s leading expert on the ICCPR, my question to you deals with the last paragraph of your both oral and written testimony, and that is that you would see no problem with a policy which gave greater consideration to the rights of non-U.S. persons within the surveillance context, alluding to the fact that the President in his directive suggested that.

But I'm wondering if you, having served the position you did as counselor in the State Department, have any more specific ideas about in this context 701, or maybe even in other surveillance programs we could do just that?

MR. BELLINGER: Thank you, Judge. It is a great question. I have not actually given a lot of thought to that.

MS. WALD: Maybe a little.

MR. BELLINGER: My general sense from the surveillance that I saw was in fact that we are very targeted on specific intelligence requirements.

These are not broad dragnets of the surveillance of average individuals and so this is not a great violation of the rights of privacy of every single foreign national, that's very much focused on individuals who may pose a national security threat or for which the United States has a valid intelligence interest.

MS. WALD: Would you, for instance, think that taking national security, assuming you didn't have a national security risk, that basically non-U.S. persons we should try to approximate as much as we can within those restrictions the equal treatment in use, retention, that kind of thing of non-U.S. persons in our surveillance, or not?

MR. BELLINGER: I think that some of the things that the Obama administration,

President Obama has been focusing on to ensure that, particularly for the information that is collected, that we ensure that it is kept private.

I mean I would be personally, I haven't seen this happen, but I would be personally extremely concerned if we found that the United States had collected information about foreigners great or small, either a world leader or a lesser known person, and then we're not careful with that information and were to let it out. That would very much interfere with that individual's right to privacy.

I think, you know, as a national security official it's important for us to collect the information that we've collected, but we need to be extremely careful with it. So my sense is that as a policy matter these privacy concerns are important.

MR. MEDINE: Mr. Dempsey.

MR. DEMPSEY: My question I guess for Laura Pitter and maybe also for Mr. Sieber. Among the major, certainly the countries that Chris Wolf

looked at and cited, but among the other major democracies that do foreign intelligence surveillance, is there anyone that has a law which you would point to as a better model?

MR. SIEBER: Could you ask the question?

MR. MEDINE: Is there a country that has a better model of surveillance than ours? Is that --

MR. DEMPSEY: Yeah. In other words, what other country has a better model, a better law, more checks and balances, more controls, more limits?

MR. SIEBER: In general.

MR. MEDINE: In general, checks and controls balancing privacy and civil liberties and national security.

MR. SIEBER: It's a very broad question --

MR. DEMPSEY: Just pick one.

MR. SIEBER: Because you have to consider many, many aspects, not only the

extraterritorial implication. I just can give you some reliable differences a between the German system and the U.S. American, that's what I can witness on.

If you have a look at the German system you have to see that Germany has a very strong constitutional court and is very much attached to fundamental rights. This is a reaction to the Nazi cruelties and any steps towards this direction should be prevented. This is the reason for some very basic differences between the U.S. and Germany.

The first one, for example, is that intelligence agencies in Germany have no executive powers. So they cannot execute arrest warrants or anything like that. They just can collect the information. This is based on the idea that the lack of control which we have in this area of intelligence agencies must be balanced by lesser constrained measures.

Secondly, Germany has constitutionally founded strong separation of powers and separation

between the police and the intelligence agencies. This has been changed a little bit after 9/11 but still there is a fundamental separation.

Information exchange is only possible in a very limited way for very, very serious, serious crimes.

So I would say the differentiation between the institutions is stricter. We don't have multipurpose institutions like the FBI.

On the institutional side there is an absolute strong separation between these institutions, despite certain common datas and things which we have done after 9/11.

You could go further, if I compare it and look around at the control agencies which you have. In Germany it's separated. For internal surveillance we have a special commission appointed by the parliament, G-10 Commission who is doing the job. It's not called a court but the functions are similar.

And for foreign intelligence agency, the BND, there is a parliamentary commission who

does these things.

Maybe one last point, if you look at the aspect of protection of foreigners' rights and applicability of the constitution abroad, the German attitude is more in favor of applying the national constitutional guarantees.

With respect to the first question, which is foreign territoriality, section 1 of the basic law says that the basic law binds all public authority. And this is in general irrespective of whether it's in the country or outside the country.

There are differences of course, but they have more to do with the different circumstances, because the risks coming from abroad might be bigger than coming from within the countries, and for that reason I absolutely agree that the systems might be different for internal intelligence and external.

But it's not based on the fact that we do not apply the constitutional guarantees abroad, and it's definitely not based on the fact that we

are giving different rights to foreigners and to citizens, at least in this area of dignity rights, of human rights, and especially in the privacy rights.

So for example, there was a German decision of the court which was controlling intelligence gathering for abroad and which checked these systems.

So with respect to this question which we are dealing here, if I generalize it I would say we are more open to applying these fundamental rules. We do not reject it as it's not applicable. We don't go into these (inaudible) stay out of it. We would apply it, but then we have a proportionality principle and we check whether the things are justified.

And for example, in this decision I mentioned, the court said, yes, dangers coming from abroad are bigger, bigger dangers, and with balances and this law was in general justified with one exception.

It was applied also by law to internal

conflicts, and the constitutional court said it cannot apply just like that.

So I think these are the main interests which I could tell you. It's impossible to say better or worse. I would never, never do that.

MR. MEDINE: Thank you. Ms. Cook.

MR. DEMPSEY: We'll come back around.

MR. SIEBER: And if you permit afterwards I would like to say a few words with these International Convention 17, the applicability, but I don't want to --

MR. MEDINE: We'll come around at the end.

MS. COLLINS COOK: So I wanted to thank you all for coming and to congratulate you for being the panel that has come the farthest set of distances to participate today. I think it's very helpful to have this type of discussion in an open forum.

We've talked a fair amount today and all through the day about skepticism about U.S. law and U.S. practices. I think it's fair to say

there is also a high degree of skepticism about the contours -- let me get closer here.

I think it's fair to say that there's a high degree of -- if I can get through this question without hurting someone, this is really going to be my goal for the day.

(Laughter)

MS. COLLINS COOK: There's a high degree of skepticism about the contours and applicability of international law as well. So having experts who are able to speak to these issues is critical, I think, to us.

And I wanted to draw off of something, Professor Sieber, that you had mentioned and I have to confess it was not a focus of mine coming into today. I had been focused on the ICCPR and the potential applicability of Article 17.

But you talked about the interests of states, and if I understood what you said correctly, that the interest of a state in its own sovereignty is inviolate, that surveillance by one country in another country is a violation of that

sovereignty, there is no exception under customary international law that would make that any less of a violation of the state's sovereign status or rights.

So that's the academic point. That would lead me to think that no one was conducting surveillance on anyone else, that no country is doing surveillance.

But as a practical matter I think it's fair to say that every country is either engaging in foreign intelligence collection or attempting to engage in foreign intelligence collection.

So if you can explain to me how you can have a principle of customary international law, here the absence of an exception that is honored by not one country in the world, as I understand it.

MR. SIEBER: Yes, I remain with the saying that there is no permission of espionage under international law because the principle of self-defense, that needs an armed conflict for it. It's not there for the ordinary case.

And customary law would require an opinio juris, the conviction of the people that espionage is right.

But our estimations, that are split. If we are considering our own law, we say, yes, we do it and we give them a medal if they are successful. If we are considering the other, we say it's illegal.

So there are two regimes of law which come to different results. We live with that but we cannot say that international law has a general view that we can, that we can do it.

We have this problem in a very interesting case with the German reunification because when the two parts of Germany came together, there have been people doing espionage in East Germany and they are now under our jurisdiction.

This question came up and here again the Constitutional Court said there is no general violation of international law, and I think you agree with that. We have to live with this

conflict.

And in the global world that's normal. The world is getting so diverse that we have many conflicting regimes today now, so we can stand with that.

MS. COLLINS COOK: So I guess my question, perhaps Mr. Bellinger, you can speak to this, is it a violation of international law in terms of infringing the interests of another state to engage in sort of foreign surveillance?

MR. BELLINGER: I was going to jump on that as well. And the answer to that I think is clearly no. I am not aware of any country who believes that the U.N. Charter's statement on the protection of territorial integrity and sovereign equality of states actually prohibits electronic surveillance of another country.

Certainly if that were the understanding of our senate that in becoming party to the U.N. Charter that prohibited us from spying on another country because it would violate their sovereign equality or territorial integrity, then

we would get out of the U.N. Charter immediately. But I am not aware that any other country believes that as well.

So there is not, the principle of territorial integrity and sovereignty would apply to, say, for example, use of force. International law does not prohibit electronic surveillance or spying. Domestic law may.

And so that's really, you know, when we talk about international law, that basically means that there is a compact between countries. Judge Wald knows this very well, you know. Countries have to have agreed that they are not going to do these things to each other.

And in the U.N. Charter, the U.N. Charter was not saying we promise not to spy upon one another, we were saying we promise not to use force against one another.

U.S. surveillance in another country might violate the other country's law, but it is not a violation of international law.

MR. MEDINE: Let's go on to another

question. We'll give Ms. Brand a chance and then we'll come back.

MR. SIEBER: Because I think I have to contradict.

MS. BRAND: All right. Let's see if this microphone will work now.

Thank you all for being here today. One of the things I find frustrating about this discussion, not here specifically but in general is that there is a tendency to not distinguish between what is law and what is -- it's not working is it?

And what is either what people would like to be the law or what is a matter of policy.

And John, thank you for making that distinction very clearly in your remarks.

I was having a little bit of a harder time, Laura, following where you were moving from what you think is actually binding law to what is not.

And so I wanted to know if we are looking, setting aside policy, aspirational policy

for a moment, if we were trying to determine whether what the government is doing under 702 is legal, do you think there is some binding international law instrument that affects that questions?

MS. PITTER: Yes. I mean from my position it is a violation of Article 17 of the International Covenant on Civil and Political Rights. The United States does not recognize that, and that's part of the problem.

MS. BRAND: So let me just ask a question then. If the U.S. government doesn't recognize that, what is the body, what is the document, what is it that then makes that law binding on the U.S., on the agencies implementing 702?

MS. PITTER: It's the treaty itself. As Mr. Bellinger said, you know, a treaty is something that governments have agreed to abide by and to honor the commitments in the treaty in good faith.

MS. BRAND: And what is the body that

has the last say on the interpretation of the treaty, right? Because obviously the U.S. government interprets the treaty differently from the way you interpret the treaty.

Is there some other body besides the U.S. government itself whose interpretation of the treaty is then binding on the way the U.S. agencies implement it?

MS. PITTER: Well, the Human Rights Committee is one of the most authoritative sources on this, but --

MS. BRAND: But is it legally binding, right? That's my question, not is it persuasive, is it binding?

MS. PITTER: I mean from the opinion of many other governments it is. The treaty is binding upon them. The United States does not recognize the extraterritorial application of it.

MS. BRAND: And this is an honest question, give me an example of a country that views the ICCPR to have extraterritorial application with respect to surveillance of

foreigners abroad that itself that takes its own advice or heeds its own interpretation.

MS. PITTER: So this surveillance, as I said, is a novel issue. It's not something that's been addressed by the case law, and especially not since the revelations from Snowden which have disclosed, I think even to policy makers in many countries, the degree to which the law, the domestic law on the books is actually being applied, and the vastness of the programs, how much data is actually being collected.

So it's a novel interpretation, I mean it's a novel question, as it is in the United States --

MS. BRAND: I'm sorry to cut you off but we have a strict timekeeper here, the Chairman, and I want one last question.

I'm interested in your interpretation of what constitutes control and how being surveilled essentially would put someone within the control.

My concern about that interpretation in

part is that I'm not sure what meaning is left in the phrase, under its jurisdiction. If the statute talks about territory and jurisdiction, if jurisdiction means something in addition to territory, it seems like a meaningless phrase if it can include surveillance.

MS. PITTER: Well, it is meaningless in the sense that the United States has taken up, used the technology to conduct surveillance on a very mass scale. So it affects an enormous number of people.

The, you know, jurisdictional clause has been interpreted extra-territorially in the context of detention and torture, in which a smaller number of people have been affected. But when you're talking about surveillance --

MS. BRAND: But detention, I mean someone being detained or tortured is, I would say, much more clearly within the control of the government who has detained or is torturing them, right?

So my question is when you get into

surveillance and the person is clearly not within the physical custody of the government in question, what is it within the ambit of the treaty?

MS. PITTER: So you can look at it two ways there. You know, their communications are within the effective control of the government and so that's one way to look at the obligation.

But in addition, they have an obligation to ensure the rights within the covenant territorially, but also to respect the rights in the covenant extra-territorially.

So although they are not necessarily bound, you know, to enact legislation domestically regarding, you know -- well, they're not necessarily bound to ensure the rights of individuals with regards to privacy extra-territorially, they are bound to respect those rights extra-territorially.

MS. BRAND: I see my time is up.

MR. MEDINE: Mr. Garfield, in your statement earlier you indicated that the

revelations about the surveillance programs, particularly 702, has had significant international impact with regard to business dealings with U.S. firms, and you proposed a number of steps to ameliorate that, and I wanted to ask you about some of them.

And you also mentioned one of them, namely transparency in your remarks earlier. Do you have thoughts about what level of transparency would be helpful to companies, but taking into account national security concerns?

As you know, our first report on 215 did recommend greater transparency, but in terms of disclosures that a company can make about surveillance requests from the U.S. government, so long as that took into account national security.

And I guess in particular if you have comments on the agreement that was reached between the Department of Justice and a number of firms, whether that agreement goes far enough and provides sufficient detail to give comfort to business partners of those firms overseas.

MR. GARFIELD: Thank you for the question, first of all. The agreement with the Justice Department is viewed as a significant step forward. There are additional steps that can be taken that would be helpful as well.

One is the level of detail that the companies are able to share, including disaggregation of data between Section 215 and 702, or whether it's a national security letter. So a greater level of granularity would be helpful.

The second part of that is it is not only important that the companies be able to share out information but that the government share information as well and provide greater transparency, which is often lost in these discussions.

The debate that's been taking place today speaks to the importance of greater transparency because 702 already includes a number of protections that are not generally known, particularly internationally.

To Christopher Wolf's point, if they were more well-known it would be clearer the extent to which steps are being taken in the United States that are not necessarily being taken in other countries.

MR. MEDINE: And you also recommended, made a couple of other recommendations that you put forward were oversight, the importance of oversight and in discriminant collection.

And I guess the question is in the 702 program isn't there already oversight through the Foreign Intelligence Surveillance Court and some of the internal government processes?

And with regard to indiscriminate collection, I think as we heard earlier there has to be a foreign intelligence purpose, and so it's somewhat constrained. Do you think that with regard to this program it meets those requirements?

MR. GARFIELD: Correct. My recommendations there weren't intended to suggest that it in fact was indiscriminate. It was

suggested, it was a suggestion that taking steps to be clear about the protections that are in place and to the extent it is not, it is in fact not indiscriminate, to reaffirm that would be helpful as we go about doing our business internationally.

MR. MEDINE: And Mr. Wolf, you analyzed other country's laws and shown that they're not only not better but maybe not even as good as our laws by some criteria. What lessons should we draw from that in terms of how countries should conduct their surveillance programs?

MR. WOLF: So the purpose of our white paper and our research was really to be expository than to reach judgements and to pick winners and losers or to decide whose was better or best.

But we thought it was important in light of the claims that were being made, particularly by the cloud industry in Europe that there is national security access obviously that goes on in the EU and elsewhere around the world, and often without the controls and safeguards and

transparency that we have here.

So the overall conclusion that we reached is that this is a global problem. Obviously it's one that has been focused on intensively here in the United States because of the Snowden revelations, but it is an international issue that needs to be resolved internationally, particularly with the sharing that goes on among intelligence authorities.

It is heartening that the European Parliament in its resolution last week adopted the draft report that came out in January that focused on the European intelligence gathering practices.

We hope that the data protection authorities in Europe who've been vigorous critics of the NSA practices will comment on their own country's practices. They've been relatively silent on that, and we think the debate that has to be made should be among all those interested in privacy protection, and obviously that would include the privacy commissioners abroad.

MR. MEDINE: Obviously countries have a

lot of self-interest in conducting surveillance programs. Do you see a forum in which countries can or even should agree with the methods by which they conduct surveillance?

MR. WOLF: So that's well above my pay grade. I really don't have a view on that.

I do have, if I can just mention on the transparency point, we did a white paper in August that then general counsel of the Commerce Department Kerry cited in his speech at the German Marshall Fund that actually showed on a per capita basis access by national security and law enforcement on a per capita basis is larger outside the United States in many instances.

MR. MEDINE: Judge Wald.

MS. WALD: I have two questions for Ms. Pitter. Given what most or many observers concede are widely varying practices in different countries about surveilling their own and other country's citizens, would you advocate, as we sitting here have to make some observations, maybe recommendations on 702, would you advocate that we

unilaterally, we recommend unilaterally putting in place one and the same protections for non-U.S. person surveillance that we have for U.S. citizens? Or two, raising the non-U.S. citizen person protections to the level that the official bodies of these international organizations that we've talked about say they should be?

If you come out on the second, what specific criteria do we have to go on as to what those practices would be?

In other words, there's a slightly cynical end to the question, what would be the additional protections in real time to privacy interests of non-U.S. persons if the U.S. took a position that the ICCPR does apply to our activities outside territorial U.S., but that we've already met those standards, such as seems to be the case with some of the other countries who espouse the official broader interpretation of ICCPR but then go on their way, as Mr. Wolf suggested, and don't really raise those?

MS. PITTER: This is to me?

MS. WALD: Yes, this is to you.

MS. PITTER: So, I mean I think one clear change that needs to be made is the purpose of the surveillance needs to be much more targeted. The definition of foreign intelligence information is just much too broad. It encompasses, you know, things that, conversations that could be just about generally the foreign affairs of the United States.

And I know we heard in the panel testimony earlier that that is somewhat reined in by certifications but those are not public and we've not seen them.

There should be a lot more transparency in the law. I think the difference in the German law is that there is a lot more transparency. The capacity also is less in Germany. I mean the U.S. has vast capacity, so you know it affects a lot more people.

But definitely a more narrow, a more targeted approach, and applying, you know, necessary and proportionate principles to the

surveillance as well, I think would go a long way.

There's probably plenty of room for recommendations. I probably can't get into all of them here but that would be --

MS. WALD: In general would your standard be that there should be a presumption that we treat non-U.S. persons like U.S. persons in our surveillance activities, or rather that we go to the best practices we can pull from that people who endorse the ICCPR, even if we don't actually endorse that application?

MS. PITTER: So I think that there can be differences in the law itself but it has to, the differences have to be ones that don't impair the impact of the right itself.

So the right to privacy has to be part of, it has to be made part and parcel of the assurances, but they can be different for practical reasons when it comes to --

MS. WALD: Can you give us, in my remaining few seconds, some application of what you've just said to 702?

MS. PITTER: Well, I'd like to go into, you know, a more detailed analysis here but right now there's --

MS. WALD: Well, just quickly.

MS. PITTER: There's not a warrant requirement, for example, under 702 for individuals, but there should be -- it may be that it's not a practical requirement to have a warrant for individuals outside of the United States.

And it's not just individuals under 702, it's also facilities and about targeting as well.

But the procedures that are in place to protect against sort of suspicionless, you know, there's no standard for what authority has to find before it can target an individual. The main distinguishing principle is that it's a foreigner, and that that information is going to be acquired for foreign intelligence purpose, for foreign intelligence purpose, so that is too broad.

MS. WALD: Okay.

MS. PITTER: Does that make sense?

MS. WALD: Yes. All right, very quickly I guess, Mr. Wolf, your testimony, you know, recited the report about the lesser, basically the lesser protections most other countries including our close allies give to privacy, at least despite some of their countries adherence to the ICCPR's broader definition of privacy, yet you also note that the economic risks to U.S.-based telecommunication companies from threats both from competing companies inside those countries and from the governments themselves that they may balkanize and insist on collection and storage activities being conducted in-country poses a real risk.

Is it above your pay grade to give us some indication of what line or policies the U.S. should follow given those two competing concerns?

MR. WOLF: Well, I think our concern in doing the work that we did on the white paper was the misperception that was arising --

MS. WALD: Let's assume you've done those and that they are real, but also are real

the threats to the competitiveness of U.S. companies if foreign governments and peoples get very excited and want to keep everything inside their own countries.

MR. WOLF: So our position is that they're deceiving themselves if they think that when they keep data presumably within the four borders, four corners of their own country that it's safer from surveillance, not only from their own surveillance authorities, but of course through the sharing arrangements from surveillance authorities from elsewhere around the world, and that the Balkanization of data is not a useful global phenomenon at all.

MS. WALD: Well, what can the U.S., or what could we recommend they bring them together?

MR. MEDINE: Judge, your time has expired. Mr. Dempsey.

MS. WALD: Right. You can think about it.

(Laughter)

MR. DEMPSEY: On my last round we were

talking about what were, if any country's laws that did a better job here, and Mr. Garfield, you were ready to jump in. Do you remember what you wanted to jump in on? I wanted to give you a chance to make the point, if you still remember what it was.

MR. GARFIELD: It really was the point that was made in response, which is that in fact our experience in carrying out our business is that there aren't many, if any, other countries that have as many safeguards in place.

The lack of open discussion through multinational engagement as well as transparency here in the U.S. furthers that false perception that somehow other nations are doing more than we are. And that is certainly something that whether through legislation or recommendations from the PCLOB, we can do something about.

MR. DEMPSEY: The question for Laura Pitter, a couple of other witnesses have raised this and a couple of times I grabbed for the book in order to raise it and didn't get a chance to,

the definition of foreign intelligence, as I read it, it means information that relates to the ability of the United States to protect against actual or potential attack, grave hostile acts of a foreign power, sabotage, international terrorism, international proliferation of weapons of mass destruction, or clandestine intelligence activities. None of those are too broad, I would think.

And then it says, information with respect to a foreign power or foreign territory that relates to the conduct of the foreign affairs of the United States.

I mean isn't that precisely what foreign intelligence is supposed to be about, information with respect to what foreign countries are doing that might affect our foreign affairs? Why is that too broad?

MS. PITTER: I think that the first category of information that you said could, it would be permissible. But the general foreign affairs of the United States allows for the

collection of a vast amount of information that does not necessarily have any national security purpose.

MR. DEMPSEY: No, but it has foreign affairs purpose. It is by definition about the intent of foreign governments, and are you saying that other countries self-restrain themselves from trying to understand what their adversaries are doing, even in matters that don't involve attack and so on?

MS. PITTER: I mean if other country's laws are overbroad and vague then they're in violation of, you know, the International Covenant on Civil and Political Rights as well.

MR. DEMPSEY: Well, I think John would say that if everybody is doing it, it probably isn't a violation of the treaty. Everybody didn't bind themselves not to do what they all were doing at the time they bound themselves to the treaty.

MS. PITTER: Well, you know, the revelations about how this is applied are just coming out now and there are going to be

challenges and there already are challenges to the law.

And I think we're going to find that there is room certainly for reining in the overbroadness of some of the statutes as they exist right now.

I think that because it allows for the communications of things that don't necessarily have to do with national security, that it just, it's overbroad and it's impacting, you know, the United States in other ways.

MR. DEMPSEY: In what way is the collection of information about foreign affairs overbroad?

MS. PITTER: Because it could be, you know, someone talking about, you know, their opinions about the foreign affairs of the United States --

MR. DEMPSEY: Not someone talking about their opinions, it's the information with respect to a foreign power. So this is not Joe Schmoe in Germany saying I like or don't like the United

States, this is about what Germany thinks about the United States.

MS. PITTER: It merely has to relate to the foreign affairs of the United States --

MR. DEMPSEY: Yes.

MS. PITTER: In my opinion it's too broad. It allows in for much too broad a type of communication.

MR. DEMPSEY: No, I'll yield. I'd like to have another round, a third round if we could, but I'll yield for now.

MS. COLLINS COOK: Mr. Bellinger, I think you had put your finger up midway through that and I'd like to follow on this conversation as well because it struck me.

First, where would you draw the line? And I'm struggling to determine what precisely is impermissible about collecting foreign intelligence in the category of foreign affairs as set forth in FISA.

MR. BELLINGER: Yeah, so thanks for that question. And I think this is a very

important point, and Judge Wald started it and you have continued it.

We have to be really very clear about what international law is. International law is not principles that we think would be fine, policy principles that you and I might agree.

International law, if we are serious about international law, and this actually is the definition of international law, are things that nations agree to, to be bound by, by treaty or that is customary internationally, meaning that countries do it so often that everybody does it and they do it by a sense of binding legal obligation.

So two points here, and Judge Wald, I heard you say that while it is true that other countries actually take a broader definition of whether the ICCPR applies extra-territorially, I'm not aware of any country in the world that believes that the ICCPR actually binds them with respect to electronic surveillance, that that right to privacy in Article 17 actually limits

their ability to conduct electronic surveillance of foreign nationals. So that is just not a treaty obligation that countries have accepted, even under the ICCPR.

It might be something that human rights groups wish were the case, but it is not something that governments have accepted, and certainly not something the United States government has accepted.

And then just one more round on the Human Rights Committee. Again, the treaty itself does not say that the decisions of the Human Rights Committee, which is basically a group of academic experts, are binding. Governments who write treaties know how to write language.

For example, the U.N. Charter says that we undertake to comply with rulings of the ICJ. But the human rights monitoring groups, countries have not said that we undertake to comply with their decisions.

And in fact, the senate, and all of you know this, the senate would never agree to cede

responsibility for the future interpretation of a treaty to a group of academic experts. That would take completely out of the hands of the shared understanding between the executive and senate, the interpretation of a treaty.

So you know, the United States, and this is the view of the Obama administration as well, you know, recognizes that other people may not agree on the extraterritorial application of the ICCPR, but you know, no country believes that the ICCPR actually limits electronic surveillance.

MS. COLLINS COOK: So I just wanted to as a follow-up question to Ms. Pitter. Thank you. I know we've aimed a lot of our questions at you.

I think there's a sense within the United States government, a little bit of exasperation, the concern is that our surveillance lacks transparency or that we are somehow outside the mainstream of what other countries are doing.

And I look at 702 in particular and I see something where our legislative branch has specifically said exactly what our executive

branch can do. The executive branch, which is headed by democratically accountable individuals then oversees the execution of that authority, it is subject to the oversight of the judicial branch and it is subject to the oversight of our legislative branch.

So I guess my question is systemically what else could the United States be doing to help build the confidence and trust of other countries?

MS. PITTER: So the oversight so far has all been in secret. I think that's one problem. I mean even the first panel today said they were in the process of declassifying a large number of documents and they were looking at doing that because they recognize the importance of transparency.

The oversight has not, I mean if you look at what happened with 215, even --

MS. COLLINS COOK: I was talking about Section 702, which is the focus of our --

MS. PITTER: We don't know the details of the oversight regarding 702, so the only

information I have about oversight would be regarding 215. And we saw that the judicial oversight in that context, you know, would up, there was an opinion that had an impact on the vast number of communications of Americans that was kept secret from the Americans, so --

MS. COLLINS COOK: Well, let me push back a little bit on this notion that the oversight is not transparent.

So again, we have a statute that tells the world exactly what the executive branch must present to the judiciary, what findings the judiciary must make, what authority judiciary has vis-a-vis that application, and the framework for this surveillance.

We have a public statute that also tells you exactly what the executive branch is obligated to share with Congress. So where's the lack of transparency in that?

MS. PITTER: Well, the judicial oversight for the 702 program is annual. They look at just the procedures. They don't actually

look at the individual targeting requirements. That's done by an NSA analyst at his computer desk.

MS. COLLINS COOK: Actually I think if you were here for the first panel the testimony by the first panel was that that is not in fact the case, that it is an ongoing process of oversight. There are regular reporting requirements, both to the court and to the Congress, so.

MS. PITTER: I was, I did hear the first panel, and I believe he said that those targeting decisions by the analysts are reviewed eventually, but it's not something that's done at the beginning. So the --

MS. COLLINS COOK: So if there's not public review of specific targeting decisions, so this, the United States government saying we would like to collect foreign intelligence information about this specific selector, that's a lack of transparency that is problematic for you?

MS. PITTER: Well, the transparency, even the certifications that the FISC court gets,

there's no, they don't even see the identifiers or the selectors, they just approve the procedures. So you know, that's a problem with the oversight. In terms of --

MR. MEDINE: I'm going to let Ms. Brand pick up since we're at time. So thank you.

MS. BRAND: Okay. I guess maybe this question is directed at John but if anyone wants to jump in, that's fine.

If the ICCPR did have application to the U.S. government surveillance of non-U.S. persons abroad, setting aside the territorial issue for a minute, what does privacy mean in that context?

I have found the lack of a universally accepted definition of privacy very frustrating writ large across everything that we do, and I mean the same issue pertains here. So I guess is there a universally accepted definition of privacy? Is there a definition of privacy that is binding on the U.S. government? If not, how would we find, who would supply such a definition? If

you can sort of help us understand that.

MR. BELLINGER: Yeah, so that's a great question. And that's really the third prong. I mean the reason that the ICCPR doesn't apply is, one, there's the within its territory and subject to its jurisdiction. Then even if it were subject to our jurisdiction, then it has to be within the power and control.

And you know, no one is really going to legitimately argue that, as I think you said earlier, power and control in the view of those who take that interpretation of power and control is someone that you actually physically have in your custody, not electronic surveillance.

And then there's the issue, even if those applied, is something unlawful or arbitrary violation of privacy? And there are not definitions that are universally accepted.

You know, people can argue about these things but for it to be law that a country actually violates, there has to be an agreed definition on privacy and there has to be an

agreed definition on what is arbitrary, and there just are not those definitions.

You know, again, someone can say that someone has an absolute right not to have any country pry into anything that they're doing and that that's a violation of their privacy, but there's not an accepted definition of that.

I mean I could frankly imagine if one were to accept the first part of your premise, which is that it were to apply extra-territorially, and let's also say that it were someone within the U.S. jurisdiction, let's say someone, the United States is actually holding a terrorist in another country and we agreed that the ICCPR applied, we agreed the person was within our power and control, and then we were to do extensive interviews of that person about the person's private life, and then we just publish it willy-nilly, not as part of a criminal proceeding but essentially just as a leak, well, you know, there might be an argument that that might be an arbitrary intervention with that person's right to

privacy.

But I think that's -- there's not a definition of privacy, or of arbitrary, or unlawful that is binding as a matter of international law.

MS. BRAND: Chris or Laura, any thoughts on that question?

MS. PITTER: Would you repeat that question again?

MS. BRAND: Just what does privacy mean in the ICCPR context? Where does the definition come from? How would you find the definition?

MS. PITTER: Well, it guards against unlawful and arbitrary interference with an individual's privacy, so there has to be a respect for correspondence, for example, and a respect for an individual's personal space, and there has to be an ability to have personal space to communicate.

MS. BRAND: Where are you getting that definition?

MS. PITTER: Well, that's, I mean

that's coming from the interpretation of, the right to privacy is connected to freedom of expression, freedom of association. It impacts that. And you know, the right to correspondence comes from that as well. So I mean it's defined in the treaty itself, and --

MS. BRAND: What is the definition? Humor me.

MS. PITTER: I mean --

MS. BRAND: I can look it up, never mind. But it sounds like what you're giving me is sort of your sense of what privacy entails, not a sort of legally defined or legally articulated definition. Chris?

MR. WOLF: So a privacy lawyer's answer goes back to Brandeis and Warren who said the right to privacy is the right to be left alone. But they recognized and I think it's been recognized ever since, that was 1890, that there are exceptions for the good of society, for law and order, for social good.

And that's really where the rubber hits

the road. What are the permissible exceptions for national security surveillance? And you know, that's the discussion that needs to be had globally.

You know, Judge Wald asked what should the U.S. government do? I think it should promote that discussion as a global matter, and at the same time I think it should promote the decoupling of national security surveillance from cross-border data flows for commercial purposes.

The threat to withdraw safe harbor, for example, the declaration that the transatlantic trade and investment partnership shouldn't address data because of what happened with national security surveillance is a non sequitur.

Those issues need to be dealt with between governments, but that shouldn't interfere with cross-border data flows, which have to have privacy protections built-in, no question. But those are not something, that isn't something, the surveillance issue is not something that the companies themselves can really address and

they've done about as much as they can in pushing for transparency, pushing very hard.

MR. MEDINE: Dean, did you want to add something?

MR. GARFIELD: The question was asked earlier about what the appropriate venue is and I would say a reminder that the strategic and economic dialogue didn't exist beyond five years ago, and so this is one issue that's getting left behind in the discussion, the importance of creating a framework and a venue for greater multinational dialogue around the surveillance issue. And I think the PCLOB in its recommendations can have a dramatic effect in this area.

MR. SIEBER: It's clear that we have not an international definition because the countries are too different. However, in the countries and national law, and European law and in other legal bodies these definitions are emerging. And of course they have to develop.

What is sure is that there is a core

area of privacy where we all would agree that privacy is infringed. For example, if you directly do intelligence gathering on the sexual life of somebody who is not a suspect, there's no reason, that's a clear core area infringement of privacy.

Now if you go further, it's becoming of course a difficult, mass surveillance of people against which there is no suspicion would be one aspect where we'd have to investigate.

Another one is to create a complete picture of the private life of somebody going back to his birth, whatever did he do, did he demonstrate in school? So collecting enormous mass of data on one person would be another aspect, just illustrating. There are cases which fall under something like that.

And we should work on this definition and the fact that we do not have something like that would not lead me to the conclusion we shouldn't go in these things.

It's the same with this attitude on

extraterritorial application and things like that. These questions are so new that you cannot find any government's position here. So for me, that's not a valid argument. If you are pioneers on these questions, we cannot say the governments are not yet there.

I agree with you it's a political question on this issue.

One final point where I do not agree what was said is the question with respect to territoriality. If you are collecting data in a foreign country from (inaudible) it's clear that's legal. You are not infringing the foreign territory.

But if you go to a foreign territory and you switch on servers, you download countries -- the electronic pulses, you are changing and you do a function that usually the police does, this is a clear infringement of territoriality.

And you can see this especially in the cyber crime convention where we are fighting about these questions. We have Article 32 B with a big

struggle between the U.S. and Russia, which is bringing down the complete process of the cyber crime convention. We all agree that except these cases mentioned in Article 32 of the cyber crime convention ratified by the U.S., any police activities doing access to foreign countries are of course infringements of privacy. Nobody would claim that this is legal. We could stop the process of the cyber crime convention if your statement would be, all right, like that in this generality.

So I would say that we have to remain -- these surveillance activities do not in any case infringe territoriality but there are many cases, especially looking at the cyber crime convention, our agreements which we have on this committee, we all would say that's a clear infringement of the sovereign territoriality of a country. And it is also undisputed that the protection of territoriality is guaranteed, not only by Article 2 of the U.N. Charter, but also by customary law. It's one of the basic principles

since the Westphalia Peace Accord.

MR. MEDINE: Let's give John a chance to respond.

MR. BELLINGER: I'll be brief. On the second point, again I would say that I don't think any country in the world would say that the Article 2 of the U.N. Charter's protection of the territorial integrity and sovereignty of states would mean that they cannot conduct essentially espionage activities from anywhere. I just don't think that's what the U.N. Charter says.

But more importantly, the first thing you said really goes to the heart of our discussion here, where you said this is an evolving national dialogue about privacy and it is a dialogue that is going on nationally in different countries, and it therefore is going on internationally.

But the question at least that was put to several of us, to me and Laura in particular is, is there a binding international law standard right now? And the answer to that is clearly no.

Germany may have laws inside Germany, given its particular past. Other countries may have particular national laws. Sooner or later countries may get together and agree on things, but right now there is not an international legal standard, either in the ICCPR or anywhere else that limits electronic surveillance from the United States, or again, from any other country.

Other countries would not agree that there's not an international legal standard -- or that there is an international legal standard.

MR. MEDINE: We have time for just a quick round that Jim had requested. Let me just ask just to clarify one point, John, the treaty ICCPR is not self-executing. What does that mean and is there any forum in which enforcement action could take place?

MR. BELLINGER: That means that it would require implementing legislation for it to be, so it's binding as a matter of international law and we have implemented it already and are in compliance with it in certain ways because of laws

that we already had on our books, or might thereby have our Congress pass. But it does not have automatic legal effect merely by the United States becoming party to it.

MR. MEDINE: And is there any forum in the world where we could be held accountable for compliance with the ICCPR?

MR. BELLINGER: The U.N. Human Rights Committee monitors our compliance and comments upon things that we are doing. That's what happened last week when we presented our report. And the United States commented on or responded to these comments, but that's not judicially or legally enforceable.

MR. MEDINE: Thanks. Judge Wald.

MS. WALD: Just a quick comment. Am I not right, John, that not in this context of surveillance, but hasn't England at times relied in some of its judicial decisions on the ICCPR for the, to disallow, I think in dealing with some detainees or asylum people, etcetera?

So my impression was there are courts

who have actually relied upon the ICCPR, not in the surveillance context but in other contexts.

MR. BELLINGER: You and I would have to look at those together. It may have been the European Convention on Human Rights. There has been a fair amount of jurisprudence recently on the extent to which the European Convention on Human Rights creates obligations on British and European forces who actually do have someone within their control of their military outside of Britain, or Germany, or elsewhere.

MS. WALD: Okay. I'll let you off. Very quickly I have one question, quickly, for Mr. Garfield, and that is that the statement that your organization provided to us spoke of the need for meaningful oversight by an independent body in government as to the surveillance programs, including access to collected data.

Just wondered very quickly, who you had in mind, was it the IGs, us, FISA, Congress? Did you have particular independent bodies who would provide the meaningful insight, which included in

your statement oversight of collected, access to the collected data?

MR. GARFIELD: We did not.

MS. WALD: Okay, that's a succinct answer.

MR. MEDINE: Gives you a concise answer.

MR. DEMPSEY: Rather than a question I'll just offer an invitation, which is if any of the witnesses could provide us with guidance on the question I posed, what would be a better way of structuring a foreign intelligence system.

I think at the end of the day any concept of law, any set of rules is going to recognize that different countries are going to have somewhat different structures. So the German structure is robust but different from the United States. The United States believes it has a robust system with different elements than Germany has, etcetera.

Has anybody put together or could anybody put together a list of the elements of a

system and then some sense of how you come up with what is the minimum?

We talked a lot about judicial oversight but Germany does not have. The court reviews the statutory structure but not the individual implementation, does not do individual targeting on the strategic surveillance in Germany. In the U.K. it's all administerial, not judicial.

Secondly, if any further thoughts on how we get from here to there. So several witnesses have said it's an evolving situation. We have new questions, questions which to my view are not answered in the existing documents. Let's just say that it's not answered. They don't apply. No one thought about this. It hasn't been answered. How do we move forward, we, the world, or maybe the U.S. and Europe, which have more shared values than we sometimes admit, how do we move forward in getting that kind of commitment?

And the industry in Garfield's paper is that a global, I think implicitly recognizes we

need global understanding, even if not all of the laws are the same.

So any thoughts that you can offer us. Not right now because we want to move along, but any further follow-up thoughts you could offer us in writing, please, it would be very helpful on both of those points.

MS. COLLINS COOK: I just wanted to thank you all for coming. As I said at the beginning I think it's important to have these discussions. I won't assign homework or request any follow-up, but it's an education process for us, as well as for the American people, particularly on these issues.

So if there is information you think should be a part of the public record, which will remain open, I'm sure David will explain, it is welcomed.

MS. BRAND: I won't take up anymore of your time since we are at the end of our schedule here. But I want to thank all of you for coming. It was very helpful to me, so thank you for taking

the time to prepare and to be here.

MR. MEDINE: Thanks again to all the speakers and the Board staff that made this hearing possible. The Board's activities for today are now complete.

The Board encourages all those who are interested to submit, panelists and members of the public, to submit written comments on this topic at our website of www.regulations.gov. And the deadline for submitting comments is March 28th. All comments submitted will be available for review by the public. A transcript of today's hearing will be posted on PCLOB.gov.

And I will now move to adjourn the hearing. All in favor of adjourning the hearing please say aye.

(Aye)

MR. MEDINE: Upon receiving unanimous consent to adjourn, we will now adjourn. The time is 3:40. Thank you.

(Whereupon, at 3:40 p.m., the hearing was adjourned.)

CERTIFICATION

I, LYNNE LIVINGSTON, A Notary Public of the State of Maryland, Baltimore County, do hereby certify that the proceedings contained herein were recorded by me stenographically; that this transcript is a true record of the proceedings.

I further certify that I am not of counsel to any of the parties, nor in any way interested in the outcome of this action.

As witness my hand and notarial seal this _____ day of _____, 2013.

_____

Lynne Livingston

Notary Public

My commission expires: December 10, 2014

A
**a.m** 1:17 4:6
**ABA** 87:9
**abide** 224:16 242:11 267:19
**ability** 74:13 192:13 221:17 230:2 246:12 285:3 290:1 298:18
**able** 102:8 111:21 222:6 261:11 273:7 273:13
**abouts** 55:6 56:9 57:7 63:2 94:10 98:4,12 160:21 163:15 163:17 164:6 168:9,18 193:19
**abroad** 37:12 40:10,20 41:1 41:7,21 49:21 58:15 96:10 148:9 182:21 182:22 236:10 249:2 258:4,16 258:21 259:7 259:19 269:1 276:21 295:12
**absence** 123:19 156:19 262:15
**absent** 122:9
**absolute** 66:21 257:11 297:4
**absolutely** 37:9 67:2 76:18 205:1 248:15 248:16 258:17
**abstracting** 106:17
**absurd** 226:5
**academic** 262:5 290:14 291:2
**academics** 6:17 6:22
**accept** 150:14 174:12 224:14 235:3 245:22 297:9
**accepted** 87:5 216:18 290:3,7 290:9 295:16 295:19 296:18 297:7
**accepting** 166:7 235:20
**access** 76:22 77:10,12,14 83:17 86:5 105:19 119:7 152:9 174:21 176:13 188:1 189:21 190:1,2 190:20 191:22 192:6,10 238:9 238:20 239:3 241:20 275:20 277:12 304:6 308:18 309:1
**accesses** 231:7
**accessing** 190:7 190:11
**accidental** 96:16 96:19 97:1
**Accord** 305:1
**account** 41:10 42:6 43:1 51:5 51:12,17,20 52:2 53:5,6 54:15 55:20,22 56:4,7 60:16 73:21 95:17 101:2 217:16 218:1 272:11 272:16
**accountable** 292:2 307:6
**accounts** 52:12 55:5 221:19 228:2
**accuracy** 73:1 74:15
**accurate** 67:19
**achieve** 228:6
**achievements** 13:10
**acknowledge** 227:11 234:3
**acknowledged** 196:21
**acknowledges** 201:19
**acknowledging** 251:22
**ACLU** 113:13 155:14 156:12 205:1
**ACLU's** 120:22
**acquire** 7:22 38:2 39:3 68:6 122:2,5,18 123:20 133:10 134:15 147:3 152:1,2,3 162:3 189:21 196:2
**acquired** 28:2 32:12 37:4,5 38:21 52:13 79:21 106:5 123:17 134:9 164:22 165:16 165:22 166:4 193:2 196:11 196:13 197:14 197:17,22 199:15,19 201:18,20 229:13 281:18
**acquires** 38:5 152:4 197:19
**acquiring** 151:21
**acquisition** 9:20 17:7 38:8,12 38:15,16 104:17 133:5 133:10 139:17 158:14 165:2 188:8,14,18 189:3 190:15 191:21 192:7 192:11 193:1 196:19 223:6
**act** 1:8 2:11 3:3 5:11,12,16 7:18 29:10 84:17 175:9 235:8
**acting** 214:7 215:4 234:14
**action** 306:16 313:11
**actions** 235:19
**activist** 207:4
**activities** 11:8 11:18 84:13 127:2 131:19 179:4 210:15 217:16 239:17 240:3 241:14 278:16 280:8 282:13 285:8 304:6,13 305:10 312:4
**activity** 19:5 38:10 86:10 105:3,19 115:15,21 118:7 142:3 149:11 156:2 198:14
**actors** 67:22
**acts** 231:9,18 235:14 285:4
**actual** 48:17 118:6 147:17 172:9 201:10 215:22 248:4 285:4
**actuality** 126:18
**add** 13:18 21:16 30:8 31:14 34:13 42:9 43:6 49:12 65:19 77:18 96:4 99:20 103:17 139:13 179:16 181:7 185:18 190:22 195:14 201:17 206:17 208:11 250:14 301:3
**added** 68:19 212:20 213:10
**adding** 30:20 162:11
**addition** 22:3 23:3 85:9,14 136:9 213:1,5 213:6 231:19 232:7 270:4 271:9
**additional** 33:5 35:2 63:2 94:5 136:2 185:18 207:11 228:11 239:10 273:4 278:13
**address** 13:18 15:2 17:2,6,7 18:8 19:16 30:6 51:8 54:18,20 67:12 79:5 83:13 92:18 112:4 116:1 120:6,7

136:19 179:2 197:11 221:1,2 300:13,22
**addressed** 116:3 146:14 231:1 269:5
**addresses** 9:5 10:8 25:12 52:7,10 71:6 88:16 120:2
**addressing** 239:1,21
**adherence** 85:14 282:7
**adjourn** 312:14 312:19,19
**adjourned** 312:22
**adjourning** 312:15
**adjudicated** 226:14
**adjustable** 47:11
**administerial** 310:8
**administration** 159:12,12 211:21 214:16 223:22 230:7 253:22 291:7
**administratio...** 214:3
**administrations** 214:2 229:17
**administrative** 157:4,5
**admit** 310:19
**admittedly** 137:12
**adopted** 213:6 276:11
**advance** 59:19 218:9
**adversarial** 204:12 206:2
**adversaries** 286:8
**adversary** 204:15
**advice** 88:7,18 269:2
**advisor** 210:9 210:10,12 212:3 214:7 234:7
**advocate** 159:13 205:7 222:7,8 237:2,5 277:20 277:22
**advocates** 6:17 6:22 210:17
**affairs** 117:17 127:1,10 279:9 285:12,17,22 286:5 287:13 287:17 288:4 288:19
**affect** 285:17
**affirm** 223:5
**affirmative** 42:11 74:10 114:16
**affords** 243:4
**Afghanistan** 236:15
**afraid** 36:19
**afternoon** 209:6
**age** 198:16 236:7
**agencies** 6:13 19:9 22:9 36:3 36:6 49:6 67:7 78:21 79:3 80:18 105:1 106:12 107:4,5 108:21 118:4 136:6 240:18 242:11 256:14 256:19 257:1 257:15 267:15 268:8
**agency** 2:16 18:3,16 107:14 107:15,16,18 109:6 110:2 122:8,13 240:14 257:21
**agent** 29:7 116:7 141:13,21 149:4,10 150:21 173:22 204:1 207:17 208:7
**agents** 67:21 126:3 149:5 234:14
**aggressive** 131:13
**aggrieved** 165:18,19,21 166:3
**ago** 86:14 145:17 214:5 301:9
**agree** 42:21 64:11 68:17 69:8 90:11 131:21 138:8 138:16 153:22 164:8 169:21 197:12 202:17 206:17 213:17 221:9 245:20 245:21 258:17 263:22 277:3 289:6,10 290:22 291:9 302:1 303:7,9 304:3 306:4,9
**agreed** 5:8 127:13 216:18 232:8 265:13 267:19 296:21 297:1,14,15
**agreeing** 5:2
**agreement** 272:18,20 273:2
**agreements** 111:19 304:16
**ahead** 125:11 149:20,20 250:16
**aim** 228:1,5,6
**aimed** 60:13 220:3 291:14
**aiming** 225:3
**Al** 120:6
**albeit** 243:20
**alien** 8:3
**aliens** 233:3
**allegedly** 238:16
**allied** 252:4
**allies** 282:5
**allocated** 64:20
**allow** 40:13,14 40:15,16 122:8 124:3 151:10 205:8,10 225:8 240:21
**allowed** 30:14 30:19 167:8 200:22 205:2 208:19 240:15 241:3
**allowing** 13:4 26:16 124:16 180:6
**allows** 187:18 187:22 285:22 287:7 288:7
**allude** 98:19
**alluding** 105:17 252:13
**alongside** 183:1
**alphabetically** 209:22
**alternatives** 228:18
**ambiguities** 37:8
**ambiguity** 161:9
**ambit** 59:9 271:3
**ameliorate** 272:5
**Amendment** 10:16 13:1 14:9,12 15:2,7 15:9,13,14,18 16:2,9 17:4 18:1 20:7,10 20:11,12 21:5 21:7,9,11,13 22:5,11,13,19 27:13,19 28:8 28:15 39:4,6 39:15 43:4 74:22 75:19,21 80:13 94:22 116:10 118:1 119:16,22 120:10,16 121:2 129:2,7 129:15 131:5,6 131:20 137:4 137:19,21 138:9,17,18 142:17 144:16 144:19 146:18 148:4 152:20 153:1,4,6,9,11 153:16,17 154:10,13,15 154:19 155:9 156:4,14,21 157:14,18,21 158:1,4,15 160:5 172:21

175:22 180:19 182:9,11 183:2 183:3,4,6,8,19 184:12 185:1,8 185:21 186:5 186:12 190:4 191:18 192:1,4 192:8,17 193:7 200:4 205:3,5
**Amendment's** 126:5 129:17 130:10
**Amendments** 5:12,16 119:18
**American** 3:6 181:13,15 235:6 256:3 311:13
**Americans** 121:4,6 123:18 124:2 131:22 151:21 152:9 159:2,8 170:17 180:21 293:5,6
**amount** 36:5,10 68:5 113:2 208:19 260:20 286:1 308:6
**analogize** 195:3
**analogizing** 14:16
**analyses** 219:13
**analysis** 15:9 20:10,11 21:11 22:5,11,14,19 23:4,8 46:15 75:20,22 77:8 101:17 114:22 120:14 143:17 145:6,7,9 146:19 153:1 154:1 174:15 176:22 185:2 190:5 193:7 194:7 201:14 216:3 235:11 281:2
**analyst** 41:10,11 45:8 59:14 79:14,15 294:2
**analysts** 41:19 42:11 46:9,10 47:1 62:5 74:11 87:14 88:17 111:21 294:12
**analyze** 80:19 142:2 154:8 184:5 194:10 226:19
**analyzed** 275:7
**angrily** 140:19
**annex** 84:18
**anniversary** 219:20
**announced** 4:9
**annual** 8:22 22:7,12,17,20 62:13,15 293:21
**annually** 22:4 22:21 43:2 59:11 112:10
**answer** 37:20 42:3 70:2 135:12 154:4,5 155:4 164:15 169:17 201:8 206:17 228:7 264:12 299:15 305:22 309:5,7
**answered** 36:9 135:16 161:14 310:14,15,17
**answering** 82:22 169:14
**answers** 16:15 92:13 135:17 136:16 161:13
**ante** 42:16 59:19 82:11
**anybody** 40:14 83:6 171:2 196:10 201:7 234:13 244:18 309:21,22
**anymore** 195:13 311:19
**anyway** 62:10 105:20 200:16
**AOL** 191:8
**apartment** 138:1
**apologize** 98:5,9 125:11 147:9 152:17
**apparent** 32:2
**apparently** 80:2
**appear** 8:11 120:21 125:8 134:9
**appears** 135:5
**applaud** 132:7
**Apple** 191:8
**applicability** 137:4 234:4,10 234:16 235:21 243:8 258:4 260:11 261:10 261:17
**applicable** 16:17 234:12 259:13
**application** 206:5,5,6 268:18,22 280:11,21 291:9 293:14 295:10 303:1
**applications** 21:20
**applied** 82:15 183:21 259:22 269:10 286:21 296:16 297:15
**applies** 111:3 129:18 151:13 184:4 185:10 186:12,14 214:10 224:5 225:17 227:16 289:18
**apply** 18:21 26:21 50:21 81:13 87:3 109:17 121:10 129:7 154:11 165:18 176:13 183:19,22 184:2,7 211:17 212:13 213:2 214:4,17 217:2 224:3 225:15 225:21 233:14 244:7,13 245:11 247:6 258:21 259:14 260:2 265:5 278:15 296:4 297:10 310:16
**applying** 236:18 237:14 258:5 259:11 279:21
**appointed** 204:15 257:18
**appreciate** 20:3 27:8 36:10 46:16 113:3 191:15
**approach** 19:18 22:1 65:12 153:1,3 158:5 230:22 279:21
**appropriate** 48:3 86:7 97:3 97:18 217:22 243:4 301:6
**appropriately** 81:10 171:14
**approval** 7:20 14:21,21 20:11 28:17 29:6 156:16 171:12 240:5,12
**approvals** 29:16
**approve** 9:9 49:3 241:4 295:2
**approved** 43:3 48:1 53:11 98:13 112:9,13 150:22 151:5
**approves** 8:22 12:22 59:10
**approving** 173:6
**approximate** 253:17
**arbitrary** 211:4 216:9,12,15,21 243:4 296:16 297:1,22 298:3 298:14
**arcane** 52:5
**area** 71:9 77:22 114:21 116:12 117:6 118:16 119:15 120:9 256:18 259:2 301:15 302:1,5
**areas** 69:14 114:1,4 120:13 172:2 218:17
**arguably** 150:4
**argue** 148:3 195:9 216:11 296:10,19
**argued** 206:12 210:18 225:16 227:8 246:17

**argues** 235:6
**arguing** 202:10 224:1
**argument** 102:16 145:16 161:1,18 163:9 164:5 176:1 210:21 211:7 235:4 238:16 244:21 297:21 303:4
**arguments** 124:20 193:20 193:21 235:20
**arises** 37:16 157:14
**arising** 282:20
**armed** 262:21
**Arnold** 3:15 209:11
**arose** 118:10
**arrangements** 242:1 283:11
**arrest** 256:15
**Article** 142:14 144:6 194:1,4 210:21 211:3,8 212:6 216:8 217:1 231:3,21 233:20 246:12 249:4 261:17 267:7 289:22 303:22 304:4 304:21 305:7
**articulable** 48:19
**articulate** 63:13 95:12 112:7
**articulated** 27:3 30:13,16 40:11 109:2,7 299:14
**articulating** 22:3 82:6
**aside** 73:19 266:22 295:12
**asked** 81:12 223:15 300:5 301:5
**asking** 58:4 111:16 146:6 154:4 168:16 169:4 174:20 230:16 240:19
**asks** 109:14
**aspect** 62:18 116:3 138:17 143:16,16 149:13 221:5 258:3 302:10 302:16
**aspects** 119:6 164:18 237:22 249:16 255:22
**aspirational** 266:22
**Assembly** 236:6
**asserts** 175:19
**assess** 63:13,18 64:6,8 81:2,13 83:1 194:2
**assessing** 63:19
**assessment** 46:7 83:11 126:11 164:12 187:8 242:8
**assessments** 62:14
**assets** 240:16
**assign** 311:11
**assist** 70:21
**assistance** 25:15 26:2 69:21 238:21
**Assistant** 2:19 35:17
**associated** 68:4 120:2,8 123:17 142:16
**association** 299:3
**associations** 125:4 153:15 174:19
**assume** 76:10 77:1 105:19 199:7,7 282:21
**assuming** 195:19 253:14
**assumption** 114:13 177:22 195:9
**assurances** 280:18
**asylum** 307:21
**atrocities** 225:6
**attach** 192:1,8
**attached** 192:4 256:7
**attack** 285:4 286:9
**attempt** 126:15 236:3
**attempted** 64:19
**attempting** 262:11
**attention** 72:10 117:12
**attitude** 258:5 302:22
**attorney** 2:19 7:21 9:1 35:17 85:20 86:12,15 86:18 87:1,5 88:9,20 106:14 118:14 140:15 141:1 151:1 155:14 161:21
**attorneys** 118:19
**audience** 35:11 35:12
**audits** 62:6
**augment** 122:1
**August** 277:8
**Australia** 239:7 240:10,20
**authoritative** 250:18 268:10
**authorities** 158:3 233:7 276:9,15 283:10,12
**authority** 11:1 121:21 122:2,5 122:18 123:20 127:14 130:16 159:16 169:11 171:5 172:3 176:8 182:21 183:13 194:4 194:18 195:16 195:19 202:14 228:10 258:10 281:15 292:3 293:13
**authorization** 84:17 127:18 194:3 198:2 242:13
**authorize** 123:14 161:22 183:17 206:10 238:9
**authorized** 102:3,11 140:16 177:10
**authorizes** 121:11 164:11
**authorizing** 194:15
**automatic** 307:3
**availability** 238:21
**available** 9:21 20:5 26:17 32:2 41:11 47:3 93:12 112:3 198:17 242:1 312:11
**Avenue** 1:16 4:8
**average** 253:7
**avoid** 151:21
**Awang** 5:6
**aware** 11:1 96:13 215:12 215:21 246:4 250:3 264:13 265:2 289:19
**awareness** 69:18 221:12,14
**aye** 4:18,19 312:16,17

**B**

**B** 303:22
**back** 25:2 29:18 30:1,4 44:8 50:14 60:17 71:11 74:18 80:22 92:22 93:5 100:16 112:6 123:15 147:9 153:22 171:16 173:3 175:16 176:16 178:15 180:9 182:3 204:1 207:2,17,19,21 208:9 233:11 260:7 266:2 293:8 299:16 302:12
**back-end** 152:8 173:12 174:7 174:12 175:17
**backbone** 26:7 248:14
**background** 125:21 126:13 194:8

**bad** 55:3,8 60:16 73:10 156:2 167:1 207:2,2
**badge** 219:8
**Baker** 2:13 22:22 32:6 35:12 61:18 67:10 70:2 73:2 82:18 85:7 92:16 105:15 111:1
**balance** 84:8 93:1 105:14
**balanced** 256:19
**balances** 255:12 259:20
**balancing** 155:18 156:3 255:16
**Balkanization** 283:13
**balkanize** 282:12
**ballroom** 4:7
**Baltimore** 313:5
**ban** 130:21
**bank** 153:13 186:15
**bans** 216:8
**bar** 178:21 179:10 180:7
**barred** 226:6,8
**barriers** 34:20 119:3,4
**bars** 89:21
**base** 78:11 106:6 109:16 210:21
**based** 5:21 7:20 10:7 18:13,17 26:10,14 41:7 56:10 57:12 60:7 71:5 73:18 104:22 132:22 149:9 153:6 160:7 170:14 173:15 177:14 219:7 222:12 228:21 230:16 238:14 256:17 258:20 258:22 282:9
**baseline** 101:13 241:17
**basic** 30:11 101:10 109:1 233:13 256:11 258:9,9 304:22
**basically** 43:10 50:11 86:21 87:6 133:11 140:11 156:3 175:17 253:16 265:10 282:4 290:13
**basis** 37:5 61:13 74:12 76:10 78:17 84:1 100:12 107:16 219:9 277:12 277:13
**Bates's** 163:4
**battle** 233:11
**bear** 58:4
**bears** 74:8
**becoming** 139:10 219:9 264:19 302:7 307:4
**beg** 116:19
**began** 238:10
**beginning** 147:10 294:14 311:10
**begun** 63:15
**behalf** 8:11 218:6
**belief** 40:19
**believe** 10:9 14:10 17:17 23:8 51:9 60:15 73:10 80:16 111:10 125:1 129:1 131:4,10,19 133:1,20 141:2 147:1 150:20 154:10 173:8 175:6,8 214:9 221:1 246:5 249:8 250:10 250:12 294:11
**believed** 9:11 37:11 39:20 40:10,20 58:15 71:17 89:9,13 122:14 131:1 136:6 148:11 162:2
**believes** 215:13 250:3 264:14 265:2 289:20 291:10 309:18
**Bellinger** 3:15 209:10 210:1,2 223:20 224:6 244:10 247:8 248:21 249:19 250:1 251:2 252:20 253:2 253:21 264:7 264:11 267:18 288:12,21 296:2 305:4 306:18 307:8 308:3
**belong** 53:12 155:13
**belongs** 52:21 73:10 103:10
**benefit** 35:10,12
**benefits** 219:22
**best** 45:1 93:11 145:15 164:5 196:12 275:16 280:9
**Beth** 34:13 82:22
**better** 25:1 26:7 34:22 255:4,8 255:11,11 260:5 275:9,16 284:2 309:11
**beyond** 59:8 88:13 97:6 131:19 140:11 301:8
**big** 48:5 88:5 109:3 252:1 303:22
**bigger** 40:6 42:10 46:14 258:16 259:19 259:19
**biggest** 205:19
**billions** 219:15
**bind** 286:18
**binding** 213:19 213:22 215:20 217:6 218:2 250:5,12 251:13,15 266:19 267:3 267:15 268:7 268:12,14,17 289:13 290:14 295:21 298:4 305:21 306:20
**binds** 258:9 289:20
**biometric** 154:16
**birth** 302:13
**bit** 20:17 23:19 23:21 24:20 28:19 30:7 39:18 44:12 45:6 61:2 80:3 82:8 89:2 93:6 98:20 104:15 105:7 116:15 147:16 149:2 158:2,8 167:21 171:7,13 185:2 191:1 195:3 204:18 223:13 257:2 266:17 291:16 293:8
**blank** 67:1
**blanket** 60:12
**blessing** 131:15
**blind** 33:21
**blocked** 108:17
**blow** 168:4
**BND** 257:22
**board** 1:3 2:1 4:12,13 5:2 6:8 7:3,5 18:21 36:9 76:22 77:2,10 83:17 87:9 111:11 120:21 125:8 125:13 128:11 132:19 134:22 135:11 136:19 149:22 173:20 174:9 182:10 207:10 209:21 210:4 223:13 231:14 242:7 243:14 312:3,6
**Board's** 4:3 5:3 312:4
**Bob** 8:8 15:5 23:17 25:8 35:14 40:11 48:11 68:19 76:6 105:16 109:7

**Bob's** 101:19
**bodies** 278:6 301:20 308:21
**bodily** 172:17
**body** 64:5 180:6 180:12 221:6 226:13,15 241:4 267:13 267:22 268:5 308:16
**bolster** 222:20
**bomb** 140:1
**bomber** 34:18
**book** 284:21
**books** 19:16 240:1 269:9 307:1
**bootstrapping** 179:20 180:9 180:17 181:8 181:20 199:3
**border** 198:6,7 200:7,10 242:1 300:10
**borders** 211:17 224:5,20 229:20 246:13 248:13 283:8
**bottom** 216:22 229:18
**bound** 212:8 271:14,16,18 286:19 289:10
**box-checking** 203:1
**Brad** 2:19 22:3 27:2 32:10 35:16 39:2 72:6,22 80:8 146:14
**Brad's** 30:20
**Bradford** 5:4
**branch** 20:8 68:20,21 84:4 84:4 85:12 127:21 128:5 140:2,4 142:13 142:14 291:21 292:1,1,4,6 293:11,17
**branch's** 128:14
**branches** 11:5 132:5
**brand** 2:4 4:14 20:2 22:13 23:2,17 24:19 27:6 56:14,19 57:1,2,9,16,21 60:21 61:14 62:21 93:5,19 95:3,9 96:3 97:4,9 145:11 146:5 148:5 149:15,20 179:6 182:6,7 184:7 186:2,10 187:3 266:1,5 267:11,22 268:12,19 269:15 270:17 271:20 295:5,7 298:6,10,20 299:7,10 311:19
**Brand's** 153:22
**Brandeis** 299:16
**Brazil** 220:6,8 239:11
**break** 6:20 113:4 209:2
**breaks** 169:5
**Brennan** 3:10 113:16 140:20
**Brian** 5:5
**brief** 7:6 8:13 21:8 34:13 113:17 132:11 208:11 209:19 223:14 305:4
**briefing** 20:21 21:15
**briefings** 100:4 100:5
**briefly** 39:18 127:3 129:4 132:16 133:2 134:21 186:3
**briefs** 77:21 78:5
**bring** 79:22 142:4 229:9 283:16
**bringing** 304:2
**brings** 11:2 139:14
**Britain** 308:11
**British** 308:8
**broad** 14:20 122:4 125:22 127:22 150:17 151:7 172:4 186:8 194:12 202:2 253:6 255:18 279:6 281:20 285:8 285:18 288:7,7
**broad-based** 68:12 131:15
**broader** 62:2,19 97:12 124:12 130:7 138:20 151:8 159:16 166:11 219:17 230:22 249:9 278:19 282:7 289:17
**broadly** 15:1 68:15 122:16 158:20 208:3
**brought** 141:9 141:18
**Brownell** 140:3
**Budapest** 232:9
**budget** 64:21
**build** 51:3 170:12 220:18 292:9
**building** 54:12
**built** 80:10 114:13 124:14
**built-in** 300:19
**bulk** 10:6,6,12 23:18,19,22 24:2,6,17 48:8 71:6 157:7,9 157:11 158:8 158:10,11,14 158:14 189:12 190:11,14,18 197:6 200:1,3 229:12
**bunch** 24:11
**burden** 48:15 114:7,9 176:16 177:19
**burdensome** 30:4
**bureau** 2:13 30:10
**Bush** 159:12 214:1
**business** 230:5 272:3,22 275:5 284:9
**bypassing** 180:5
**Byron** 140:10

**C**

**C** 3:16
**call** 4:16 90:6 138:2 159:6 163:18 174:17 177:9 189:1,2 189:12 197:6,7
**called** 61:6 118:2 124:15 155:14 210:22 252:5 257:19
**calling** 103:10 103:15 220:12
**calls** 46:2 47:22 124:16 156:11 190:15,19,20 191:21
**camp** 225:9
**Canada** 239:7 240:10,21
**candidate** 75:6
**candidates** 75:8
**candidly** 215:16
**capabilities** 67:20
**capable** 124:15 150:11
**capacity** 279:17 279:18
**capita** 277:11,13
**capture** 201:1
**card** 153:13
**care** 85:15 168:5 168:12
**careful** 203:7 254:9,16
**carefully** 11:17 203:4 205:8,9
**carrying** 284:9
**carve** 33:7
**case** 23:12 29:12 39:14 48:3 55:2 60:6 64:17 74:3 77:8 79:16 115:11 116:6,8 137:22 139:22 140:10 141:9 141:14 144:16 147:8 149:10 155:19,21 157:4 196:12 197:21 198:4

198:21 204:19 225:2,18 226:15 227:5 234:1 237:19 249:8 262:22 263:14 269:5 278:18 290:6 294:7 304:14
**cases** 6:7 17:18 43:11 73:19,19 74:6 77:21 137:20 139:19 142:7 143:1 150:2,9,18,19 150:19 160:4,5 160:6 184:12 184:15 185:7 186:21,22 198:6,8,15 199:13,16 200:7,8,10,12 205:12,13,21 206:1 235:17 249:11 302:16 304:4,15
**catch** 227:8
**categories** 9:2 81:8
**category** 32:9 32:20 105:6 207:6 285:20 288:19
**cause** 116:5 118:6 124:7 141:11,20 150:20 155:19 156:9 157:19 160:8 172:10 172:16 173:1,8 173:16,17,19 174:3,5 180:8 193:6 227:22
**caution** 149:22
**cede** 100:15
290:22
**celebrating** 219:19
**cell** 73:10,13
**Center** 3:10 113:16
**central** 114:1
**centralized** 106:14 107:2
**CEO** 3:16 209:12
**certain** 66:19 85:11 95:19 102:7 104:2 106:7 134:5 177:17 195:13 216:4 233:8,13 236:19 237:14 238:12 239:15 245:20 257:12 306:22
**certainly** 44:14 83:9,14 102:7 112:6 118:12 126:19 135:6 135:14 137:6 186:18 190:13 192:2 196:16 197:18 203:16 216:11 217:9 246:2 247:8 250:1,9 251:9 254:22 264:18 284:16 287:4 290:7
**certainty** 200:1
**certification** 22:7,8,18 62:15 313:1
**certifications** 8:22 9:7 59:10 59:11 279:12 294:22
**certify** 313:6,9
**chair** 21:5
**chair's** 26:21
**chairman** 2:3 4:5,11 238:2,3 269:17
**challenged** 77:19
**challenges** 185:4 218:20 287:1,1
**chance** 35:9 45:9 132:12 142:20 160:15 182:17 266:1 284:5,22 305:2
**change** 23:6 157:16 158:2,9 205:14 213:7 230:9 245:7,10 251:16 279:3
**changed** 76:11 144:9,10 229:16 257:2
**changes** 79:19 139:11 157:12 201:5 230:8
**changing** 137:18 220:3 303:17
**characterized** 167:7
**charge** 92:22
**charges** 141:18 142:5
**charities** 153:15
**Charter** 231:4 264:20 265:1 265:15,16 290:16 304:21 305:11
**Charter's** 264:14 305:7
**chats** 191:9
**chatting** 171:21
**cheapest** 228:22
**check** 114:17 178:5,8,9 259:16
**checked** 259:8
**checking** 41:17
**checks** 62:8 255:12,15
**Chicago** 73:12
**chief** 127:10 140:14
**choose** 6:5
**Chris** 209:18 254:22 298:6 299:14
**Christopher** 3:22 274:1
**CIA** 18:4,15 78:22 119:7,9 119:10 140:1
**circuit** 130:4
**circuits** 15:22
**circular** 105:8 105:12
**circumscribed** 115:2
**circumstance** 23:9 88:19 178:17
**circumstances** 41:8 42:5 85:11 94:16 106:8,11 107:13 111:17 112:7 126:22 178:12 186:18 236:13 258:15
**cited** 255:1 277:10
**citing** 147:5
**citizen** 8:3 128:9 130:2 131:8 138:2 278:4
**citizen's** 125:4
**citizens** 126:9
129:7,12,13,19 183:22 184:2 215:18 230:3 230:20 232:19 233:5,6 236:22 259:2 277:20 278:4
**civil** 1:3 3:7 4:3 93:2 211:1 218:10 222:7,8 223:17 233:21 255:16 267:8 286:14
**claim** 165:21 304:8
**claimed** 127:21 128:6
**claiming** 121:20 145:1
**claims** 127:4 238:11 239:1 275:18
**clandestine** 285:7
**clarified** 185:7
**clarify** 30:14 78:20 183:10 202:10,11 306:14
**clarifying** 57:5
**clarity** 40:12 194:22
**class** 133:15
**classic** 137:21 144:16
**classified** 6:2,3 6:7 13:11 84:18 85:3 135:9
**clause** 100:12 152:11 224:7 224:12 248:9 270:12
**clauses** 69:3

**clear** 11:16 12:8 14:2 36:13 37:9 39:2 49:15 69:16 90:11 129:6 133:22 152:21 155:1 179:11 213:1,11 225:12 275:2 279:3 289:3 301:16 302:5 303:12,19 304:17
**clearer** 274:2
**clearly** 139:18 163:21 177:8 196:5 264:13 266:16 270:19 271:1 305:22
**Cleveland** 252:6
**client** 86:12,15 86:18,19 87:1 87:6 88:20 118:14
**clients** 87:7
**Clinton** 211:20 214:2
**close** 13:7 154:14 192:21 216:2 217:4 282:5
**closed** 206:13
**closely** 81:5
**closer** 206:4 229:11 261:2
**cloud** 238:12,14 239:2,4 275:19
**clouds** 220:13 237:7 238:17 242:4
**co-approach** 243:12
**co-existent** 91:3
**code** 71:9
**colleague** 30:9 215:10
**colleagues** 13:17 29:1 36:3 54:4 68:9 100:14
**collect** 8:18 16:3 16:10 26:16 29:13,21 38:2 39:3 51:10 53:5 59:2 60:4 80:18 147:22 148:11,16 159:17,17 167:9 180:20 189:21 196:2 242:2 246:13 254:14 256:16 294:18
**collected** 9:3 13:3,5 15:12 16:20 17:11 19:12,19 27:16 28:5 29:9,15 29:19 30:21,22 31:3 32:15,17 37:14 38:21 43:18 72:19 95:5 100:20 101:2 102:20 106:20 133:20 134:6 136:15 146:4,6 163:6 170:10 176:8 176:18 177:14 179:12,19,21 180:3,7,12 199:18 200:3 243:19,20 245:6 254:3,7 254:15 269:11 308:18 309:1,2
**collecting** 13:13 51:15,19 58:19 73:14 85:22 89:4 94:13 95:20 142:12 159:21 161:5 162:10,18 167:19 177:17 181:10 198:22 288:18 302:14 303:11
**collection** 7:14 10:6,6,7,12 11:2,4,8 12:5 12:10,14 13:9 14:1,13,20,22 15:3,5,17 16:7 16:18 17:4,22 21:3,12,18 23:18,20 24:3 24:7,7,9,17,17 25:4,5,7,16,20 25:22 26:4,5,6 26:6,12,14,15 26:18,20 27:2 27:14,22 29:3 29:4,5 30:13 30:15 31:17 32:22 33:22 36:22 37:1,9 37:22 38:8,12 38:15,16 40:17 42:16 47:8,12 47:13,16 48:8 48:9 49:14,20 53:6 54:11 55:6 56:5 57:5 57:6,7,11,19 57:20 58:17 59:5,7 60:12 63:3,6,8 64:12 64:14 65:1,4 65:15,18 66:14 66:15 67:18 68:13 70:14 71:4,7 77:18 81:4 82:3,7,13 86:14 88:8 93:6,8,9,16,21 93:22 94:3 95:16 96:6,8 97:1 98:11 100:18 101:8 101:18 102:2 102:10 103:19 109:2,7 132:21 133:4,21 134:3 134:17,19 145:18,20 146:1,10 148:4 148:8,19 150:11 157:7 157:11 158:14 159:6,8 160:10 161:4 162:22 163:7 170:8,17 170:22 177:11 178:1 186:13 186:14 187:6 188:4,8,12,15 188:16 189:2 189:13 190:18 196:19 197:6 199:8,10,11,12 200:2 208:15 208:16,20 227:2 228:17 229:10,12,14 236:14 245:8 248:14 262:11 262:12 274:9 274:15 282:12 286:1 287:13
**collections** 30:18 54:14 56:8 59:17 94:10 137:5,8 157:9
**collects** 38:4
**Collins** 2:7 4:14 27:7 28:13 35:5 63:1,5,9 67:5 97:11 98:3,15,18 100:13 111:13 116:14,22 152:13 155:3 155:10,12 156:6,17 157:1 157:15 189:18 191:14 192:5 192:12,19 193:16 207:12 207:15 260:14 261:8 264:6 288:12 291:12 292:19 293:7 294:4,15 311:8
**collision** 143:19
**colloquial** 38:4
**combed** 166:12
**come** 25:19 33:3 34:11 41:3 65:3 99:14 118:3 136:17 160:16 169:1 176:16 184:1 198:6 221:18 226:22 260:7 260:12,16 263:10 266:2 278:8 298:12 310:1
**comes** 32:14,16 72:9 181:5 227:11 280:19 299:5
**comfort** 94:21 272:21
**coming** 27:7 126:14 152:14 182:19 183:15 194:10 204:19 207:2 258:15 258:16 259:18

260:15 261:15 286:22 299:1 311:9,21
**commencing** 1:17
**commend** 242:7
**comment** 14:16 40:5 63:22 82:18 83:14 86:3 111:1 195:22 196:3,8 196:15 234:2 249:20 276:16 307:16
**commented** 87:9 307:12
**comments** 7:10 19:15 32:7 132:12,13 182:16,17 210:5 272:18 307:9,13 312:8 312:10,11
**Commerce** 277:9
**commercial** 300:10
**commercializ...** 219:20
**commission** 172:8 257:17 257:18,22 313:17
**commission's** 172:15
**commissioners** 276:21
**commissions** 34:16,19 35:4
**commit** 155:20 172:17,18
**commitment** 310:20
**commitments** 267:20
**committed** 76:14 136:8 155:20 231:19 235:16
**committee** 211:22 212:4 213:9,16 214:7 214:8,22 215:5 226:12 234:1 244:22 249:21 250:4,6,18,22 268:10 290:11 290:13 304:17 307:9
**Committee's** 213:19
**committees** 84:11 98:21 99:11,18 100:3 100:6,9
**committing** 155:20
**common** 257:12
**commonly** 10:5 29:10
**communicate** 298:19
**communicating** 92:9
**communication** 7:15 12:12 25:15 50:9 52:10 87:21,22 90:14 91:20 94:13 95:5,20 103:16 108:14 108:18 120:4 123:8,12 134:16 138:13 138:14 139:12 175:8 197:3,8 221:3 288:8
**communicatio...** 9:14 12:2,10 12:17,19 13:3 14:8 15:11 19:17 24:7,12 25:22 26:17 37:4 40:17 51:19 52:14 54:16 55:5,7 55:16 73:15 82:8 86:15,18 87:3 91:9 92:3 92:7 94:14 95:22 101:3 115:14,18 118:19,22 119:1 121:5,5 122:3,6,12,14 122:19,21 123:6,16,21 124:1,4 125:5 131:9 132:1 133:4,13,19 134:5,7 135:20 136:5 137:11 138:6 144:10 144:11 148:1,2 151:21 152:4,7 152:9 155:16 159:17,22 161:4 162:10 163:6 164:1,21 165:16,22 166:4 167:9 170:18 174:19 175:11 180:20 188:17 189:10 189:11,12 190:3 192:6,14 195:6 197:14 199:1 201:18 201:18 226:3 227:13 229:22 234:19 271:6 287:8 293:5
**community** 46:19 64:21 99:15 241:11
**compact** 265:11
**companies** 53:18 70:5 218:7 221:16 228:17 240:20 272:10 273:7 273:13 282:9 282:10 283:2 300:22
**company** 52:1 53:10,14,21 69:21 70:8,16 107:1 272:14
**comparative** 237:21
**compare** 257:14
**compared** 184:4
**compatibility** 241:13
**competing** 282:10,17
**competition** 241:15
**competitiveness** 283:1
**complementary** 66:3
**complete** 130:21 302:11 304:2 312:5
**completely** 12:8 64:10 69:8 129:14 172:4 195:5 291:3
**complexity** 34:2
**compliance** 11:12,19 23:10 62:7,12 72:13 73:7,16 94:21 152:10 212:1 250:7 251:12 306:22 307:7,9
**complicated** 97:14
**complies** 21:4 132:21
**comply** 21:6 53:19,22 290:17,19
**comprehensive** 62:7
**compromise** 131:12 132:4
**compulsory** 25:13 70:15
**computer** 12:19 147:18 197:15 226:9 231:8 294:2
**computers** 198:7,9
**concede** 277:18
**concentrate** 233:20
**concentration** 225:9
**concept** 167:11 236:4 309:14
**concepts** 102:1 189:16 196:6 218:12
**concern** 18:9 36:18 45:13 92:19 94:2 95:17 118:16 119:22 120:9 157:17 181:5 205:19 269:22 282:18 291:17
**concerned** 114:4 114:22 199:13 254:6
**concerning** 63:11
**concerns** 14:10

15:2 23:11 94:5 114:2 118:1,11 119:16 120:16 152:20 153:5,7 153:9,11,16,19 200:4 217:11 236:18 239:22 254:17 272:11 282:17
**concise** 309:6
**conclude** 128:17 130:20 131:10 166:1
**concluded** 16:5 53:11 55:9 60:3 127:12
**concluding** 151:12 166:2
**conclusion** 29:21 55:2 120:12 164:14 166:5 276:2 302:20
**conclusions** 235:3
**conclusively** 178:20
**concrete** 103:9 189:7
**condemn** 132:7
**conditions** 212:14
**conduct** 12:15 22:11 121:3 123:15 124:4 126:1,16 127:1 127:8,14 128:1 128:6,14 131:13 182:21 183:13 195:17 216:5 240:15 246:6 270:9 275:12 277:4 285:12 290:1 305:9
**conducted** 21:19 25:14 37:19 62:19 75:22 129:21 130:3 139:1 179:4 282:13
**conducting** 20:9 29:11 75:19 130:12,14 134:16 168:22 262:6 277:1
**confers** 229:20
**confess** 261:15
**confidence** 42:10 292:9
**confine** 113:22
**confirm** 6:9 114:12
**confirmed** 129:9 129:16 134:12 214:2
**confirms** 212:18
**conflate** 49:16
**conflated** 133:21
**conflating** 162:12
**conflation** 182:14
**conflict** 140:21 262:21 264:1
**conflicting** 264:4
**conflicts** 260:1
**conform** 109:21
**confused** 147:16 171:8,13 191:2
**congratulate** 260:15
**Congress** 5:9 11:14 12:9 62:13 68:22 69:6 72:16 83:22 85:10 98:16 100:7,11 131:14,18 164:15,19 166:16 177:8 180:1 185:19 293:18 294:9 307:2 308:20
**congressional** 84:10
**connect** 46:20
**connected** 299:2
**Connecticut** 1:16 4:8
**connection** 33:18 100:3
**Conrad** 212:3 212:11 213:9
**consensus** 220:21
**consent** 4:21 312:19
**consequence** 77:5 94:18
**consider** 27:18 92:10 144:15 171:2 255:22
**considerably** 48:22
**consideration** 252:11
**considerations** 232:5
**considered** 19:17 69:12 75:16 140:15 141:6 145:8 216:6 251:14
**considering** 127:11 241:22 263:5,7
**consist** 6:12,16 6:21
**consistent** 9:19 12:22 22:15 43:4 74:21 86:7 104:19 128:20 169:13 211:16 214:12
**Consistently** 34:19
**conspiring** 140:1
**constitutes** 216:12 269:19
**constitution** 10:16 126:1,20 127:7,11 169:13 183:15 198:21 258:4
**constitutional** 5:18 6:18 11:1 71:12 74:18 82:14 109:20 109:22 114:2 125:14 126:10 127:4,14 128:1 128:6 131:17 136:10 137:14 194:2,8 197:9 197:11 235:5 237:19 256:7 258:6,21 260:1 263:20
**constitutional...** 75:16 76:4 78:3 121:19 170:14,21
**constitutionally** 194:11 256:21
**constrained** 256:20 274:17
**constraints** 128:13,18,19 128:19,22 183:7
**construction** 118:2,13
**consult** 88:17
**consulting** 87:7
**consumption** 106:10
**contain** 122:15 134:8 136:7
**contained** 313:6
**contemplate** 165:14
**contemplated** 80:5 163:22 164:15 166:8
**contemplates** 165:20
**contemplating** 164:20 166:17
**contend** 242:4
**content** 48:12 49:18,20 115:17 118:20 133:12,13 141:22 147:21 148:2
**contents** 155:15 165:3
**context** 39:13 46:17 47:2 48:15,16 50:21 62:2,19 65:22 83:20 86:19 88:16,21,22 96:15 107:9 118:20 138:19 146:15 154:19 154:21 156:5 158:17 160:5 165:19 179:4 197:18,20,21 206:7 225:1,2 225:20 226:5 252:12,18 270:14 293:3 295:14 298:11

307:17 308:2
**contexts** 12:15 28:10 29:13 105:9,13 124:6 160:6 308:2
**continue** 20:6 50:6 110:14 195:11,18,18 224:2 252:2
**continued** 289:2
**continues** 118:16 184:18 214:9
**continuing** 131:13 220:10 232:11
**contours** 236:3 261:2,9
**contracting** 213:4
**contradict** 266:4
**contrary** 35:3 41:12 122:9 133:22 134:19 166:18 178:7
**contrast** 19:2
**contributes** 74:13,15
**contributions** 134:22
**control** 192:8 215:3,3,8 224:14 225:19 226:1 227:13 232:19 234:13 234:18,18,22 241:9 244:16 244:20 245:4 245:14 246:21 256:18 257:15 269:19,21 270:19 271:7 296:8,11,12 297:16 308:10
**controlled** 246:8
**controlling** 15:7 249:15 259:6
**controls** 239:17 241:20 255:12 255:16 275:22
**controversial** 175:10,11
**controversially** 232:14
**controversy** 36:18
**convention** 231:21 232:9 246:16,17 249:5 251:6,20 260:10 303:21 304:3,5,9,16 308:5,7
**conventional** 159:7
**conventions** 234:10
**conversation** 98:9 124:21 189:20 288:14
**conversations** 14:4 124:17 142:1 156:13 279:7
**converse** 247:14
**convey** 108:15
**conviction** 263:2
**convincingly** 234:9
**Cook** 2:7 4:14 27:7 28:13 35:5 63:1,5,9 67:5 97:11 98:3,15,18 100:13 111:13 116:14,22 152:12,13 155:3,10,12 156:6,17 157:1 157:15 189:17 189:18 191:14 192:5,12,19 193:16 207:12 207:15 260:6 260:14 261:8 264:6 288:12 291:12 292:19 293:7 294:4,15 311:8
**Cook's** 82:22 93:3
**cooperation** 132:4
**copies** 231:7
**copying** 174:17
**core** 301:22 302:5
**corners** 283:8
**correct** 37:6,7 39:11 41:13 42:3 44:20 46:12 56:2 63:7 70:1,11 71:3,10,10 75:4 101:14 204:7 274:20
**correctly** 79:18 101:1 179:17 261:20
**correspondence** 120:4 211:6 298:16 299:4
**costs** 34:7 68:4
**Council** 3:17 209:13 210:11
**counsel** 2:13,15 2:17 3:9 35:13 35:14,15 87:15 88:17 113:15 119:8 277:9 313:10
**counselor** 252:16
**count** 38:15
**counterparts** 240:10 242:10
**counterterror...** 5:10 59:12 68:14,16 69:12 69:15 83:18
**countries** 71:3 128:7 213:17 214:20 228:16 229:3 230:2 232:15 233:8 241:21 244:8 250:10 254:22 258:17 265:11 265:12 269:8 274:5 275:11 276:22 277:2 277:19 278:18 282:5,6,11 283:4 284:10 285:16 286:7 289:12,17 290:3,18 291:19 292:9 301:18,19 303:16 304:6 305:17 306:2,4 306:9 309:15
**country** 11:2 123:12 138:4 191:22 213:21 229:2 235:11 255:7,11 258:11,12 261:22,22 262:7,10,16 264:13,17,21 265:2,19 268:20 283:8 289:19 291:10 296:20 297:5 297:14 303:12 304:19 305:6 306:8
**country's** 124:16 265:20 275:8 276:17 277:20 284:1 286:11
**country-specific** 220:13
**County** 313:5
**couple** 10:2 27:11 30:8 32:7 33:3 63:17 86:13 88:5 207:9 244:11 249:10 274:7 284:20 284:21
**course** 74:15 81:18 132:11 132:19 134:12 134:16 136:15 180:1 258:13 283:10 301:21 302:8 304:7
**court** 7:16,19 8:21 9:8 11:13 11:14,17,20 12:22 14:18,21 15:8,15 16:12 18:14 20:9,13 20:17,18 21:3 21:9 22:4,15 22:18 23:12,12 28:17 29:6,16 29:18 30:1 43:3 44:22 45:4 48:1 49:2 49:7 55:9 74:19 75:13,15 75:17 76:3,15 83:8 94:8,17 94:20 98:13 112:14 115:16

116:2,16 127:11,16 129:9,22 139:21 140:2,4 141:4,6,10,16 142:6,8,9 151:5 167:6 171:12 173:4 186:9 204:19 205:4 206:5,12 207:8 222:9 226:17 233:22 235:5,6 240:5 240:12 246:15 249:11 256:7 257:19 259:6 259:18 260:1 263:20 274:12 294:9,22 310:4
**court's** 20:10 76:9
**court-approved** 86:8
**courtroom** 142:4
**courts** 15:14,21 17:21 85:10 118:2 121:14 126:7 127:21 129:16 130:4,9 132:1 138:21 139:18 150:3 150:10,12 154:13 184:1 186:18 199:13 234:3 236:12 307:22
**covenant** 211:1 213:2 214:10 223:16 224:7 224:11,17,18 233:21 248:1 250:19 267:8 271:11,12 286:13
**covenant's** 214:13
**cover** 165:5
**covered** 10:20
**covers** 118:9
**create** 33:11,21 118:5 183:3 217:5 220:7,14 233:16 247:14 302:11
**created** 139:4,9
**creates** 183:6 226:5 308:8
**creating** 32:9,20 174:18 301:11
**creation** 174:22
**credibility** 42:7
**credible** 244:21
**credit** 153:13
**crime** 17:16 19:6 29:12 32:2 108:1,2 109:4 136:7,13 148:16 155:21 172:18 232:7 303:21 304:3,4 304:9,15
**crimes** 257:6
**criminal** 3:21 12:15 19:5 29:8 77:19 86:20,21 88:11 88:13,16,19,22 115:10,15,21 115:21 117:22 118:7 141:18 142:3,4,15 144:4 145:3 146:10 148:7 148:20 149:5 149:11 174:4 176:9 181:2 198:14 201:13 205:16 209:17 210:13 297:19
**criminality** 149:12,13
**criteria** 49:8 78:9,12 81:20 107:6 109:11 275:10 278:9
**criterias** 106:13
**critical** 112:11 261:12
**critically** 221:4
**criticizing** 239:15
**critics** 126:16 276:15
**cross** 241:22 300:9
**cross-border** 238:22 300:18
**crucial** 206:20 207:5
**cruelties** 256:9
**CT** 83:20
**current** 74:14
**currently** 84:12 178:1
**curtain** 203:10
**custody** 28:9,12 30:3,6 271:2 296:14
**customary** 231:16 262:1 262:14 263:1 289:11 304:22
**customer** 228:18
**customs** 198:10
**cut** 269:15
**cyber** 53:13 60:19 108:10 108:10 223:2 232:7 303:21 304:2,4,9,15
**cycle** 46:2
**cynical** 278:12

**D**

**D.C** 1:17 4:8
**dangerous** 170:12
**dangers** 259:18 259:19
**data** 31:9 34:10 37:17,20 38:14 45:2 47:7 58:9 70:19 79:21 95:18 115:11 117:7,20 120:15 172:11 172:22 189:3,4 189:5 196:11 196:13 198:16 220:7 223:6 228:17,18,21 229:2,5,10,11 229:13,19 230:3,3 231:8 231:9 233:8 235:10 236:14 238:9,13,20 240:20 241:1,5 241:20 248:12 269:11 273:8 276:14 283:7 283:13 300:10 300:14,18 302:15 303:11 308:18 309:2
**databank** 47:22
**database** 37:4 38:5 39:10 48:4,22 175:1 199:21 200:2 201:2
**databases** 62:6 86:5 114:17 119:7 123:22 178:9,9 192:3 201:14
**datas** 257:12
**dating** 233:11
**David** 2:3 4:5 311:17
**David's** 58:1 97:12
**day** 42:18 62:8 260:21 261:6 309:13 313:13
**days** 36:1 59:22 61:20 181:12 214:5
**De** 2:15 22:2,15 23:5 25:2 30:8 35:13 37:7 38:11 39:5,11 40:6 44:8,14 44:20 45:18,21 46:7,12 49:12 54:5 56:3,22 57:3,11,17 58:20 62:1 63:4,7 65:19 68:17 70:12,20 71:4,10 72:6 74:8 76:20 78:18 79:2,14 82:2 83:13 87:8 88:13 90:7,18 93:11 94:7 95:7,11 97:5 98:1,14 98:17 99:20 103:17 106:16 108:1 109:1,18 110:5,10,14,21 112:2 178:11
**de-task** 73:13
**de-tasked** 73:3
**deadline** 312:10
**deal** 222:4 235:4
**dealing** 235:18

259:10 307:20
**dealings** 272:4
**deals** 49:17,18 49:22 252:8
**dealt** 249:3 300:16
**Dean** 3:16 209:11 301:3
**debate** 70:4 77:13 224:4 252:1 273:18 276:18
**debated** 220:6
**decade** 34:14,15
**deceiving** 283:6
**December** 236:6 313:17
**decide** 107:6 110:2 111:21 275:16
**decided** 74:4
**decides** 78:11
**decision** 44:5 45:7 78:9,15 110:13 129:10 140:11 259:6 259:17
**decisions** 61:21 62:17 77:22 79:1 217:13 226:20 290:12 290:20 294:12 294:16 307:19
**decisive** 235:2
**declaration** 300:12
**declassification** 75:6,8,12
**declassified** 5:22 11:16 76:16 93:13 134:14
**declassifying** 292:13
**decoupling** 300:8
**dedicated** 36:11
**dedication** 36:6
**deepening** 235:15
**deeper** 236:1
**deeply** 36:4 99:16
**default** 46:3 47:5,6,8 96:2 202:10
**defendants** 77:19
**defending** 167:5
**defends** 158:22
**Defense** 188:11
**defenses** 159:1
**defer** 72:6
**deference** 249:6
**deficiencies** 241:19
**define** 143:9 236:3
**defined** 117:13 117:15 122:16 161:12 215:1 299:5,13
**defines** 212:7 216:19
**definitely** 37:7 68:17 97:22 156:9 258:22 279:20
**definition** 24:5 82:3,12 87:5 96:7,11,12 104:14 105:8 165:1,10,17 173:21 196:1 279:5 282:7 285:1 286:5 289:9,17 295:16,19,20 295:22 296:22 297:1,7 298:3 298:11,12,21 299:7,14 301:17 302:18
**definitions** 50:15 173:22 296:18 297:2 301:20
**definitive** 250:11
**degree** 80:9 185:1 194:14 242:13 261:1,4 261:9 269:8
**degrees** 6:13
**delay** 33:4,9
**delegation** 212:21
**delete** 104:9,11
**deleted** 101:8,13 108:16
**delve** 23:19
**delving** 36:4
**democracies** 240:3 255:2
**democracy** 175:12
**democratic** 125:1 221:8 237:6
**democratically** 292:2
**demonstrate** 302:14
**Dempsey** 2:6 4:14 35:20 38:1,22 39:8 39:14,18 69:16 70:4,18 71:1,8 71:11 74:17 75:5,9,15 77:14 100:16 101:15 102:5 102:15,21 103:3 104:4 105:7 160:18 162:16 163:13 164:4,17 165:4 165:9 195:21 195:22 197:10 197:13 199:5 199:17 200:6 200:11 254:19 254:20 255:10 255:20 260:7 283:18,22 284:19 286:4 286:15 287:12 287:19 288:5,9 309:8
**Dempsey's** 176:22
**denied** 205:4
**deny** 226:12
**Department** 2:20 11:9 35:18 42:19 59:20 61:13 62:9 167:7 210:9,13 234:7 252:17 272:19 273:3 277:10
**Department's** 188:11
**depend** 64:15 190:7
**depending** 105:2,5 143:9
**depends** 66:7
**deprived** 233:6
**deprives** 232:19
**Deputy** 2:19 3:6 35:16 113:12
**derivative** 109:20
**derived** 65:14
**describe** 153:3
**described** 30:15
**describing** 158:18
**description** 108:21 187:13
**designations** 200:21
**designed** 13:2 16:22 17:10 60:11 104:16
**desirability/n...** 204:12
**desire** 191:15
**desk** 294:3
**despite** 216:22 252:2 257:12 282:6
**destroy** 122:11 152:4
**destroyed** 201:21
**destruction** 59:13 201:17 201:22 285:7
**detached** 141:3
**detail** 11:7 25:10 87:11 120:13 159:5 241:16 272:21 273:6
**detailed** 95:15 281:2
**details** 112:5 130:8 237:21 292:21
**detained** 270:18 270:20
**detainees** 307:21
**detention** 225:20 270:14 270:17
**determination** 14:19 40:8

41:4,5,15 42:11,13,18,21 45:22 47:1 48:19 58:22 59:15 61:12,22 71:16 73:17 74:7,9,12,14 74:16 156:9 163:1,10,17 192:22 193:6 242:15
**determinations** 42:15 43:8,13 52:18
**determine** 42:20 46:17 64:20 74:20 76:15 88:1 102:13 140:6 178:20 267:1 288:17
**determined** 44:9 44:15 65:6 74:19 75:1 162:17
**develop** 301:21
**developed** 222:21 236:11
**developing** 68:2 222:9
**device** 189:9
**dialogue** 27:9 301:8,12 305:15,16
**Diane** 5:5
**difference** 48:5 48:7 101:21 182:2 192:10 279:15
**differences** 19:8 238:8 256:2,11 258:13 280:13 280:14
**different** 15:22 18:16,17 19:3 25:3 26:20 27:2,3,4 30:16 30:18 34:9 38:18 50:8 55:6,18 57:20 58:3 66:8,9,10 68:8 73:6 86:12 102:1 103:22 104:7 104:12,21 105:2,4,8,9,12 105:13 106:12 106:13 107:5 125:10 132:4,5 138:14 139:16 144:13,15 146:5 154:8 160:6,10 162:13 176:4 180:10,15 182:5 188:6 192:20 199:12 224:1 230:16 233:7 236:10 236:13,13 258:14,18 259:1 263:10 277:18 280:18 301:18 305:17 309:15,16,17 309:19
**differentiation** 257:7
**differentiations** 236:16
**differently** 20:17 34:4 175:9 268:3
**difficult** 30:4 46:16 125:1 302:8
**difficulty** 137:17
**dig** 99:15 178:15
**digital** 236:7
**dignity** 217:17 259:2
**diligence** 114:16
**diminishing** 219:6,7 225:5
**Diplomatic** 231:22
**direct** 79:19 105:22 117:12
**directed** 49:20 80:21 110:16 168:11,14 295:8
**directing** 66:18
**direction** 256:10
**directions** 66:19 84:20
**directive** 24:5 47:20 50:18 54:8 79:18 217:15 229:9 237:13 252:14
**directives** 7:20 26:3 53:16,17
**directly** 35:3 97:19 302:3
**Director** 2:18 3:6,20 7:21 9:1 11:10 35:15 42:20 59:21 64:18 85:20,21 113:13 161:22 209:15
**Disabilities** 251:7,20
**disaggregation** 273:8
**disagree** 76:18 127:5 223:19
**disagreed** 223:21
**disagreement** 245:17
**disallow** 307:20
**disclose** 111:7,7 241:1
**disclosed** 111:10 269:7
**disclosure** 84:9 197:21
**disclosures** 218:18 219:1 238:11 272:14
**discourse** 157:13,17
**discover** 71:18 71:22,22 101:5 101:6
**discovery** 66:13
**discriminant** 24:8 274:9
**discriminators** 147:20
**discuss** 95:16 121:12 166:18 166:19,21 200:19
**discussed** 58:5 94:11
**discussing** 6:8 37:13,18 38:19 54:17 55:21 57:6 113:2 155:15 190:17
**discussion** 5:18 5:21 6:1,4 14:1 20:7 36:18 50:7,12 58:9 58:21 113:21 209:2 235:6 236:1,8 237:3 237:22 243:17 260:18 266:9 284:12 300:3,7 301:10 305:14
**discussions** 55:21 166:13 273:17 311:11
**disinclination** 33:13
**disinterested** 140:5 141:3 155:22
**disparate** 46:21
**disposal** 31:11
**dispute** 127:6,22 158:12 232:15
**disseminate** 17:13 31:21 80:19 104:1,10 107:19
**disseminated** 81:10 106:6 110:7
**disseminating** 110:11
**dissemination** 9:22 17:8 81:5 103:20 104:17 111:17 117:7 117:21 120:15 174:14 229:10
**distances** 260:17
**distinction** 14:17 38:7 50:1 94:1 137:14 139:3 145:18 146:9 148:6 158:7 187:16 188:7,9 188:13 196:18 196:18 219:3 266:16
**distinctions** 196:2
**distinguish** 73:6 266:10
**distinguishing** 281:17
**District** 139:21 142:9

**diverse** 264:3
**diverts** 189:9
**division** 2:20 35:18 139:10 210:13
**DNI** 62:10 85:20 99:16 110:16
**doctrine** 179:7 200:10
**document** 59:17 59:19 61:5 62:5 76:2 267:14
**documentation** 42:17 60:22
**documented** 42:16 59:18
**documenting** 61:8
**documents** 6:2,5 6:10 11:15 75:11,14 119:2 119:10 147:17 178:8 188:2,9 292:14 310:14
**doing** 28:17 86:9 89:22 96:21 150:13 162:9,10 175:8 181:21 204:11 215:19 226:9 257:19 262:8 263:16 267:2 275:5 282:19 284:15 285:17 286:9,16,18 291:19 292:8 292:14 297:5 304:6 307:10
**DOJ** 43:7
**dollars** 219:15
**domain** 93:7 227:1
**domestic** 9:13 40:17 42:1 94:14 95:5,20 95:22 122:5,11 134:16 136:4 139:20 142:6 163:8 184:5,8 184:18 185:9 185:11 265:8 269:9
**domestically** 114:15 138:22 139:6 184:14 271:14
**Donohue** 3:4 113:10,19 116:19 117:3 120:19 139:13 145:13 146:2 146:13 149:1 152:16,17 153:21 155:7 155:11,17 156:2,15,22 157:3 160:17 168:10 171:7 176:5,15 177:16 190:22 193:14 198:5 200:7,9 201:9 204:22 205:13
**door** 123:15
**dots** 46:20
**Douglas** 140:20
**download** 303:16
**draft** 213:2 276:12
**drafters** 225:3
**dragnets** 253:6
**dramatic** 301:14
**draw** 169:12 187:15 188:9 261:13 275:11 288:16
**drawer** 226:8
**drawing** 188:7
**drawn** 207:6
**draws** 188:13 191:7
**drive** 170:21
**drug** 29:12
**dual** 212:12
**due** 114:16 240:1 251:12
**duty** 114:16 226:4 248:1,3 248:6,17
**dynamic** 218:7

**E**

**earlier** 26:22 55:19 58:20 61:20 74:5 80:8 85:5 93:20 96:7 147:16 186:6 187:4 191:2 195:4 196:17 220:19 243:17 249:1 271:22 272:8 274:15 279:11 296:11 301:6
**early** 45:7 46:1 70:4
**easier** 182:3
**easily** 207:3
**East** 263:17
**echo** 170:4
**economic** 117:17 218:22 219:12,17 240:16 241:14 282:8 301:8
**education** 58:1 311:12
**effect** 83:11 192:15 213:20 250:21 301:14 307:3
**effective** 67:8,10 67:14 68:18 69:9 85:17 215:3,3,8 224:13 225:22 233:16 234:13 241:9 271:7
**effectively** 64:20 221:2 225:5
**effectiveness** 66:5 68:22 69:7
**effectual** 230:19
**effectuate** 57:20 59:16
**effectuated** 54:9 109:5
**efficacy** 63:13 63:18,19 64:2 64:6,8 83:2,3 92:22
**efficient** 228:22
**efficiently** 31:5
**efforts** 5:6 11:21 213:7 218:9,15 237:10
**either** 10:4 14:4 33:13 64:5 66:18 91:16 107:20 114:11 117:13 149:9 154:3 158:2 173:5 189:9 245:10 254:8 262:10 266:13 306:6
**elaborate** 23:2 23:21 94:4 95:14 127:3 170:5
**Eleanor** 212:21 247:12
**electronic** 7:15 25:15 126:1 133:14,16 137:11 140:16 165:1,4,6,9,11 171:17 188:13 188:18 210:6 244:19 246:6 246:10,18 264:16 265:7 289:21 290:1 291:11 296:14 303:17 306:7
**element** 32:4 79:8 95:1 103:21 149:12 155:18 179:20 204:13 221:21 245:11
**elements** 309:19 309:22
**eleven** 113:5
**eliminate** 34:20
**eliminating** 203:17
**Elisebeth** 4:14
**Elizabeth** 2:7
**email** 9:5 10:8 14:5 25:12 50:13 51:4 52:6,10 54:8 54:14,18,20 71:6 73:21 167:20 174:17 191:9
**emailing** 56:19
**emails** 26:2,10 26:11 120:4 190:15
**embassies** 231:20
**embedded** 104:5
**emergency** 33:7
**emerging**

301:21
**emphasis** 220:22 237:10
**emphasize** 69:10 105:16 121:18 144:18 151:12
**emphasized** 183:20
**emphasizing** 13:8 143:14
**employed** 129:3
**employee** 111:7
**empowering** 84:10 225:4
**en** 227:5
**enables** 8:17
**enabling** 222:10
**enact** 228:16 271:14
**enacted** 15:20
**enactment** 127:20 128:4 130:18 194:13 194:18 195:20
**encompasses** 87:19 279:7
**encounter** 87:16
**encountering** 59:12
**encourage** 64:8
**encouraged** 46:20
**encourages** 312:6
**encroach** 126:22 202:11,12,13
**encrypted** 118:21 119:1 135:20,21
**encryption** 222:18,20
**endorse** 123:8 280:10,11
**endpoint** 124:19
**ends** 82:8
**enforceable** 307:14
**enforcement** 13:6 19:7 118:5 136:5 143:19 144:20 156:1 203:18 277:13 306:16
**engage** 127:19 175:10 196:22 197:1 262:12 264:10
**engaged** 16:6 115:14 156:2 158:11,14 194:12 196:21
**engagement** 113:12 221:3 284:13
**engaging** 233:12 242:7 262:10
**England** 307:18
**enjoy** 15:7
**enlightening** 209:1
**Enlightenment** 233:11
**enormous** 270:10 302:14
**ensure** 9:10,18 16:22 24:8 44:22 61:2 212:8 224:9 243:14 248:1 254:1,3 271:10 271:16
**ensuring** 58:18
**entails** 106:11 299:12
**entire** 71:3,9 98:8 105:6 110:10 165:13
**entirely** 159:9 167:11 197:12
**entities** 240:22
**envision** 176:3
**envisioning** 207:21
**equal** 253:18
**equality** 231:5 264:16,22
**equally** 186:12
**equates** 43:10
**equivalent** 205:15
**eroded** 222:13
**erroneous** 43:12 73:17 178:2,4
**erroneously** 74:7
**error** 43:9
**especially** 119:19 126:3 129:20 163:4 170:15 233:7 236:20 259:3 269:5 303:20 304:15
**espionage** 231:18,19 241:14 262:19 263:3,16 305:10
**espouse** 278:19
**essential** 245:10
**essentially** 24:6 43:10 61:6 91:7 104:15 108:20 118:9 130:15 144:11 145:5 198:2 224:16 229:7 269:20 297:20 305:9
**establish** 40:18 42:2 177:20 179:9,10
**established** 116:5 141:11 141:20 200:1
**establishes** 212:13
**estimate** 93:14
**estimating** 65:17
**estimations** 263:4
**etcetera** 109:16 120:4 161:5 171:6,6 173:7 179:7 196:2 307:21 309:20
**EU** 238:12,13 239:15 241:8,9 241:14,15 275:21
**Europe** 220:9 220:12 275:19 276:15 310:18
**European** 226:17 239:14 241:6 246:9,15 246:16 276:10 276:13 301:19 308:5,7,9
**evaluate** 64:2,12 64:14 66:4 84:14 186:22 205:10
**evaluated** 22:22 65:22 94:17
**evaluating** 110:22 243:3
**evaluation** 63:12 69:7 72:11 83:16,19 84:6 94:18
**event** 5:7 141:8
**eventually** 294:13
**everybody** 35:22 169:21 188:5 215:6 286:16,17 289:12
**everybody's** 174:18 252:1
**everything's** 185:3
**evidence** 17:15 19:6 21:18 32:1 108:1,2 109:4 122:9 136:7 142:3 146:20 148:16 169:1,6 186:15
**evident** 204:18
**evolution** 193:22
**evolving** 305:15 310:12
**ex** 20:18 21:19 21:20 42:16 59:19 82:10 206:8
**exact** 93:17 222:6
**exactly** 13:12 44:1 185:8 248:14 291:22 293:11,17
**examination** 205:16
**examine** 110:16
**examining** 238:7
**example** 17:12 17:18 19:2 26:14 32:16 47:7,13 59:12 66:10 71:9 73:7 81:7 83:17 99:22 109:10 153:8

165:18 167:1 169:19 186:16 188:10 190:11 207:1 222:16 225:8 256:13 259:5,17 265:6 268:20 281:6 290:16 298:16 300:12 302:2
**exasperation** 291:17
**exceedingly** 69:14
**exception** 14:11 15:19 16:1 115:7 117:12 130:7 139:14 143:6 149:18 150:2,4,5,15 150:17 151:6,9 183:3,6 184:16 185:14 186:5,8 186:20 259:21 262:1,15
**exceptions** 95:13 102:7 117:9 152:6 202:2,4 299:20 300:1
**exchange** 7:7 84:3 166:15 233:8 257:4
**excited** 283:3
**excitement** 35:8
**exclude** 86:18
**excluded** 195:5
**exclusive** 218:13
**Excuse** 162:16
**execute** 256:15
**executed** 85:15
**execution** 292:3
**executive** 20:8 68:20,21 81:7 81:11 84:3 85:12 125:22 126:16 127:21 128:5,14 140:2 140:4 142:13 142:14 182:20 183:1 187:17 188:12 229:15 256:14 291:4 291:22 292:1 293:11,17
**exempted** 229:13
**exercised** 127:7 234:20
**exercising** 121:20
**exist** 102:8 160:13 184:18 227:6 240:7 287:6 301:8
**existence** 156:12
**existing** 128:19 310:14
**expanded** 87:4
**expect** 5:20 46:22 58:15 77:22 83:19 169:2,7
**expectation** 121:6 190:9,13 227:9
**expeditiously** 32:19
**experience** 45:6 99:2,14 187:1 210:14 219:5 284:9
**experiencing** 218:17 219:6
**expert** 252:7
**experts** 261:11 290:14 291:2
**expire** 69:4
**expired** 50:5 56:13 283:18
**expires** 313:17
**explain** 11:6 20:7 44:1 50:11,19 58:2 58:12 82:7 129:5 193:8 262:13 311:17
**explained** 21:5 28:2 212:3,22 213:10
**explaining** 21:8 39:2 91:14
**explanation** 56:21 76:4
**explicate** 76:8
**explicates** 87:11
**explicitly** 164:10 164:11 165:5
**explosives** 56:20
**exposes** 229:5
**expository** 275:14
**expression** 124:12 299:3
**expunged** 117:10
**extended** 110:17
**extensive** 11:5,7 44:20 45:16 210:14 235:1 241:7 297:17
**extent** 20:13 45:1 65:4 81:3 88:8 112:14 163:11 170:4 207:22 221:11 274:3 275:3 308:7
**external** 84:22 258:19
**extra** 33:15 297:10
**extra-territori...** 214:4,18 225:17 227:17 229:5 234:12 244:14 245:12 270:13 271:12 271:18,19 289:18
**extraterritorial** 216:5 224:3 234:4,9,15 256:1 268:18 268:21 291:9 303:1
**extreme** 168:3 169:19 242:3
**extremely** 49:2 251:5 254:6,16
**eye** 99:5

**F**

**FAA** 123:17 165:14,19 166:16
**fable** 221:10
**face** 142:4 187:22
**Facebook** 191:7
**faces** 130:21
**facetious** 167:20
**facial** 154:17
**facilitate** 229:14
**facilities** 281:11
**facility** 162:15 168:4
**facing** 218:21
**fact** 10:19 12:1 16:21 27:15 32:8 40:9,19 45:2 46:19 47:6 52:20 59:4 64:17 66:15 74:14 77:2 84:16 87:22 92:8 95:8 103:12 134:14 135:22 139:7 143:18 150:1,15 155:13 158:10 158:13 159:9 160:11 163:4 166:1 172:14 173:7 177:22 180:18 200:16 214:5 215:16 218:13 219:13 221:10 244:12 245:5,7 246:14 251:14,15 252:13 253:3 258:20,22 274:22 275:3 284:8 290:21 294:6 302:19
**fact-specific** 41:15
**factor** 33:8 157:1 235:2
**factors** 23:6
**facts** 33:14 41:16 187:10
**failed** 213:7
**failure** 229:4 230:4
**fair** 54:3 102:21 108:21 113:1 158:6,7 159:6 164:12 193:18 208:19 260:20 260:22 261:3 262:10 308:6
**fairly** 84:3 97:14 99:13 102:9 158:4 180:7
**faith** 71:19 250:21 267:21
**faithfully** 85:15
**fall** 94:9 104:13

229:22 302:17
**falling** 9:6
**falls** 144:14
**false** 284:14
**familiar** 35:11 219:2,21
**family** 211:5
**far** 48:15 88:19 97:6 117:2 144:3 151:9 245:1 272:20 292:10
**far-reaching** 205:20
**farthest** 260:16
**fashion** 66:3 243:5
**faulty** 239:1
**favor** 4:17 130:11 258:5 312:15
**FBI** 18:4,15 19:2,3 30:6 35:13 61:19 78:22 85:21 86:4 105:17 108:3 257:9
**FBI's** 106:1
**federal** 2:13 4:10 5:10 86:21 111:6
**feel** 136:22 137:2 154:3
**fellow** 240:3
**field** 233:19
**fifty** 214:14
**fifty-six** 218:6
**fighting** 303:21
**figure** 24:15 29:12 32:18 67:4 172:1
**figuring** 24:13
**filed** 223:12
**files** 45:15
**filing** 77:21
**fill** 8:15 67:1
**fills** 26:15
**filter** 192:15
**filtering** 192:17
**final** 6:21 120:15 124:9 208:21 303:9
**finally** 13:7 31:20 42:22 44:4 119:15 123:13 136:3 216:2 222:11
**find** 12:19 32:16 90:13 114:17 115:20 152:14 153:2 154:15 164:1 172:3 178:16 266:8 281:15 287:3 295:22 298:12 303:2
**finding** 21:11 43:12 124:7 135:22 153:19 153:20 193:12
**findings** 239:9 241:18 242:18 293:12
**finds** 123:1 169:6
**fine** 102:16 289:5 295:9
**finger** 288:13
**fingers** 116:17
**fingertips** 112:5
**finish** 85:4
**firm** 107:1 218:11 222:19 238:4
**firm's** 238:5
**firmly** 221:1,9
**firms** 272:4,19 272:22
**first** 6:12,19 8:7 10:3 20:2 24:3 25:19 27:12 31:11 32:7 33:3 38:22 39:3 59:3 75:1 76:3,12 80:6 114:3,5 119:16 119:18,22 120:10,16 121:22 125:18 129:6 132:14 132:19 133:5 135:2,16 147:9 152:2,20 153:1 153:4,6,9,10 153:16,17 154:12,14,18 155:8 156:4,14 156:20 157:14 157:18,21,22 158:4,15 161:14 164:7 165:1 169:11 171:15 179:12 180:17 182:15 187:9,15 201:20 205:3,5 210:2 211:14 211:21 218:22 221:5 223:10 232:4 235:8 236:3 247:16 248:21 256:13 258:7 272:12 273:2 285:19 288:16 292:12 294:5,6,11 297:9 305:12
**FISA** 5:12,16 7:19 8:21 9:8 12:16,22 15:15 15:20 16:12 20:16 29:4,6 48:1 49:7 74:19 75:13,15 76:15 83:8,9 98:13 109:2 111:3 112:13 112:21 117:15 118:10 121:16 125:19 126:12 127:20 130:18 139:4,5,9 141:7,10 149:2 150:4,6,8 158:3 165:14 173:4 184:22 184:22 185:4,5 185:6,17 186:21 187:2 194:1 195:4,6 200:20 202:9 204:13 207:8 208:2,7,14 222:8 288:20 308:20
**FISC** 22:10 59:10 62:12,13 62:16 72:14 112:10 115:1 134:13 202:18 202:21 222:8 294:22
**five** 4:12 17:18 47:8 69:5 99:9 101:8,10,11,12 104:8 172:5 214:5 301:8
**flavor** 37:10
**flip** 182:3
**flipping** 192:5
**flowing** 248:12
**flows** 85:19 127:9 228:21 229:20 300:10 300:18
**focus** 5:15 6:17 7:1,13 66:20 86:16 132:16 174:13 201:4 210:4 218:16 261:15 292:20
**focused** 56:3 57:12 68:11 85:22 92:19 124:10 145:20 253:10 261:16 276:4,12
**focusing** 51:11 55:20 254:1
**folks** 76:21 77:6 98:5,6 127:5 128:20 219:2,4
**follow** 14:15 27:11 81:16 98:4 120:10 192:20 206:13 247:1 282:17 288:14
**follow-up** 56:16 152:18 207:13 291:13 311:5 311:12
**following** 28:13 56:15 93:2 97:11 117:4 196:9 235:10 238:15 239:18 266:18
**follows** 66:16 166:7
**force** 265:6,18
**forces** 215:4 308:9
**forecloses** 164:10
**foreign** 1:7 2:10 3:3,21 7:14,17 7:22 8:4,18 9:2 9:5,19 10:10 11:12,16 12:3

12:12 13:5 14:11 15:22 16:3,6,17 17:14,15 29:7 31:18 32:1 43:2,21 44:15 44:21 45:3,22 46:7,8,17 47:2 49:1 51:10 58:10,16 59:6 59:9,15 60:10 60:14,18 61:1 61:8,21 67:19 67:21 68:12 73:11 79:10 80:1,16,19 81:18,19 82:1 82:2 85:6 92:6 95:9 102:13 103:1 104:20 106:6 107:21 107:22 108:6 109:4 110:3,7 111:18,22 112:1 115:6 116:2,6,7 117:11,17 122:9,15 126:2 126:2,6 127:1 127:2,8,10,14 127:19 128:2,7 128:8,14 129:3 129:12,13,21 130:3,7,15 131:13 133:10 133:15 134:3,8 138:3,3,11 139:1,5,8,15 141:5,13,13,15 141:21,21 142:12 143:3,4 143:7,15,22 144:5,12,21 145:7,18 146:9 147:2 148:6,9 148:11,14 149:2,3,4,5,7,9 149:10,14,18 150:1,12,15,21 151:2,6,9,15 162:3,7,19,22 163:8,10,17 164:3 167:11 167:11,12 169:20 171:11 173:19,22,22 174:1,2 176:9 179:22 180:14 181:1,11,14,21 183:13 184:9 184:17 185:9 185:14 186:4,8 186:13,19 195:10 202:13 204:2,2,3 207:17,18 208:1,3,8,17 209:16 210:6 210:18 215:12 215:16,17,21 231:9,10 232:6 232:17 233:1,2 235:18 236:22 239:3 240:6 245:2 253:9 255:2 257:21 258:8 262:11 262:12 264:10 274:12,16 279:5,8 281:19 281:19 283:2 285:1,5,11,11 285:12,15,16 285:17,21 286:4,6 287:13 287:17,21 288:4,18,19 290:2 294:18 303:12,13,15 304:6 309:12

**foreigner** 281:17

**foreigners** 10:20 109:11 180:18 181:21 229:10 254:7 258:3 259:1 269:1

**foreignness** 41:4 42:2,12 43:8 43:12 52:18 58:21 61:12,22 74:12

**foreseeable** 159:9

**foreshadowed** 239:14

**forge** 220:20

**forgive** 93:15 145:15

**form** 10:5 17:4 76:16

**forma** 99:2,6,12 99:19

**format** 144:15

**former** 234:6

**forms** 238:22

**Fort** 34:17

**forth** 52:11 67:22 94:19 104:3 288:20

**forthright** 159:14

**forum** 260:19 277:2 306:16 307:5

**forward** 32:19 113:21 242:19 247:18 273:4 274:8 310:17 310:20

**foster** 5:17

**found** 11:21 17:21 18:15 34:20 43:9,20 63:11 82:21 99:1,6,9 166:15 184:17 240:9,20 246:9 254:6 295:15

**foundation** 221:8,10

**founded** 256:22

**four** 41:20 42:1 113:22 114:4 178:13 283:7,8

**fourth** 10:16 12:1 13:1 14:9 14:11 15:2,7,9 15:12,14,17 16:2,9 17:4,22 20:6,9,11,12 21:4,7,9,11,13 22:4,11,13,19 27:13,19 28:7 28:15 39:4,6 39:15 43:4 74:21 75:19,21 80:13 94:22 116:10 117:22 119:15,18 121:2 126:5 129:2,6,14,17 130:10 131:5,6 131:20 137:4 137:19,21 138:8,16,17 142:17 144:16 144:19 146:18 148:3 154:10 154:15 160:4 172:21 175:22 180:19 182:9 182:11 183:2,3 183:4,6,8,19 184:11 185:1,8 185:20 186:5 186:12 190:4 191:18 192:1,4 192:8,17 193:7 200:4

**frame** 125:15 126:11 145:9

**framework** 216:19 222:6,9 226:19 227:18 293:14 301:11

**frameworks** 239:7

**France** 239:7 240:11,14,21

**Franklin** 5:4

**frankly** 246:3 251:4 297:8

**Frazelle** 5:5

**free** 136:22 137:2 199:3

**freedom** 125:1 299:2,3

**Freiburg** 209:17

**frequently** 144:3 154:15

**fresh** 74:14

**friendly** 244:7

**froms** 163:14,16 168:7

**front** 24:6 58:12

**front-end** 160:12 193:10

**frustrating** 63:11 266:8 295:16

**frustration** 96:14

**full** 12:9 69:21 75:19

**full-up** 21:14

**fuller** 87:11

**fully** 33:1 84:12

**fulsome** 76:4

**function** 57:22

58:1 204:16,21 205:1 303:18
**functions** 230:20 232:18 257:20
**Fund** 277:11
**fundamental** 87:13 256:8 257:3 259:12
**fundamentally** 182:4,8 251:16
**funneled** 185:3
**further** 128:22 130:8 171:12 175:22 202:11 205:16 235:12 257:14 302:7 310:10 311:5 313:9
**furthers** 284:14
**future** 229:17 291:1

**G**

**G-10** 257:18
**gap** 26:16 33:11 33:20
**gaps** 33:12
**gardens** 220:7
**Garfield** 3:16 209:11 218:4,5 271:21 273:1 274:20 284:2,7 301:5 308:14 309:3
**Garfield's** 310:21
**gather** 142:15 145:3 151:2 181:1 186:15
**gathered** 144:11
**gathering** 14:8 54:16 89:16 115:7 128:15 130:16 131:14 139:6,15 143:21 144:5 144:22 145:8 149:14 183:18 184:9 186:14 195:11 235:18 259:7 276:13 302:3
**general** 2:13,15 2:17,19 7:21 9:1 11:9 28:10 29:3 35:13,14 35:15,17 62:14 80:17 81:2 85:20 87:15 112:20 119:8 119:22 126:12 140:15 141:1 151:1 161:21 167:6 231:3 234:2 236:5 249:20 253:2 255:14,15 258:10 259:20 263:11,20 266:9 277:9 280:5 285:21
**General's** 106:15
**generality** 206:11 304:11
**generalize** 259:10
**generally** 106:17 107:17 107:19 130:9 149:14,19 163:3 167:7 187:5 216:18 219:19 273:21 279:8
**generated** 65:2
**generic** 57:14 106:19
**generis** 207:22
**generous** 137:7 138:21
**generously** 130:11
**Geneva** 214:5
**gentlemen** 36:2
**geographic** 91:6 133:7 162:8
**geography** 138:10 228:21
**Georgetown** 3:4 113:11
**German** 235:4 237:19 246:14 247:17 256:2,5 258:5 259:5 263:14 277:10 279:15 309:16
**Germany** 3:21 209:17 225:8 226:7 239:7 240:11,21 246:19 256:6 256:12,14,21 257:16 263:15 263:17 279:17 287:22 288:1 306:1,1 308:11 309:19 310:4,8
**getting** 24:11,21 35:8 51:16 62:3 99:9 103:13 125:11 154:6 264:3 298:20 301:9 310:20
**give** 8:13 60:17 61:3 63:22 110:3 122:4,18 142:19 159:16 160:15 197:16 213:21 250:9 250:20 256:1 263:6 266:1 268:20 272:21 280:20 282:5 282:15 284:4 305:2
**given** 26:19 42:1 54:1 123:19 128:11 131:14 200:16 249:7 252:3,21 277:17 282:17 306:2
**gives** 121:21 143:10 190:2 309:6
**giving** 259:1 299:11
**glad** 8:14 56:14 58:3
**global** 220:19,22 221:3 233:5,16 238:5 264:2 276:3 283:14 300:7 310:22 311:1
**globally** 232:8 300:4
**globally-integ...** 220:4
**go** 29:17 30:1,4 33:6,15 51:13 51:14 52:19 53:14,18 58:18 78:14 80:22 93:5 100:4 115:15 131:19 142:2 143:1 149:20,20 159:4 164:4 171:4,16 172:9 175:9,16 178:15 241:16 245:1 250:16 257:14 259:13 265:22 275:5 278:9,20 280:1 280:9 281:1 302:7,21 303:15
**goal** 261:6
**goals** 67:15,17 143:20
**goes** 46:14 53:20 78:21 97:12 143:12 158:20 183:11 272:20 275:21 276:9 299:16 305:13
**going** 21:10 34:3 36:3 48:14 50:4 51:15 52:15 53:4 60:15,17 61:9 64:15 71:11 74:17 83:1 84:7 92:16 100:16 104:15 104:21 105:1,4 132:16 136:21 143:1,18 145:9 149:17 167:3 170:8 173:3 178:1 179:16 180:2,9 181:21 182:10,14 183:18 195:11 196:1 209:2 210:4 213:15 223:13,19 226:6 227:2 228:8 244:2 250:14 261:6 264:11 265:13 281:18 286:22 287:3 295:5 296:9 302:12 305:16,17

309:14,15
**good** 4:2 56:17 68:2,7 71:19 75:5,7 145:11 209:6 250:21 267:20 275:9 299:20,21
**Google** 191:7
**Google.com** 51:7 55:4 60:17 167:2 207:2
**gotten** 29:6,16 29:21 251:5
**govern** 111:20 229:11
**governing** 105:3
**government** 2:10 6:12 8:1 11:6 16:3 20:19 30:22 31:6 38:4,14 40:14 54:10 64:4 66:19,20 67:4 70:13,21 94:19 97:17 108:6 109:13 110:4 111:18 121:3,20 122:4 122:11,18,21 123:7,10,15 124:20 125:3 126:8 130:12 130:21 131:7 132:5 142:1 143:12,21 145:1 151:14 151:17,20 152:8 158:11 158:13,22 159:16 160:3 162:17 163:2 166:6,22 167:8 169:5 171:3 174:16,21 175:5,6,19 183:12 187:19 187:21 189:4,8 190:20 194:12 194:17 196:4 196:16,20 197:16,17,19 198:22 199:20 201:19 206:22 207:1,7 211:16 215:12 222:14 222:22 225:18 228:10 234:17 239:3 241:1,2 242:5 246:3,4 246:9,14 248:22 250:3 251:10 267:2 267:12 268:3,6 270:20 271:2,7 272:15 273:14 274:13 290:8 291:16 294:17 295:11,21 300:6 308:17
**government's** 7:14 28:9 31:11 37:15 122:2,19 125:16 159:1 159:21 169:10 174:15 187:10 188:2 189:5 192:7 241:4 303:3
**governmental** 238:9,20 239:1
**governments** 106:7 112:1 126:2 215:17 215:21 234:3 240:22 242:2 246:5,20 250:8 267:19 268:16 282:11 283:2 286:6 290:7,14 300:17 303:5
**grabbed** 284:21
**grade** 277:6 282:15
**grand** 4:7 153:12 156:7 156:18 194:6
**grandmother** 81:22 167:21 167:22
**grandmothers** 171:20
**grandson** 168:1
**granted** 183:14
**granting** 228:9
**granular** 62:18
**granularity** 273:10
**grave** 285:4
**gray** 172:2
**great** 13:20 52:19 58:2 80:11 136:20 137:16 201:15 222:4 251:12 252:21 253:8 254:8 296:2
**greater** 47:16 48:15 94:2,11 221:12,14,21 240:1 252:11 272:13 273:10 273:15,19 301:11
**greatest** 7:6
**grievances** 200:17
**ground** 5:20
**grounds** 205:3,4
**group** 8:12 203:20 211:22 228:8 290:13 291:2
**groups** 45:13 213:16 215:19 251:12 290:6 290:18
**growth** 118:12
**guaranteed** 304:20
**guarantees** 237:11 242:10 258:6,21
**guards** 298:13
**guess** 15:1 29:1 33:12 54:12 61:21 83:5 146:8 171:22 176:11 186:11 189:22 193:8 203:12 207:21 208:2 209:22 243:7,11,22 254:20 264:6 272:17 274:10 282:2 292:7 295:7,18
**guidance** 226:18 249:14 309:10
**guideline** 104:6
**guy** 55:3,8 60:16 73:10 137:22 167:2 207:2,2

**H**

**hacker** 108:10
**half** 34:15 98:6
**halves** 162:6
**hand** 41:16 119:19,19 188:14 191:3,4 206:3 247:22 313:12
**handed** 139:22
**handle** 19:9 34:10 168:8
**handling** 217:20
**hands** 174:15 291:3
**hanging** 24:12
**happen** 21:21 254:5
**happened** 115:13 171:3 292:18 300:14 307:11
**happening** 68:20 137:10 185:3 248:11
**happens** 62:4,4 72:8 73:13 120:7
**happy** 27:9 50:10 116:1 120:12 198:8 200:9
**harbor** 220:11 300:11
**hard** 33:14 39:2 191:10 301:2
**harder** 138:8 266:17
**harms** 228:14
**Harold** 223:20 234:6 252:6
**Harper** 212:3 212:11 213:9
**head** 87:12 95:12 101:20 210:12 212:20
**headed** 292:2
**hear** 76:6 171:8 215:9 294:10
**heard** 70:7,8 115:4 172:12 186:6 193:17 274:15 279:10 289:16
**hearing** 1:5,15

4:4,9,16,17 5:1 5:17 7:13 117:5 206:13 312:4,13,15,15 312:21
**hearings** 57:22
**heart** 305:13
**heartening** 276:10
**heeds** 269:2
**held** 1:15 15:21 16:12 129:22 130:5 142:6 147:13 150:3 186:19 201:10 201:14 213:5 307:6
**help** 20:14 66:13 135:11,12 146:11 194:8 194:10 202:14 218:19 292:8 296:1
**helpful** 24:2,18 50:16 58:6 88:1 117:16 152:15 153:2 192:19 221:15 221:20 222:15 223:8 260:18 272:10 273:5 273:11 275:5 311:6,22
**helping** 66:20
**high** 32:6 34:11 103:16 124:22 178:22 179:10 180:7 221:2 261:1,4,8
**higher** 95:21
**highly** 129:17 234:22
**hill** 222:3
**historic** 51:19
**historical** 128:21 233:10
**historically** 10:21 82:14 88:7 97:7 183:10,12
**history** 12:8 123:3 125:20 128:11 130:13 166:12,15 167:12 181:20 185:16 214:13
**hits** 299:22
**Hofstra** 3:8 113:14
**Hogan** 3:22 209:18 238:4,6
**hold** 93:3 97:9
**holding** 297:13
**holistic** 83:3
**home** 169:5 211:5 232:22 235:11
**homeland** 236:14
**homework** 311:11
**honest** 268:19
**honestly** 41:2 203:22
**honor** 219:9 267:20
**honored** 262:15
**Hood** 34:18
**hope** 46:22 132:12 136:16 173:20 276:14
**host** 100:6 136:9
**hostile** 285:4
**Hotel** 1:16 4:7
**hours** 98:6
**house** 138:1 217:10 226:7
**huge** 36:5 175:1 180:20 198:22
**human** 3:19 207:4 209:14 210:17,22 211:22 213:9 213:15,16,18 214:6,22 215:5 215:19 226:12 226:17 227:20 231:1 233:14 233:17,19 234:1 235:22 236:2 237:5,9 244:22 246:15 246:17 249:21 250:4,6,17,22 251:4,8,10 259:3 268:9 290:5,11,12,18 307:8 308:5,8
**humanly** 45:1
**humans** 233:14
**humility** 222:4
**Humor** 299:8
**hundred** 36:13 168:20
**hunting** 45:9
**hurting** 261:5
**hypothetical** 174:11 190:1 190:17 191:20
**hypotheticals** 167:17 170:6 170:15,19

**I**

**i.e** 26:9 173:2
**ICCPR** 211:8 211:10,14 212:1,4,6,9 214:3,17 215:13 216:3,4 216:8 217:1 224:3 225:17 226:13 234:4,8 234:12,16 236:21 242:21 244:13 246:8 246:12 248:8 249:1 252:7 261:16 268:21 278:15,20 280:10 289:18 289:20 290:4 291:10,11 295:10 296:4 297:15 298:11 306:6,15 307:7 307:19 308:1
**ICCPR's** 282:7
**ICJ** 290:17
**idea** 256:17
**ideas** 252:17
**identifiable** 81:14 179:3
**identification** 154:16,18
**identifier** 28:18 193:5
**identifiers** 37:3 37:19 295:1
**identifies** 163:2
**identify** 9:2 65:5 87:14 123:6 178:20
**identifying** 53:9 104:10
**identity** 60:8
**idiosyncrasies** 97:15
**ignore** 41:12 168:7 169:3,7
**ignored** 46:4
**ignoring** 172:4
**IGs** 308:20
**II** 3:1 142:14 144:6 194:1,4
**III** 3:13 29:10 121:16 155:21 197:18 206:7
**illegal** 263:8
**illegitimacy** 159:20
**illegitimate** 163:18
**illustrating** 302:16
**imagine** 30:3 76:17 204:22 297:8
**immediately** 101:19 201:21 265:1
**impact** 28:20 29:2 87:4 184:4 218:22 219:12,14,18 272:3 280:15 293:4
**impacting** 287:10
**impacts** 232:3 299:3
**impair** 280:14
**impermissible** 89:5 288:18
**implement** 58:13 268:8
**implementation** 69:19,20 188:11 310:6
**implemented** 69:20 74:21 306:21
**implementing** 187:19,21 196:6 267:15 306:19
**implicate** 192:17
**implicated** 115:20 153:4

171:16 191:19 248:18
**implicates** 14:9
**implicating** 94:12 155:8
**implication** 47:17 157:22 256:1
**implications** 27:14 33:2 114:20 120:10 123:4 138:15 170:22 171:10 175:1,22 198:12 205:20 205:21 219:18 220:16
**implicitly** 162:5 162:5 165:19 310:22
**import** 42:7 88:20
**importance** 247:20 273:19 274:8 292:15 301:10
**important** 10:2 12:13 13:13 19:8 36:12,17 49:19 60:1,10 65:13 69:9,14 80:7 82:5 119:12 124:10 125:18 139:11 143:5 151:11 187:15 198:19 199:15 201:5 221:4 222:10 223:4 236:9 248:7 251:1,3 254:14,18 273:13 275:17 289:1 311:10
**importantly** 305:12
**impose** 216:4
**imposed** 128:15 129:4 131:18
**imposes** 129:2 212:4 215:14 229:5
**imposing** 194:16
**impossible** 260:4
**imprecise** 208:10
**impression** 77:6 98:20 100:8 307:22
**impressionistic** 65:11
**in-country** 282:13
**inadvertent** 97:2 101:1,6 101:18,22 102:2
**inadvertently** 94:13 100:20 122:12 201:17
**inaudible** 259:14 303:12
**incident** 72:13 73:16 88:4
**incidental** 12:10 12:14 14:1 15:3 43:19 45:14 81:17 82:6,13 94:12 96:6,7,8,15,19 96:22 97:2 100:18 101:4,7 101:18,22 102:4,10 103:12 115:13 158:21 159:7 160:2,4,10 201:1
**incidentally** 12:2 13:3 15:12 16:10,20 17:11 43:18 52:13 79:21 80:1 92:9 106:4 108:13 159:3 160:13 180:3
**incidents** 11:12 11:20 34:17
**include** 75:13 109:11 117:16 117:17,18,19 124:1 135:13 151:4 215:2 270:6 276:21
**included** 128:9 200:18 308:22
**includes** 11:7,11 11:13 84:17 239:10 273:20
**including** 6:18 21:12 121:16 172:14 187:7 203:11 222:2 233:6 250:8 251:4,18 273:7 282:5 308:18
**inclusion** 114:5
**inconvenience** 49:6,10
**incorrect** 38:16 72:11 211:8
**increasing** 118:11
**increasingly** 219:9 220:2
**incredibly** 152:14 221:20 223:4,8
**incrementally** 228:10
**increments** 42:18
**independent** 240:2 308:16 308:21
**indicated** 271:22
**indicates** 84:2 171:15
**indication** 118:7 282:16
**indicator** 172:11
**indicators** 48:4 172:22
**indicia** 121:14
**indictment** 86:20,21 88:11 118:18
**indifferent** 198:22
**indiscriminate** 223:7 274:14 274:22 275:4
**individual** 29:13 64:11 73:18 106:22 114:10 114:18 116:8 123:5 141:12 149:8 154:7 170:1 177:20 178:6 205:12 205:13,21,22 212:14 225:19 225:22 227:12 228:12 237:17 281:16 294:1 310:6,6
**individual's** 254:11 298:15 298:17
**individualized** 10:17 158:7,17 160:7 199:2 206:4
**individuals** 115:20 118:3 120:1 140:1 141:17 212:9 214:11 217:11 229:22 237:15 237:16 242:5 244:15 245:13 248:4 253:7,10 271:17 281:7,9 281:10 292:2
**industry** 3:17 209:13 232:12 237:7 275:19 310:21
**ineffectual** 126:15
**inevitable** 83:5
**inevitably** 6:1
**informally** 24:11
**information** 3:16 5:22 6:3,6 6:10 7:15,19 8:1 9:21 10:1 13:4,14 14:13 15:11 16:10 17:8,11,13,19 18:9,22 19:3,5 19:10,12,16,19 19:22 27:16 28:1,6,7,8,11 29:9,14,17,18 30:2,5,21,21 31:2,4,10,16 31:19,21 32:10 32:11,21 33:16 34:21 35:3 36:4 37:15 38:20 41:11,12 41:21,22 42:8 43:17,17,20 44:9,14 45:14 46:13,18,21 47:3,4 48:22

51:8,11,15,16
52:2 53:5,15
57:7,8,12
58:11,16,19
60:17,18 65:9
67:20 68:6
69:22 70:9
72:9,18 73:3
77:20 79:11
80:20,20 81:9
81:14,17 83:18
86:1,2,14 89:4
89:16 93:12
95:10 100:19
103:12 104:1
104:10,12,18
104:20 105:5
106:4 107:20
108:9,11,15
109:12 110:3,6
110:11 111:8,9
111:22 112:8
112:21 114:5
115:5,9 117:10
117:11,16,18
117:19 118:3
119:5 120:5
122:15 133:11
134:8 136:2,14
139:17 141:7
142:2 143:21
144:1,2 145:3
146:3 147:4,12
147:13,19
148:10,17
151:3 154:3,7
154:9 157:10
157:12 158:15
159:2,8,17
162:3,18
167:19 169:21
170:9 171:4,14
173:8,9 174:1
174:15 175:20
176:6,6,7,17
177:13,18
178:16 179:3
179:11,18
180:2,6,10,12
181:1 191:10
193:1,2 198:1
198:11,17
199:14,18
200:3 201:1,3
201:10,12
203:17 209:12
217:21 226:22
237:16 239:10
240:6 242:2
243:18 244:5
254:2,7,10,15
256:17 257:4
273:14,15
279:6 281:18
285:2,10,16,20
286:1 287:13
287:20 293:1
294:18 311:15
**information's** 146:16
**informative** 67:19 152:15
**informed** 84:12 226:22
**infringe** 304:14
**infringed** 234:21 302:2
**infringement** 231:17 232:12 302:5 303:19 304:18
**infringements** 232:1,5 235:15 304:7
**infringes** 235:8 235:9
**infringing** 264:9 303:13
**inherent** 10:22 125:22 127:13 131:17 182:20 183:1
**initial** 64:3 74:9 78:9 114:1 118:7
**initially** 79:13 118:10
**initiate** 231:9 237:1
**injury** 172:17
**innocent** 171:21
**innovative** 218:7
**inquiry** 56:17
**insensitive** 217:8
**insert** 205:14
**inserting** 201:11
**inside** 9:16 20:8 91:10 97:20 128:2 159:19 212:5 245:6 282:10 283:3 306:1
**insight** 308:22
**insights** 194:6
**insist** 282:12
**insofar** 249:6
**inspect** 123:8 189:21
**inspecting** 197:2
**inspectors** 11:9 62:14
**installed** 190:2
**installs** 189:8,8
**instance** 31:12 111:20 114:11 119:21 120:2 136:13 253:13
**instances** 277:14
**Institute** 3:20 209:16
**institutional** 99:10 257:10
**institutions** 257:8,9,12
**instrument** 267:4
**integrated** 220:15
**integrity** 219:10 223:2,3 231:5 232:2,6,11 264:15,22 265:5 305:8
**intel** 98:21
**intelligence** 1:7 2:11,18 3:3 7:14,17,22,22 8:4,18 9:2,3,6 9:19 10:10,19 11:11,12,17 12:4 13:5 14:11 16:1,4,7 16:18 17:14,15 31:18 32:1 33:22 35:16 42:20 43:3,21 44:15,22 45:4 45:11,22 46:8 46:8,15,17,19 47:2 49:1 51:11 58:10,16 59:2,7,9,15,21 60:10,14,18 61:1,8,22 64:18,21 65:13 65:21 66:2,8 67:20 68:12 72:10 79:10 80:2,16,18,19 81:2 82:1,3 83:16 84:10,12 84:16 85:6 86:1 92:6 95:10 99:11
100:3,6,9
102:13 103:2,5
104:11,20
107:21,22
109:4 110:7
111:22 115:6,8
116:2 117:11
118:4,8 122:15
127:2,8 128:2
128:8,15 129:3
129:21 130:3,7
130:15 131:14
133:11,15
134:4,8 139:1
139:5,8,15
141:5,16
142:12,15
143:3,4,7,15
143:20,22
144:5,12,22
145:7,19 146:9
147:3 148:6,10
148:12,15
149:8,14,18
150:1,12,15
151:2,6,9
161:22 162:3,7
162:19,22
163:8,11,17
164:3 169:20
171:11 173:19
174:1,2 176:9
179:22 180:14
181:1,11
183:18 184:9
184:17 185:9
185:14 186:5,8
186:13,19
188:12 195:10
195:12 202:14
204:2,3 208:1
208:3,17
210:15 217:15
235:18 240:6

240:14,18 241:10 253:4 253:12 255:2 256:14,19 257:1,21 258:19 259:7 262:11,12 274:12,16 276:9,13 279:5 281:19,20 285:1,7,15 288:19 294:18 302:3 309:12
**intend** 100:22 223:1 239:12
**intended** 77:9 97:7 122:1,17 274:21
**intensively** 276:5
**intent** 89:15 286:6
**intention** 134:3
**intentional** 11:21 40:16 96:16 130:22
**intentionally** 9:13 97:18 131:8
**intentions** 67:21
**interact** 175:3,4
**interaction** 99:19
**interactions** 99:10,11,17
**intercept** 9:13 12:17
**intercepted** 12:3
**intercepting** 51:18 233:2
**interception** 118:20 161:4 233:4 235:7
**interest** 102:22 103:16 140:21 148:21 159:21 237:20 253:12 261:20
**interested** 91:15 92:7 132:20 251:5 269:18 276:19 312:7 313:11
**interesting** 147:15 263:14
**interests** 16:5 27:4,4 47:17 131:12 143:12 145:5 217:20 218:1 224:2 230:6,17,17 240:17 260:3 261:18 264:9 278:14
**interfere** 254:11 300:17
**interference** 211:5 216:9,12 298:14
**interfering** 230:2
**internal** 41:18 54:10 70:12 236:10 241:15 257:16 258:18 259:22 274:13
**international** 3:21 121:5 122:2 123:21 138:14 147:4 148:1 209:17 210:5,15,20,22 211:10,11,11 215:14 216:1 216:13,16,19 217:3,5 218:1 223:16 227:10 230:14 231:3 231:13,17 232:6 233:17 233:19,21,22 235:22 236:2,4 236:12 237:3,9 252:2 260:10 261:10 262:2 262:14,20 263:11,21 264:8 265:6,10 265:21 267:4,8 272:3 276:7 278:6 285:5,6 286:13 289:4,4 289:7,8,9 298:5 301:17 305:21 306:5 306:10,11,20
**internationally** 138:22 139:7 238:20 273:22 275:6 276:8 289:11 305:18
**Internet** 26:7,8 191:9 219:19 219:21 220:4 220:15
**interpret** 107:6 225:7 244:1,3 268:4
**interpretation** 87:1,2 202:15 212:19 213:18 214:10 225:14 247:22 249:5,9 250:11,19 268:1,6 269:2 269:12,18,22 278:19 291:1,5 296:12 299:1
**interpretations** 243:8 249:14
**interpreted** 125:20 130:10 137:19 184:12 224:13,22 270:13
**interpreters** 249:7 252:5
**interpreting** 246:16 249:12 249:13
**interpretive** 226:13
**interprets** 268:3
**interrelated** 230:18
**interrupting** 48:11
**intervene** 205:2 205:6
**intervention** 297:22
**interviews** 297:17
**introduce** 35:9 37:8 209:8
**introducing** 33:9
**intrusions** 131:22
**invaded** 190:8
**invasion** 190:12
**investigate** 34:16 302:10
**investigation** 116:9 141:19
**investigations** 2:14 124:5
**investment** 300:13
**inviolate** 261:21
**invitation** 230:13 309:9
**inviting** 218:8
**involve** 21:18 86:15 150:19 286:9
**involved** 70:6 88:1 132:2 141:3 149:11 150:19 160:5 198:13
**involvement** 141:20 202:18 202:21
**involves** 188:16 190:18
**involving** 199:14
**invulnerability** 239:3
**IP** 120:1,6,7
**irrelevant** 165:10
**irrespective** 183:2 258:10
**islands** 220:14
**isolate** 66:4
**isolation** 66:5
**ISPs** 26:2
**Israel** 225:13
**issue** 21:8 37:16 37:17 49:15 56:11 57:4 69:17 91:6 106:18 110:21 138:9 223:20 225:10 226:18 240:18 269:4 276:7 295:13 295:18 296:15 300:21 301:9 301:13 303:8
**issued** 5:13 21:10 75:2,18 156:18
**issues** 3:2,14 5:19 6:18,19 7:2 20:22 21:10,22 34:6 36:15 73:7

74:18 113:3 132:17 136:10 136:11 144:19 197:9,11 198:6 198:7 209:9 221:2 227:3 243:1,7,15 261:12 300:16 311:14
**It'll** 76:18
**Italy** 239:11 240:11
**item** 73:3

**J**

**Jaffer** 3:6 113:12 120:18 120:20 149:17 149:21 158:6 164:7,18 165:7 165:12 168:18 168:20 173:10 173:15,18 180:16 186:7 186:17 187:14 190:6 192:2,9 192:16 193:13 196:15 198:18 199:9,22 201:16 202:2 205:18
**Jameel** 3:6 113:11 149:16 153:22 160:20 164:4,5 186:2 196:10
**Jameel's** 170:4
**James** 2:6,13 4:14
**Janosek** 5:5
**January** 5:13 47:19 221:7 237:14 276:12
**Jazeera** 120:6
**Jim** 32:5 35:12 69:10 96:3 160:15 306:13
**job** 64:19 80:18 99:8 257:19 284:2
**Joe** 108:5,7,12 287:21
**John** 3:15 209:10 266:15 286:15 295:8 305:2 306:14 307:17
**joined** 113:10 209:10
**joining** 209:1
**jointly** 162:1
**journalist** 207:4
**judge** 43:14 77:13,16 78:7 82:6 106:2 111:14 117:8 163:4 167:14 171:11 200:14 248:19 252:20 265:11 277:15 283:17 289:1 289:15 300:5 307:15
**Judge's** 50:5
**judged** 185:19
**judgement** 76:9 76:12 97:7 140:13
**judgements** 275:15
**judicial** 11:3 14:18 119:18 124:6 156:16 156:20 157:19 160:11 201:11 205:19 206:9 237:1 241:4 292:4 293:2,20 307:19 310:3,9
**judicially** 307:13
**judiciary** 293:12 293:13,13
**Julian** 3:8 113:13
**jump** 137:2 264:11 284:3,4 295:9
**juris** 263:2
**jurisdiction** 22:16 83:21 212:10,15 213:3 214:12 214:21 215:2 216:7 224:10 224:12 230:1 243:10 244:2,4 244:4,5 247:3 247:5,11 248:2 263:18 270:2,3 270:4 296:6,7 297:12
**jurisdictional** 224:7 243:1,6 243:15,16 245:11 246:21 248:9 270:12
**jurisdictions** 226:16
**jurisprudence** 308:6
**jury** 153:12 156:7,18
**justice** 2:20 3:11 11:9 35:18 42:19 59:20 61:13 62:9 66:6 67:3 74:4 106:14 113:17 140:3,10,19,20 167:7 210:13 233:22 272:19 273:3
**justices** 140:10 140:18 249:11
**justifiably** 175:8
**justification** 54:15 187:13
**justified** 259:16 259:20
**justify** 159:13 186:9

**K**

**Katz** 140:9
**keep** 6:6 7:5 72:8 84:11 101:10,11 102:18,22 103:7,11,15 104:8 116:15 119:4 126:13 128:12 138:10 171:5 283:3,7
**Keeping** 54:5
**kept** 45:8 106:5 135:9 207:1 254:3 293:6
**Kerry** 277:10
**key** 26:14 56:4,6 57:13 108:6,11 135:15
**kick** 102:12 154:1
**kid** 128:18
**killing** 224:19
**kind** 11:2 12:14 18:21 21:14 33:7 35:1 53:20 65:4 73:20 76:2 86:1 92:18 124:5 138:5 157:7 159:6 160:12 162:8 162:11,11 166:13,19 168:4 173:13 174:11,22 177:10 180:5,8 180:9 188:22 189:1,2 190:17 199:12,12 202:8 216:20 226:5 230:13 242:13 253:19 310:20
**kinds** 20:12 158:18 180:17
**Kingdom** 239:8 240:11
**knew** 12:9 70:10 177:8 180:1
**know** 16:14 20:16 22:6 32:18 33:20 34:6 36:9 40:1 41:2 51:6,7 55:3 70:18 76:1 78:15 81:21 82:10,10 83:10,11 84:13 84:20 85:5 90:5,14 91:19 92:13,22 93:17 99:15 104:5 105:16 106:10 108:11 110:9 114:12 120:1 120:22 131:3 132:19 134:2,6 135:5,7 136:12 139:14 151:16 154:18 155:15 157:21 158:21 159:4 163:4 167:2,10 168:22 169:3,4 169:17 170:15 172:8 173:3,6

174:9,9,12 175:13 177:3,4 179:1,2,2,3 184:11 186:22 187:20 188:3 188:19 190:7 194:6 197:15 198:18,20 199:15 200:21 202:4,13 206:1 206:9,12 208:12,15,19 210:8,16 213:14 217:10 220:9,15 222:5 222:5 240:4 243:17 244:17 245:21 247:21 249:6,8 251:8 252:4 254:13 265:9,12 266:21 267:18 270:12 271:6 271:14,15 272:12 279:7 279:10,18,21 281:2,14 282:3 286:13,20 287:10,16,16 290:15,22 291:6,8,10,14 292:21 293:3 295:3 296:9,19 297:3,20 299:4 300:2,5
**knowing** 229:3
**knowledge** 69:21
**known** 25:20 27:15 29:10 89:12 123:18 133:6 254:9 273:21
**knows** 87:20
265:12
**Koh** 234:6,8 252:6
**Koh's** 223:21 247:21
**Ku** 3:8 113:13 125:6,7 137:3 137:16 139:14 142:20,22 145:12 149:15 181:6,7 182:15 183:5 184:10 193:17 194:5 202:6,7
**Ku's** 147:1

**L**

**lack** 26:7 180:19 193:9 194:22 198:13 200:20 239:16 241:8 256:18 284:12 293:19 294:19 295:15
**lacking** 99:3
**lacks** 121:13 291:18
**laid** 94:8
**language** 123:2 161:18 214:13 224:21 290:15
**large** 47:6 57:21 121:3 150:10 187:6,12 188:4 189:3,10,11 232:2 292:13 295:17
**largely** 75:18 144:7
**larger** 49:1 138:9 144:17 277:13
**latitude** 19:4
**Laughter** 261:7
283:21
**Laura** 3:4,18 113:10 136:4 209:13 213:14 245:17 251:19 254:21 266:18 284:19 298:6 305:20
**law** 3:4,5,8,21 8:1 13:6 19:7 85:14 102:3,11 104:6 113:10 113:11,14 118:5 125:14 127:4 136:5 143:19 144:20 155:22 182:11 182:12,12 196:12 197:21 198:4,21 203:17 209:17 210:5,15,20 211:10,11 215:14 216:1 216:16,19 217:3,5 218:2 224:21 226:15 227:8,10 230:8 231:3,13,17 232:7 234:1 237:5,19 238:4 240:9 255:3,12 258:9,9 259:20 259:22 260:22 261:10 262:2 262:14,20 263:1,5,9,11 263:21 264:8 265:7,8,10,20 265:21 266:11 266:14,19 267:4,14 269:5 269:8,9 277:12 279:15,16
280:13 287:2 289:4,4,7,8,9 296:20 298:5 299:20 301:19 301:19 304:22 305:21 306:21 309:14
**lawful** 21:4 32:12 53:19 111:8,10 193:2 199:8 227:21
**lawfully** 13:5 28:5 29:19 30:20 31:3 34:21 37:14,20 38:21 102:20 175:20 177:14 179:11,19,21 180:12 181:16 193:2 196:11 196:13 197:14 197:17,19,22 198:9 199:14 199:19
**lawless** 126:16
**laws** 85:15 198:10 226:19 228:16 239:11 241:15 242:11 275:8,10 284:1 286:12 306:1,3 306:22 311:2
**lawyer** 87:21 88:1 156:12
**lawyer's** 299:15
**lawyers** 87:6,19 153:14
**lead** 34:6 195:1 201:12 236:12 238:5 262:6 302:20
**leader** 254:8
**leaders** 217:12
**leading** 237:4
252:7
**leads** 164:14
**leak** 297:20
**leaked** 6:1
**leaking** 144:3
**leaks** 70:13
**learn** 134:14
**leave** 76:20 100:8
**leaving** 121:18
**led** 249:17
**left** 204:9 270:1 299:17 301:9
**legal** 3:2,6 5:18 6:17 10:13 20:22 21:15,22 25:13 29:21 53:21 54:8 70:15,21 72:12 72:20 106:21 113:12 126:11 140:14 145:6 210:8,10 211:12 212:3 213:20 214:7 215:20 218:2 230:14 232:20 234:6 237:21 238:8,21 267:3 289:13 301:20 303:13 304:8 306:5,10,11 307:3
**legally** 176:12 250:5,12 268:12 299:13 299:13 307:14
**legislation** 220:5 229:16 271:14 284:17 306:19
**legislative** 12:8 84:4 123:3 166:12,15 167:12 291:21

292:6
**legislators** 166:19
**legitimacy** 163:14
**legitimate** 91:8 92:12 106:5 143:11 151:15 172:20 206:13 206:14 217:19 227:22 228:1,5
**legitimately** 95:4 167:18 169:22 207:7 296:10
**length** 121:12
**lengths** 52:20
**lengthy** 84:17 223:12
**lesser** 254:8 256:19 282:3,4
**lessons** 275:10
**let's** 29:11 32:16 73:9 78:11 91:7 108:9 120:7 156:6,17 157:6 160:15 176:7 197:15 265:22 266:5 282:21 297:11 297:12 305:2 310:14
**letter** 87:8,10 132:21 181:13 181:15,17,18 273:9
**letters** 226:7
**level** 32:6 34:11 72:22 206:11 221:3 272:9 273:6,10 278:5
**LEVINSON-...** 202:20
**Levinson-Wal...** 3:9 113:15 132:9,10 161:8 162:20 163:20 168:19 170:3 179:13,15 202:16 203:5 203:12 204:6 207:16,20
**libertarian** 222:7
**liberties** 1:3 3:7 4:3 93:2 218:10 222:8 255:16
**liberty** 3:9 113:15 228:13 242:16
**license** 199:17 199:18,20 200:3
**life** 297:18 302:4 302:12
**lift** 204:1 207:16
**light** 16:2,13,21 130:13 135:3 135:12 275:18
**likelihood** 40:2 94:12
**limit** 17:19 196:12 206:22 213:12 238:9 246:18
**limitation** 123:20 196:14
**limitations** 81:4 126:5,19 129:2 131:18 185:22 240:9 245:22
**limited** 63:5 68:16,21 137:4 184:3 191:3,13 220:8 225:7 234:16 240:5 257:5
**limiting** 197:22 198:4 200:12 201:9 203:16
**limits** 31:9 79:20 169:10 169:12 185:8 203:8 207:6 214:19 246:12 255:13 289:22 291:11 306:7
**line** 56:17 79:22 119:20 138:12 201:15 216:22 229:18 282:16 288:16
**lines** 41:20 57:15 58:8 168:1
**link** 154:14
**linking** 235:11
**list** 81:11 208:13 309:22
**listen** 115:17
**literally** 123:10 161:18,20 162:14
**Litt** 2:17 8:8,10 21:16 24:1,22 34:13 35:14 39:12,17 48:6 48:13 49:9 53:7 63:15 64:9 69:8 70:11 75:7,10 80:6 84:7 96:22 97:22 98:2 99:8 101:14,21 102:6,20 103:1 103:4 104:13 105:11 107:8 107:15 112:11 112:18,20
**Litt's** 14:15
**little** 19:4 20:17 23:19,21 24:20 25:1 28:19 30:7 39:18 41:17 45:6 61:2 80:3 82:7 89:1 93:6 98:20 104:15 105:7 147:16 149:2 159:4 171:7,13 181:19 185:2 189:7 191:1 195:3 204:18 223:13 253:1 257:2 266:17 291:16 293:8
**live** 263:10,22
**lived** 99:22
**lives** 220:1
**Livingston** 1:22 313:4,15
**local** 239:4
**localize** 228:17
**located** 4:7 8:3 37:11 40:10,20 40:22 41:6 49:21 52:17,21 73:21 114:15 176:19 231:8 231:10
**location** 60:8 114:10
**logical** 124:19
**long** 17:19 124:17 125:2 127:6 130:13 181:20 185:16 230:5 233:10 272:16 280:1
**long-lasting** 235:12
**long-standing** 213:18
**longer** 73:14
**look** 16:16 24:4 29:20 30:2,5 32:14,15,17 33:18 49:13 65:1,16 68:5 68:13,14,15 80:22 81:19,20 83:2 92:17 93:1 111:2 119:12 130:20 140:22 142:2 158:2 159:11 165:17 173:4 178:14,19 188:10 193:21 194:20 198:16 242:19 249:13 256:5 257:15 258:2 271:5,8 291:20 292:18 293:22 294:1 299:10 308:4
**looked** 121:15 141:10 239:6 255:1
**looking** 50:12 65:8 113:21 161:18,20 200:6 202:8 242:9 266:22 292:14 304:15
**looks** 144:16 149:16 206:6
**loop** 192:21
**loopholes** 97:15
**loose** 204:4
**loosely** 126:4
**losers** 275:16
**losing** 233:9
**loss** 219:17
**lost** 71:13 192:9 273:16
**lot** 36:14 43:2

44:6 68:8 75:7 75:11 76:7 94:7 99:14 105:20 143:21 184:21 195:8 213:16 222:16 226:22 252:22 277:1 279:14 279:16,18 291:14 310:3
**lots** 215:17 216:14
**louder** 44:12
**loudly** 238:18
**Lovells** 3:22 209:18 238:4,6
**lunch** 6:20 209:2
**Lynne** 1:22 313:4,15

**M**

**magistrate** 141:1,4 155:22
**magistrate's** 140:13
**magnitude** 93:17
**mail** 7:12
**main** 133:2 134:22 226:13 260:3 281:16
**mainstream** 291:19
**maintain** 237:4
**major** 254:22 255:1
**majority** 42:4 150:5
**makers** 65:14 103:5 269:7
**making** 5:6 8:8 20:4 22:17 34:20 43:12 88:6 124:20 145:17 165:8 214:6 222:6 266:15
**malicious** 108:10
**managed** 84:8
**Manfred** 252:6
**mangle** 104:15
**manipulates** 231:7
**mankind** 233:10
**manner** 223:7 224:3
**manufacturer's** 179:6
**March** 1:10 4:6 4:10 7:12 312:10
**Marco** 225:9
**market** 241:15
**marketplace** 218:18
**Marshall** 277:11
**Mary** 214:8
**Maryland** 313:5
**mask** 109:11
**masked** 106:8 106:12 107:7 107:13
**masking** 106:10 106:13,17 109:16,18
**mass** 59:13 270:10 285:7 302:8,15
**massive** 175:1 241:13
**match** 208:4
**matching** 208:6
**material** 33:19 33:19 62:6 88:9,21
**materials** 32:15 32:17 41:18
**matter** 28:15,16 72:14 78:5 118:12 174:8 176:15 194:2 215:19 226:14 254:17 262:9 266:14 298:4 300:7 306:20
**mattered** 139:8
**matters** 21:17 23:11 119:20 138:11 141:1 286:9
**Max** 3:20 209:16
**Mayflower** 1:16 4:7
**McLeod** 214:8
**mean** 24:21 38:3 41:9 44:2 48:5 49:9 50:3 51:21 61:2 67:13 68:14 74:19 76:6,13 78:4,11 85:9 85:19 87:21 91:5 96:8,9,19 102:15 104:5 107:1,12 109:13 125:18 137:17 142:22 146:7 151:13 151:15 152:11 158:12,19 161:8 168:5,8 180:16 181:7 182:10 183:10 186:10 193:4 199:21 202:1,5 202:7 207:20 224:13 227:5 227:17 229:2 246:5,5 248:12 248:16 250:20 254:4 267:6 268:15 269:12 270:17 279:2 279:17 285:14 286:11 292:12 292:17 295:13 295:18 296:4 297:8 298:10 298:22 299:5,9 305:9 306:15
**meaning** 39:9 55:19 58:2 134:20 270:1 289:11
**meaningful** 123:19 308:16 308:22
**meaningless** 270:5,7
**meanings** 39:1
**means** 20:19 25:9,11 38:19 41:9,11,14 44:2,17 51:14 52:8 53:5 55:21 73:14 78:21 102:17 103:3 104:7,8 104:9,11 105:8 105:9,12 106:22 133:12 151:19 152:1 171:3 179:1 181:15 217:7 224:16 227:15 229:1 249:1 265:10 270:4 285:2 306:18
**measures** 151:20 232:21 256:20
**mechanism** 201:11
**mechanisms** 98:7 131:3 240:7
**medal** 263:6
**media** 6:2 64:5 120:8
**Medine** 2:3 4:2 4:5,20 13:20 17:2 18:2,8,19 19:11 20:1 35:7 43:14 50:4 53:2,16 54:12 55:18 56:12 77:10,16 78:7 85:4 86:11 88:10 89:1,19 90:3 90:10,19 91:1 91:12,17,19 92:1,15,21 106:2 112:22 113:8 116:16 120:17 125:6 132:8 136:20 142:19 152:12 160:15 167:14 168:13,16 175:16 177:6 179:13 181:6 182:6 189:17 195:21 200:14 207:9,14 208:21 209:6 218:4 223:9 230:10 238:1,3 242:20 247:1 247:15 248:19 254:19 255:7 255:15 260:6 260:12 265:22 271:21 274:6 275:7 276:22 277:15 283:17 295:5 301:3

305:2 306:12 307:5,15 309:6 312:2,18
**meet** 142:16
**meeting** 180:7 198:3
**meets** 21:13 274:18
**member** 7:5 100:5,5 239:16 241:8,10,13
**members** 2:1 4:12,13 6:8 7:3 7:10 36:9 100:11 207:10 210:4 218:6 220:20 312:7
**memo** 223:21
**memorandum** 234:6
**mention** 110:6 134:5,21 202:17 277:7
**mentioned** 43:1 49:17 57:13 60:16 61:20 62:15 68:19 73:8 74:5 83:22 102:6 109:7 118:15 118:22 136:4 146:14 152:18 161:11 236:5 259:18 261:14 272:7 304:4
**merely** 122:22 124:11 134:5 288:3 307:3
**merit** 76:11
**message** 48:12
**messages** 190:19
**met** 72:11,19 104:2 116:11 215:10 278:17
**metadata** 47:22 49:17,22 66:11 66:12 157:7 190:12 227:10
**methods** 98:11 206:14 277:3
**metric** 68:3
**microphone** 266:6
**Microsoft** 191:7
**midway** 288:13
**Milanovic** 225:10
**military** 308:10
**millions** 124:1
**mind** 6:6 33:3 34:12 126:13 128:12 138:10 196:5 299:11 308:20
**mine** 261:15
**minimization** 9:9,18 12:7,21 15:16 16:13 17:3,5 18:2,4 18:10,13,20 19:13,18,20,22 21:6,12 22:8 26:20 30:17 45:3 79:5 86:8 86:17 94:17 95:13 100:17 101:4 103:3,18 104:7,8,9,10 104:14,22 105:2,4,6,18 105:22 107:9 107:18 109:5 109:21 112:12 112:16 114:13 117:14 119:11 119:14 122:3 135:19 178:21 180:4 186:1 203:14 205:8
**minimize** 9:20 88:8 104:16 131:22
**minimizing** 87:3
**minimum** 23:15 136:12 310:2
**Minneapolis** 103:15
**minute** 204:9 295:13
**minutes** 116:20 172:6 207:10
**mischaracteri...** 10:4
**misconception** 10:4 41:2
**misimpression** 76:21
**misleading** 242:3
**misperception** 56:4 282:20
**mission** 18:14 19:7 27:4
**missions** 105:1
**mistake** 100:21
**mistaken** 111:2
**misunderstan...** 36:14
**mix** 6:21
**mobster** 115:12
**model** 255:4,8 255:11
**moment** 25:21 44:9 106:18 115:5 146:15 146:19 147:3 192:3,4 242:22 267:1
**money** 84:21 85:16
**monitor** 250:7
**monitoring** 171:12 197:4 290:18
**monitors** 307:9
**Monroe** 179:7
**month** 124:17
**months** 210:16
**morning** 4:2 20:3 27:8 167:1 182:16 188:6
**morphing** 162:12
**motion** 205:3
**move** 32:18 182:10 196:4,7 310:17,20 311:4 312:14
**movement** 73:18 175:7
**movements** 125:4 174:19
**moves** 128:21
**moving** 29:8 266:18
**multinational** 284:13 301:12
**multiple** 119:7
**multipurpose** 257:9
**mutual** 238:21
**mutually** 218:12 218:13
**mysterious** 76:21 77:7
**MYSTIC** 124:15,19 190:16

**N**

**name** 57:14 106:19 108:5 108:12 179:1,6 179:6
**names** 198:8
**narrow** 36:17 86:19,22 102:9 152:6 186:18 279:20
**narrowing** 208:3,9
**narrowly** 228:5
**nation** 13:16 34:22 103:6
**national** 2:15,18 2:20 3:10,18 7:21 9:1 11:10 35:15,17 42:20 59:21 64:18 65:10 93:1 113:16 119:19 139:19 140:16 141:2 161:22 209:14 210:10 210:12 218:10 228:4 230:5 232:7 234:3 235:19 236:12 236:22 237:10 240:12,16 241:20 242:12 245:2 253:9,10 253:14,15 254:13 255:17 258:6 272:11 272:16 273:9 275:20 277:12 286:2 287:9 300:2,9,14 301:19 305:15 306:3
**nationality** 133:7 162:8 217:18 233:15 237:15
**nationally** 305:16
**nationals** 210:7 210:18 290:2

**nations** 284:15 289:10
**natural** 203:15
**naturally** 41:14
**nature** 26:19 46:15 47:12,15 47:15 49:14 65:9 94:10 105:3,5 144:9 191:13 234:20
**Nazi** 225:6,8 256:9
**necessarily** 55:7 55:15 98:19 151:18 153:1 157:18 185:21 227:4,12 228:21 271:13 271:16 274:4 286:2 287:8
**necessary** 17:14 25:5 29:16 31:22 50:1 79:3 107:21 108:5 109:3 175:11 183:17 227:22 236:16 279:22
**necessity** 28:15
**need** 16:6 23:6 23:20 34:20 67:4 84:9 85:2 85:3 94:14 103:5 104:19 108:4 109:21 125:19 127:17 128:17 131:13 142:16 147:2 169:9,12 170:19 171:18 173:11 185:15 185:20 193:5 217:10 239:22 254:15 300:16 308:15 311:1
**needs** 9:19 16:3 18:17 23:16 31:1,10 59:14 72:20 79:9 100:10 145:8 151:18,20 262:21 276:7 279:3,4 300:3
**negotiated** 211:19
**negotiating** 212:17 214:13
**neither** 6:8 12:4 114:14 140:22 211:10 250:9
**networks** 138:3
**neutral** 140:5 141:4 155:22 241:3
**never** 11:20 35:9 70:7 101:5,6,7 161:3 205:5 251:17 260:5,5 290:22 299:11
**new** 32:9,20 72:9 161:16 198:16 245:19 303:2 310:13
**news** 120:8
**nexus** 147:4,6 198:13
**NIST** 222:19
**non** 300:15
**non-arbitrary** 227:22
**non-citizens** 215:15 217:9
**non-intelligence** 44:6
**non-public** 9:21 231:8
**non-targeted** 109:15
**non-U.S** 8:2 9:11 14:3 15:6 16:11 17:1 37:11 40:9,19 40:22 41:6 43:19 49:21 52:17,21 53:12 55:11,13 58:14 60:2,4,12,13 71:16 72:4 74:1 79:20 80:11 81:15 82:13 90:13 91:10,20 92:2 92:5 96:10 103:14 109:12 110:17 111:6 129:7 148:8 176:19 177:7 177:18,20 178:2 182:22 237:11 243:21 252:12 253:16 253:19 278:2,4 278:14 280:7 295:11
**nonsensical** 166:5
**norm** 216:13,17
**normal** 32:22 197:19 264:2
**normally** 32:13 33:18 87:5
**norms** 215:20 231:12
**notarial** 313:12
**Notary** 313:4,16
**note** 12:13 239:13 282:8
**noted** 8:17 238:20
**notes** 145:15
**noting** 126:7
**notion** 40:1 204:14 293:8
**novel** 21:22 158:5 204:19 226:11 227:3 244:17 269:4 269:12,13
**Nowak** 252:6
**NSA** 17:18 18:3 18:15 19:2,6 28:3 30:6 31:16 35:14 41:19 43:12,16 44:17 47:7 61:6 62:8 72:20 78:18,22 85:21 86:17 106:17 107:3 109:10 114:11 114:16 119:2 119:10 124:3 124:14,16 134:15 147:17 147:18 177:19 178:4 191:5 203:19 210:18 211:7,12,12 214:19 215:7 215:11 216:14 218:18 219:1 238:11 276:16 294:2
**NSA's** 45:1 79:7 122:3,7,20 123:14,20,22 124:3
**number** 11:19 15:21,21 34:15 48:17,21 51:5 52:3,3 54:8,15 54:18,21 77:19 93:18 103:10 103:13 117:9 219:13 270:10 270:15 272:5 272:19 273:20 292:14 293:5
**numbers** 9:4 10:8 25:11 26:1,10,11 48:18 52:6,11 52:12 71:6 219:14 221:20
**numerous** 100:4
**NW** 1:16 4:8

**O**

**O** 140:20
**o'clock** 113:5
**Obama** 214:1 214:16 223:22 253:22 254:1 291:7
**Obama's** 217:14
**object** 225:1
**obligated** 293:18
**obligation** 21:2 42:12 53:22 74:11 85:13 87:14 178:5,10 179:9 215:14 224:8 227:16 229:21 248:8 250:20 271:8 271:10 289:14 290:3
**obligations** 98:22 212:4,13 213:12 216:4 218:2 223:16 227:5,20 230:14 231:20 251:16 308:8
**obliges** 178:15
**observations** 126:11 277:21
**observer** 140:5

**observers** 277:17
**obtain** 29:17 67:18 115:16 122:21 136:1
**obtained** 7:19 69:22 70:9,10 70:19 115:5 122:12 141:7 142:1 146:16 171:14 175:20 180:13 181:16
**obtaining** 8:5 146:20
**obtains** 38:5
**obviously** 33:4 43:5 68:7 82:8 82:15 85:11 106:22 135:8 159:20 161:9 174:4 187:20 203:18 208:6 223:19 238:15 239:22 242:14 268:2 275:20 276:4,20,22
**occasionally** 99:16
**occur** 12:11 72:5
**occurred** 84:6 138:2 139:6 147:7
**occurring** 131:16
**occurs** 12:14 25:6 27:22 28:1,4 39:3 42:17 146:16 155:18 170:16 242:14
**October** 93:12
**off-cycle** 23:13
**off-limits** 32:21
**offer** 220:18 222:6 228:18 309:9 311:3,5
**offered** 222:3
**office** 2:17 11:10 42:19 64:18 87:15 88:6
**officer** 4:11 111:6 140:14 156:1
**official** 249:7 252:5 254:14 278:5,19
**officials** 6:12 85:13 159:12
**oh** 40:2 56:12 71:12 155:7 156:1 171:9
**okay** 23:17 29:20 39:1 47:18 50:22 51:21 53:4,21 54:12 57:16,21 60:3 62:21 65:1 78:8 79:16 82:20 85:1 92:10,21 93:19 96:5,13 97:4,9,9 142:22 154:12 156:17 157:15 160:17 177:13 179:18 186:2 187:3 193:16 201:15 202:5 204:8 247:15 250:13 251:21 281:21 295:7 308:12 309:4
**old** 181:12
**older** 137:20
**once** 22:14 23:1 23:3,15,16 28:5 29:15 30:21 37:15 42:13 60:3 74:10 141:22 146:4
**one's** 53:10
**onerous** 172:13 185:2
**ones** 46:13 76:16 280:14
**ongoing** 219:1 294:7
**online** 7:11
**open** 200:5 206:12 220:3 220:15 259:11 260:18 284:12 311:17
**opened** 161:15
**opening** 4:17 8:9 136:21 152:19 209:20
**operate** 79:4 175:2 177:5 183:1
**operated** 1:6 183:12
**operates** 20:17 183:7 200:17
**operating** 86:7
**operation** 45:17
**operational** 18:17 28:20 29:2 32:4 48:14 54:7
**operative** 51:2 224:7
**opinio** 263:2
**opinion** 75:2,18 76:3 77:7 93:13 94:8 116:3 134:13 140:8 163:5 234:11 268:15 288:6 293:4
**opinions** 20:12 21:10,10 75:13 76:7,14,15,19 77:2 78:4 206:10 287:17 287:20
**opportunity** 8:11 50:6 84:14 113:20 120:20 125:8 136:18 223:11 242:17
**opposing** 182:8
**option** 208:6
**oral** 239:8 252:9
**order** 4:16 6:4 31:20 34:22 53:20 67:14 70:21 81:7,12 93:17 95:17 123:6 136:14 145:2 151:16 179:9 180:20 188:12 206:5 221:1 229:16 237:3 284:22 299:21
**orders** 53:18
**ordinary** 175:2 262:22
**organization** 308:15
**organizations** 251:11 278:6
**organize** 31:13
**organized** 29:12
**original** 50:3 195:6
**originally** 183:21
**ought** 206:11 217:8
**outcome** 313:11
**outlier** 225:12
**outnumbers** 135:7
**outset** 149:12 164:9 238:3
**outside** 8:4,19 9:12,15 10:15 10:21 39:20 40:4 45:13 69:14 71:17,17 72:2 73:11 83:10,11 88:19 88:21 89:10,11 89:15,21 90:1 90:9,12,15 97:21 129:8,13 129:19 131:1 137:13 151:17 159:18 162:2 162:17 176:19 180:18 210:7 211:17 215:4 216:6 219:4 224:5,18,19 233:3 235:19 241:21 245:9 245:12 246:7 246:13,19,22 248:4,10 258:11 277:14 278:16 281:9 291:18 308:10
**outweighs** 135:7
**over-collection** 170:16
**overall** 22:14 276:2
**overarching** 53:20 72:7
**overbroad** 286:12 287:10 287:14
**overbroadness** 287:5
**overhear** 115:13

160:4
**overheard** 159:2 160:13
**overhears** 158:21
**overlooked** 166:14
**overseas** 15:6 52:17,22 53:12 55:11,13 60:4 60:13 73:21 89:3 91:8,15 91:21 92:5,10 103:9,14 126:3 126:9 128:10 128:14 130:2,6 130:12 131:8 131:15 132:1 137:5,22 138:1 147:7 183:22 184:3 206:22 272:22
**overseeing** 150:11
**oversees** 212:1 292:3
**oversight** 1:3 4:3 11:5,6 61:1 85:1,2,10 86:7 98:7,22 132:2 160:11 222:1 240:2,6 241:9 274:8,9,11 292:4,5,10,17 292:22 293:1,3 293:9,21 294:7 295:3 308:16 309:1 310:4
**overview** 8:13 10:3

**P**

**p.m** 312:21
**page** 96:18
**Paltalk** 191:8
**panel** 2:9 3:1,13 6:16,21 7:4 8:7 8:9 14:7 113:1 113:6,9 115:4 117:8 118:15 119:1,9 132:14 132:15 135:2 135:16 146:14 147:10,16 161:14 166:22 171:8 173:20 175:19 178:11 182:9 187:10 191:2,16 196:17 209:3,8 260:16 279:10 292:12 294:5,6 294:11
**panelist** 136:22 207:1
**panelists** 4:22 7:5 35:10 125:10 167:1 176:14 188:6 191:18 208:22 209:19 244:1 312:7
**panels** 6:11,19 152:14
**paper** 238:7,19 239:5,10,13,19 240:8 241:17 242:18 275:14 277:8 282:19 310:21
**paradigmatic...** 161:6
**paragraph** 252:8
**parallel** 118:2,6 118:13
**parameters** 109:1,22
**parcel** 280:17
**pardon** 116:19
**parliament** 220:10 239:15 241:7,16 257:18 276:11
**parliamentary** 257:22
**parsing** 38:6,11
**part** 10:22 22:7 22:12,17 27:9 36:6 57:21 64:15,19 69:2 77:12 107:8,9 112:12 135:1 138:13 143:5 145:6 150:10 161:10 192:12 203:15 205:4 211:11 267:10 270:1 273:12 280:16,17 297:9,19 311:16
**parte** 20:18 21:19,21 206:8
**participate** 260:17
**participating** 5:1
**participation** 69:17
**particular** 14:19 23:11 24:9 26:10,16 28:2 29:7 41:16 46:18 50:13 51:20 54:11,20 54:20 55:16 59:2 61:10 63:18,20 64:16 65:17 66:4 67:16 78:19 79:16 88:3 89:12 95:13 98:21 104:22 116:8 117:4 119:21 120:3,9 123:18 154:7 154:21 174:4 178:16 179:5 197:8 220:11 246:1 272:17 291:20 305:20 306:2,3 308:21
**particularity** 14:19 193:10 199:2
**particularized** 37:5 157:19 193:11 200:21
**particularly** 86:16 100:10 114:4,22 132:20 219:6 221:12,19 226:16 254:2 272:2 273:22 275:19 276:8 311:14
**parties** 132:5 249:15 313:10
**partly** 36:19
**partner** 3:15,22 209:11,18 238:4
**partners** 112:4 112:9 272:22
**partnership** 300:13
**parts** 162:13 176:11 208:14 263:15
**party** 20:20 21:1 106:18 112:4,8 180:21 212:7 215:4 234:14 264:19 307:4
**party's** 213:12 215:1
**pass** 108:12 243:2 307:2
**passed** 12:9 84:16 118:4
**passing** 108:6 229:2
**Pat's** 58:9
**Patricia** 2:5 4:15
**PATRIOT** 5:11
**pause** 223:8
**pay** 131:21 277:5 282:15
**payments** 153:14,14
**PCLOB** 5:8 66:18 136:1 218:6 221:6 284:18 301:13
**PCLOB's** 4:5
**PCLOB.gov** 7:9 312:13
**Peace** 305:1
**pen** 156:7,8,10 157:9
**penalties** 142:16
**people** 15:13 33:13 52:5 60:2,14 83:7 89:9 133:16 159:18,19 160:13 163:15 166:18 168:6 168:17 171:15 175:2,6 195:8 207:6 215:2 216:6,14,17 225:4 245:20 246:7,22 247:9 247:10 249:2 252:4 263:2,16 266:13 270:11

270:15 279:19 280:10 291:8 296:19 302:8 307:21 311:13
**peoples** 50:12 283:2
**percent** 36:13 39:19 40:2,3 40:21,22 43:9 93:16 168:21
**perception** 97:13 157:16 284:14
**perfectly** 217:22
**period** 37:1 44:18 47:9,11 47:14 93:22 94:20 95:21 103:7
**periodic** 11:13 74:12 84:1 214:6
**periodically** 42:12 64:7
**periods** 47:7
**permanent** 8:3 125:3 174:18
**permissible** 14:14 54:21 56:20 90:16 98:2 285:21 300:1
**permissibly** 175:21
**permission** 262:19
**permit** 7:6 89:14 107:19 122:13,20 231:13 260:8
**permits** 8:1 121:3 231:17
**permitted** 40:5 59:5 96:1 106:7 124:6
**person** 9:15 14:3,5,6 17:8 17:13 19:5,21 28:18 30:12,14 31:21 36:21 37:2,19 40:9 40:20,22 41:6 41:13,21,22 43:19 48:3 51:9 52:17,21 53:12,13 55:11 55:13 56:6 58:14 60:4,8,9 60:13 71:16,16 71:19,20,20 72:4 73:11,12 74:1,2 78:10 81:18,19 82:16 89:4,12,14 90:1,12,14,15 90:22,22 91:9 91:10,14,20,20 92:2,5,8,9 94:12 96:8,9 96:10,10 101:3 101:8,19 103:11,13,14 106:3,19,20,21 107:20 108:16 108:19 109:15 111:5,6 114:8 114:14,18 131:1 137:1 138:11 142:7 148:8 149:3 161:7 162:17 162:19 164:1 164:21 165:15 165:15,18,19 165:20,21,21 166:3 167:18 172:11,16,21 173:8 175:17 176:5 177:3,7 177:8,10,17,18 177:21 178:6 179:4,5 180:2 181:13,14 193:5 244:6 254:9 271:1 278:3,5 297:15 297:17 302:15
**person's** 40:4 51:12,17 55:4 92:2 109:12 297:18,22
**personal** 81:8 81:14 217:21 228:12 242:15 242:16 298:17 298:18
**personally** 150:22 179:3 254:4,5
**personnel** 86:5
**persons** 8:2 9:11 9:22 10:14,14 12:2,11,17,19 13:2 14:9,13 15:6,10 16:5 16:10,11,20 17:1,10 37:11 39:19 40:13 43:17,20 49:21 54:16,17 60:2 60:12 79:20,22 80:11,12,12 81:6,9,15 82:13,14 89:16 89:21 90:9 97:19 102:12 104:19 109:17 109:19,22 110:17 112:17 133:6,6 142:18 152:5 161:3 162:1 176:18 176:19 178:2 182:22 213:2 214:19 217:16 217:19 229:11 230:17 237:11 243:21 245:8 252:12 253:16 253:19 278:14 280:7,7 295:12
**perspective** 2:10 15:18 43:7 48:7 138:15 144:5 194:21 195:1 218:11
**persuade** 21:3
**persuasive** 176:1,2 268:13
**pertain** 94:5
**pertains** 237:16 295:18
**pertinent** 108:14
**Peter** 5:5
**phenomenon** 283:14
**philosophy** 124:12
**phone** 25:11 26:1,10,11 51:5 52:3,3,6 52:11 54:8,15 54:18,20 71:5 73:10,13,21 96:9 115:17 124:16 138:2,6 156:11 174:17 177:9 191:21
**phonetic** 140:3
**phrase** 26:7 106:19 122:16 212:19 215:1 270:2,5
**phrases** 147:20
**physical** 225:19 227:13 234:15 271:2
**physically** 128:10 138:1 296:13
**pick** 13:22 167:15 255:20 275:15 295:6
**picked** 133:13 170:1
**picture** 40:7 88:5 302:12
**piece** 46:18 170:9 189:19
**pieces** 41:20,22 46:21
**pillaging** 224:19
**pioneers** 303:4
**piqued** 148:20
**Pitter** 3:18 209:13 213:15 223:9,10 245:17 247:15 247:16 250:14 250:17 254:21 267:6,17 268:9 268:15 269:3 270:7 271:5 277:17 278:22 279:2 280:12 281:1,5,22 284:20 285:19 286:11,20 287:15 288:3,6 291:13 292:10 292:21 293:20 294:10,21 298:8,13,22 299:9
**place** 15:16 16:14 31:15 59:3 94:18 98:7 124:18 152:2 160:1

166:20 169:11 171:15 179:12 201:20 214:19 218:2 220:22 221:13 227:19 233:4,15 248:15 273:18 275:3 278:2 281:13 284:11 306:17
**placed** 128:13 211:11 237:10
**places** 210:5 222:2
**Planck** 3:20 209:16
**plans** 67:21
**plate** 199:17,19 199:21 200:3
**play** 205:11
**please** 4:17 63:22 311:6 312:16
**pleased** 113:9
**pleasure** 230:13 237:20
**plenty** 280:2
**plot** 169:2,7,19
**plots** 66:22
**plotting** 168:3,4
**plus** 232:7
**point** 10:13 22:2 22:16 30:11,20 34:14 42:10 44:5 46:14 47:4 48:13 49:12,19 60:2 68:18 69:10 72:8 80:7 82:5 85:5 88:14 89:7 97:13 99:20 102:11 103:17 110:10 110:15 112:12 115:10 121:17 124:9 129:1 132:13 138:20 142:5 144:17 146:14,19,21 147:1,9 148:4 153:22 154:1,2 154:6,9 157:6 157:21,22 165:8,12 166:11 183:9 183:11 192:1 195:4,14 207:13 214:15 216:13 221:7 227:5 239:18 244:14 255:4 258:2 262:5 274:1 277:8 284:5,7 289:1 303:9 305:5 306:14
**pointed** 140:20 225:11
**pointing** 180:18 180:22
**points** 8:15 10:3 27:12 30:9 85:7 88:6 110:5 117:4 125:14 170:4 251:3 289:15 311:7
**Poland** 225:9
**police** 257:1 303:18 304:5
**policies** 220:3 239:20 282:16
**policy** 3:14 5:18 7:2 24:5 28:16 28:16 31:9 65:14 103:5 209:9 215:19 217:12,15 229:8 232:4 236:20 237:18 245:21 252:10 254:17 266:14 266:22,22 269:7 289:5
**political** 117:18 119:20 132:3 157:12,17 211:1 223:17 233:21 267:8 286:14 303:7
**Porter** 3:15 209:11
**portion** 188:2 189:10,11
**pose** 7:3 167:16 199:6 232:10 253:10
**posed** 155:4 309:11
**poses** 282:14
**position** 6:9 126:21 135:11 140:6 152:20 190:10,14 193:3,14 211:16,18 212:17 214:3 224:1 229:19 237:18 244:13 247:17 249:1 252:3,16 267:7 278:15 283:5 303:3
**positively** 178:20
**possessed** 127:22
**possesses** 127:13
**possession** 31:6 34:22 37:16 192:7
**possibility** 45:15
**possible** 5:7 32:19 45:1 46:1 81:3 88:8 166:14 257:4 312:4
**possibly** 181:19
**post** 114:21 118:17 124:13 173:5 174:10
**post-targeting** 120:14
**post-World** 225:2
**posted** 7:9 312:13
**pot** 33:16
**potential** 103:1 156:11 261:17 285:4
**potentially** 33:11 87:16 89:3 94:2,11 132:13 153:10 156:13 203:16 208:19
**power** 29:7 116:6,7 125:22 126:6 127:7 128:1,6 131:17 141:13,13,21 141:21 149:2,4 149:4,5,9,10 173:22 183:1 183:14 195:2 204:2 207:17 207:18 208:8 215:2,7 224:13 234:13 244:15 244:20 245:3 245:13 285:5 285:11 287:21 296:8,11,12 297:16
**powers** 67:21 127:1 256:15 256:22
**PPD** 110:16
**practicability** 49:11
**practical** 136:11 262:9 280:19 281:8
**practicality** 170:14
**practice** 19:11 104:6 123:1,4 123:9 128:21 150:8 214:15 238:5
**practices** 125:16 239:15,20 242:8,9 260:22 276:13,16,17 277:18 278:10 280:9
**pre** 173:5
**pre-FISA** 150:18
**precedent** 15:8
**precise** 93:15 193:19
**precisely** 150:13 285:14 288:17
**predate** 150:4,6 186:21
**predecessor** 75:17 212:2,11
**predecessors** 128:5,13
**predicate** 25:5 25:18 79:3
**prefer** 37:8 202:9
**preference** 208:9
**premise** 87:13 149:22 297:9
**premises** 231:20

**prepare** 312:1
**prepared** 63:16
**prerequisite** 116:10
**prescriptive** 84:18
**presence** 243:10
**present** 4:12 21:21 154:22 242:18 293:12
**presented** 234:6 307:11
**President** 3:16 5:9 47:18 79:17 80:21 81:12 85:12,19 110:15 127:12 127:13,18 140:13,22 150:22 195:2 195:11,16 209:12 217:14 229:7 252:13 254:1
**President's** 10:22 24:4 125:22 127:1,9 131:16 172:8 172:14 202:13 203:19
**presidential** 126:6 217:14 229:8 237:13
**presidents** 127:6
**presiding** 4:11
**press** 86:13 88:5
**presumably** 82:9 170:6 283:7
**presume** 23:14 122:8
**presumption** 280:6
**pretend** 33:1 222:5
**pretty** 163:21
**prevailing** 234:11
**prevent** 174:16 236:20
**prevented** 256:10
**previous** 117:8 146:13 152:21 171:8 178:11 191:16 195:16 206:17 238:19
**price** 131:21
**primary** 132:17 143:8 151:1 208:17
**principle** 80:17 236:11,17 239:18 259:15 262:14,20 265:4 281:17
**principles** 109:3 220:19 221:9 279:22 289:5,6 304:22
**prior** 62:8 72:10 118:19 127:20 128:4,16 130:17 139:4 156:15 157:18 194:13,18 195:19 198:2 201:13 204:10
**priorities** 65:1,3 65:11
**PRISM** 25:20 26:13,17 31:17 37:10 47:8 48:4 56:10 57:18 63:3,7 70:7,8,12 78:11 93:9,22 101:12 109:15 172:22 187:7
**privacy** 1:3 4:3 8:20 13:2 16:4 17:21 27:4 47:17 93:2 94:2,5 114:20 121:7 123:5 131:12,22 185:18 190:9 190:13 198:12 210:19 211:5 215:15 216:10 217:6,20 218:1 225:16 226:4 227:10,14 228:12 229:4 229:21 232:13 233:1 234:19 235:8,15 236:2 236:4,7,19 238:5 239:21 242:15 247:20 248:10,17 253:8 254:12 254:17 255:16 259:3 271:17 276:20,21 278:13 280:16 282:6,8 289:22 295:13,16,20 295:20 296:17 296:22 297:6 298:1,3,10,15 299:2,12,15,17 300:19 302:1,2 302:6 304:7 305:15
**private** 6:22 58:5 155:15 156:12,13 240:22 254:3 297:18 302:12
**privilege** 86:13 87:1,6 88:10 88:12 118:14
**privileged** 87:17 87:22 88:9,21
**pro** 99:2,6,12,18
**probable** 116:5 118:6 124:7 141:11,19 150:20 155:19 156:9 157:19 160:8 172:10 172:16 173:1 173:16,17,19 174:3,4 180:8 193:6
**probably** 24:2 24:22 66:5 74:8 87:11,19 116:17 160:2 171:20,21 185:19 200:15 208:10 252:2 280:2,3 286:16
**problem** 36:20 147:8 181:3,4 188:5 226:2 247:12 252:10 263:13 267:10 276:3 292:12 295:3
**problematic** 294:20
**problems** 172:20
**procedural** 131:2 171:10 185:22
**procedure** 90:4 140:12 176:3 176:13 199:21 203:1
**procedures** 9:9 9:10,18 12:7 15:16 16:13,21 17:3,6,6,9,20 18:3,5,13,20 19:13,22 21:6 21:9,13 22:9 22:12,20 23:7 26:21 27:1 30:17,17 32:3 43:1 45:3,21 79:5,7 80:22 86:9,17 87:12 88:15 94:17,21 95:1,14,15 98:11,12 100:17 101:4,5 104:16 105:18 107:10 109:6 109:16,19,21 111:20 112:2,3 112:9,13,16 117:14 119:11 119:13 122:4,7 122:10,20 123:14 124:3 135:20 148:17 174:7,12 178:21 180:4,6 203:14 205:9 205:10 281:13 293:22 295:2
**proceed** 4:21,21 209:20
**proceeding** 21:1 204:16 297:19
**proceedings** 4:1 21:19 204:13 237:1 313:6,8
**proceeds** 236:8
**process** 11:3 20:8 22:6,8,12 22:18 25:14 32:12 33:5 35:2 45:7 54:9 62:3,15 63:12 70:16,21 72:17 72:18 78:15

100:2 103:18 103:22 106:10 107:3 136:18 167:19 174:4 180:3 206:2,16 222:9 240:2,19 292:13 294:7 304:2,9 311:12
**processes** 274:13
**processing** 46:2 231:10
**produce** 9:5 104:19
**produces** 86:1
**professionals** 65:21
**Professor** 3:4,8 113:10,13 125:6 137:3 139:14 142:19 145:12,13 147:1 149:15 152:17 156:2 176:4 181:6 182:15 193:17 200:7 202:6 215:10 230:11 261:14
**profound** 123:4
**program** 1:6 3:10 4:4 5:11 5:12,13,16,19 7:8 10:12 14:2 22:14,16 36:15 36:16 37:6 49:14,16,16,22 50:3 57:18 62:7,12,18 63:18,20 64:2 64:7,13,16 65:20,20 66:9 66:11,11 67:8 67:11,16,17 68:3,13,16,18 69:1,1,5,9,11 69:12,13 70:6 70:15 71:7 74:20 75:17 76:5 79:2 83:2 97:6 100:10 113:16 157:8 170:11 187:12 190:16,18 191:4,13 216:15 243:3 243:19 274:11 274:18 293:21
**programmatic** 14:21
**programs** 5:10 6:14 63:12,14 64:15 66:8 67:18 69:3,7 83:4,7,16,18 83:20 84:1,5 84:14 85:16 99:1,21 118:4 170:7,8,13 211:13 230:15 232:3,17 233:13 235:1 252:19 269:10 272:1 275:12 277:2 308:17
**prohibit** 9:22 265:7
**prohibited** 264:20
**prohibition** 91:3 91:4
**prohibits** 90:8 123:13 264:16
**proliferation** 60:19 285:6
**proliferator** 53:13
**prominent** 225:10
**prominently** 234:21
**promise** 265:16 265:17
**promote** 6:4 235:22 300:6,8
**prompt** 23:7
**prong** 296:3
**proof** 114:7,10 176:16 177:19
**proper** 86:6 169:10
**properly** 135:9
**proportion** 190:21
**proportional** 228:1
**proportionality** 236:11,17 259:15
**proportionate** 279:22
**proposed** 128:20 213:1 272:4
**proposition** 196:13 197:22 200:13
**prosecution** 115:10,22 117:22 139:18 141:8 145:4,21 146:1,7 201:13 205:16
**prosecutions** 144:4 181:2
**prosecutor** 156:19
**protect** 13:2 17:10,21 34:22 230:3,3 232:22 240:15 281:14 285:3
**protected** 80:12 206:15 242:16
**protecting** 8:20 103:6 228:3
**protection** 60:11 160:12 184:13 230:18 232:20 233:7 236:2 258:3 264:15 276:14,20 304:20 305:7
**protections** 80:9 80:10 82:15 110:17 174:14 185:18 186:1 221:13 243:4 273:21 275:2 278:2,5,13 282:4 300:19
**protective** 230:19 232:21 233:9
**protects** 231:4
**protocol** 191:9
**provide** 5:8 81:3 111:22 132:2 136:1 226:18 237:11,20 239:4 242:4 273:15 308:22 309:10
**provided** 26:2 54:2 65:13 88:7 160:12 308:15
**provider** 51:16 52:2 53:21 137:11 238:14
**providers** 7:16 25:16 26:8 69:18,19 238:12 239:2
**provides** 81:8 211:3 272:21
**providing** 52:1 103:5
**provision** 88:15 89:21 90:8 106:15 136:2 215:13 217:3
**provisions** 69:4 112:3
**provocative** 82:22
**PRTT** 157:6
**pry** 297:5
**public** 1:5,15 5:9,17 7:10 57:22 70:14 75:3 77:12,14 77:21 78:3,6 79:8 83:16 84:2,9 87:10 87:10 93:7,10 94:8 95:2,15 106:9 112:7 113:3 135:6 154:17 221:17 227:1 228:13 231:12 243:18 258:9 279:12 293:16 294:16 311:16 312:8 312:12 313:4 313:16
**publicly** 32:2 93:11 112:3
**publish** 239:12 297:18
**published** 238:6
**pull** 192:14 280:9
**pulses** 303:17
**purely** 122:5,11 149:7 184:4,8 194:7
**purge** 45:2,6,7 45:18,18 82:1

101:19 102:14 102:19
**purged** 43:22 44:16 72:20 73:4 82:4 94:15 95:6 96:2 102:3,5
**purging** 44:1,17 45:16 58:9 72:18 202:1
**purports** 229:9
**purpose** 5:17 10:10 59:16 61:1,8 89:12 90:21 92:5 111:8,10 133:9 134:10 143:4,4 143:7,8,8,15 145:20 146:1,7 146:9,10 148:7 148:10,15,20 149:8 151:1 159:10,15,15 179:22,22 180:14 181:1,9 181:9 184:8 186:13,15 190:4 193:20 204:3 208:17 208:18 212:22 225:1 228:3 274:16 275:13 279:3 281:19 281:20 286:3,5
**purposes** 8:5 13:6 18:1 27:19 38:6,17 39:7,16 40:8 44:4 66:9,10 128:2,8 129:21 130:3 139:2,15 139:17 143:22 144:12 145:19 146:3 147:3 148:3 150:12 176:9,10 181:11 184:17 199:10 203:18 300:10
**pursuant** 1:6 7:16 12:16 26:3 30:22 32:12 70:15 131:16 193:1 221:18 223:6
**pursue** 33:15 45:5 61:9 66:14 149:19
**push** 149:1 293:7
**pushing** 301:1,2
**put** 62:1 94:19 115:16 140:5 192:3 219:14 269:20 274:8 288:13 305:19 309:21,22
**puts** 38:5
**putting** 73:19 188:20 278:1
**puzzled** 169:17

**Q**

**qualifies** 55:12
**quality** 68:7
**quantities** 134:7
**quarterly** 62:11
**queried** 27:17 45:16 196:14 198:1
**queries** 30:12,14 30:19 50:10
**query** 27:18 28:17 29:18 31:16,22 32:13 35:2 39:9,10 39:15 48:21 49:3 56:21 79:9 86:9 193:4 199:20
**querying** 28:6 31:3,9,12,15 39:8 47:21 57:5 79:1 196:11 197:13 200:2
**question** 14:7 16:8,15 26:22 31:8 37:21 40:7 41:19 45:19 49:5,10 49:11 62:2 63:2,21 64:4 66:22 67:3,6 67:13 77:11 79:17 83:1,6 92:14 93:3 97:12 98:4 100:17,18 109:14 111:15 117:8 127:12 137:8,16 143:10 150:16 154:13 155:4 157:14 158:9 158:19,20 159:22 160:20 163:19 164:16 168:21,22 169:9,15 172:12,19 174:20 175:15 177:1,12 179:17 182:18 186:3 187:17 187:19 189:22 190:8 191:17 193:16,19 196:1,9 198:19 200:5,16 201:4 204:9 206:17 207:13 219:10 228:7,9 243:22 249:4 250:13 251:21 252:8 252:21 254:20 255:6,19 258:7 259:9 261:5 263:19 264:7 266:1 267:12 268:13,20 269:13,17 270:22 271:3 273:2 274:10 278:12 284:19 288:22 291:13 292:7 295:8 296:3 298:7,9 300:19 301:5 303:8,10 305:19 308:13 309:8,11
**questioned** 241:12
**questioning** 35:8 93:20 163:14 209:21 220:10
**questions** 7:3,4 8:16 13:19 19:14 36:8 53:1 58:2,4,9 61:3 63:17 71:12 97:10 100:15 135:2 135:11,13,14 135:17 136:17 136:22 160:16 161:14,16 175:18 192:21 207:11 208:21 226:11 242:19 248:20 267:5 277:16 291:14 303:2,5,22 310:13,13
**quick** 73:2 85:9 105:15 111:1 195:22 204:9 204:14 207:13 306:13 307:16
**quickly** 82:21 147:10 191:1 201:7 251:22 281:4 282:2 308:13,13,19
**quirk** 89:8
**quite** 30:3 99:5 154:4 159:14 203:22 221:14 222:14
**quorum** 4:13
**quote** 43:22 106:4 211:3,6 212:22 213:10 214:8 216:9 228:8
**quoting** 140:2 148:12 160:21

**R**

**Rachel** 2:4 3:9 4:13 56:19 57:2 113:14 160:20 164:8 196:10 206:18
**radio** 195:5,6,10 195:12,13
**raise** 23:11 56:12 114:1 119:16 138:8 153:9,16 183:11 200:4 278:21 284:22
**raised** 19:14 27:12 117:22 135:17 171:22 200:19 284:20
**raises** 152:20 197:9

**raising** 136:9 165:20 278:4
**Raj** 24:22 28:1 35:13 36:19 43:7 60:5 61:19 102:6 108:22
**Rajesh** 2:15
**ran** 62:22
**random** 80:20
**range** 88:7 117:19
**RAS** 48:18
**rate** 43:9
**ratified** 211:2 304:5
**rationale** 54:13 59:19 69:2 150:7,9
**re-articulated** 211:20
**reach** 94:20 275:15
**reached** 272:18 276:3
**reaching** 226:8
**reaction** 256:8
**read** 71:1 92:16 151:7 182:17 188:1 285:1
**reader** 200:3
**readers** 199:18 199:19
**ready** 13:18 113:8 284:3
**reaffirm** 74:11 275:4
**reaffirmance** 249:18
**reaffirmed** 214:15 244:12 248:22
**real** 51:18 73:2 85:8 90:21 105:15 144:19 219:12 278:13 282:14,22,22
**reality** 33:8
**realize** 36:1 116:20
**realized** 101:7
**really** 27:8 28:10 36:10 45:17 52:5,6 60:5,7,11 62:2 63:21 67:13 68:1,2,10 69:10 91:8 158:3 161:3 169:2 175:18 177:18 182:4 185:17 191:17 194:15,16 196:3 206:21 214:14 224:20 228:13 242:22 261:5 265:9 275:14 277:6 278:21 284:7 289:3 296:3,9 299:22 300:22 305:13
**realm** 37:14 88:19
**reason** 10:9 27:1 44:19 47:6,10 51:9 59:1,7,9 60:15 80:15 88:16 94:1 143:14 171:22 178:3 183:11 237:12 256:10 258:17 296:4 302:5
**reasonable** 15:17 16:9,12 16:21 17:3,22 18:16 40:18 48:18 121:6 140:7,17 151:20 173:7 185:15 190:8 190:12 227:9 236:20
**reasonableness** 16:19 121:14 130:9,10 137:7 143:11,13
**reasonably** 9:11 31:18 37:11 39:20 40:10,20 41:6 58:14 71:17 79:10,12 89:9,13 131:1 136:6 148:11 162:1
**reasoning** 249:17
**reasons** 30:16 106:5 121:22 129:5 134:18 172:13 211:9 280:19
**reassessed** 240:1
**reauthorization** 100:1
**rebuild** 222:12
**recall** 48:17
**received** 70:17 70:20 86:6
**receives** 38:14
**receiving** 4:20 312:18
**recipient** 70:16
**recipients** 235:13
**recite** 102:8
**recited** 282:3
**recognize** 226:3 227:9 230:4 233:3,13 236:9 236:17 248:22 267:9,13 268:18 292:15 309:15
**recognized** 66:18 151:9 154:13 210:20 229:8 241:7 299:18,19
**recognizes** 95:7 291:8 310:22
**recognizing** 47:14 88:20
**recommend** 68:11 221:22 272:13 278:1 283:16
**recommendat...** 172:15 203:21
**recommendat...** 35:4 274:7,21 277:22 280:3 284:17 301:14
**recommended** 173:2 274:6
**reconsider** 76:12
**record** 78:4,6 84:2 99:4 113:7 125:3 174:18 209:5 311:16 313:8
**recorded** 7:8 313:7
**recording** 124:15 174:17 235:9
**records** 153:13 205:17
**redacted** 75:18 76:16
**reevaluate** 84:1
**refer** 38:9 54:7 115:21 234:5
**reference** 6:5 179:6
**referred** 26:5 134:13 178:11 187:4
**referring** 41:5 187:4,5 207:18 208:10
**refers** 26:6 67:2 102:2 103:18 161:3
**reflect** 99:4
**reflected** 132:17 133:3 241:17
**reflects** 137:17
**reforming** 206:18
**refrain** 230:1
**regain** 237:4
**regard** 79:7 80:5 114:3,9 116:4 147:11 154:22 155:18 176:17 177:2 205:11 243:3 251:1 272:3 274:14,18
**regarding** 1:5 15:2 114:7,10 250:19 271:15 292:22 293:2
**regardless** 217:18 233:14 237:15
**regards** 271:17
**regime** 62:20
**regimes** 238:8 263:9 264:4
**regional** 238:17 239:2 242:4
**regions** 71:3
**register** 4:10 156:7,8,10 157:9
**regular** 20:18

21:1,14 29:5 61:13 294:8
**regulate** 126:15 165:11
**regulated** 133:14,17
**regulations.gov** 7:11
**rein** 199:3
**reined** 279:11
**reinforcing** 218:13
**Reingold** 5:4
**reining** 287:4
**reinserted** 36:20
**reiterate** 244:12
**reject** 166:6 259:12
**rejoining** 209:7
**relate** 242:9 288:3
**related** 51:16 179:5 239:21
**relates** 221:16 222:1 285:2,12
**relating** 5:19 102:12 147:14 152:5
**relation** 249:2
**Relations** 231:22
**relatively** 75:19 276:17
**released** 11:16 147:18 191:6 220:19 223:21
**relevance** 169:22
**relevant** 10:9 42:7 46:13 65:7 108:8 143:17 146:10 158:16,16 165:8 200:11 235:5 242:14
**reliable** 256:2
**relied** 130:6 307:18 308:1
**relying** 24:8 160:3 196:6,18
**remain** 6:7 13:11 85:3 262:18 304:13 311:17
**remaining** 16:8 280:21
**remains** 230:8
**remarks** 63:16 113:18,22 114:1 116:21 125:11 152:19 230:22 266:16 272:8
**remediate** 218:20
**remember** 100:4 125:19 204:10 249:6 284:3,5
**remind** 125:9,13
**reminder** 301:7
**remote** 154:16
**remotely** 226:10 227:15
**removed** 44:17
**Renaissance** 1:15
**render** 15:17
**renewed** 238:18
**repeat** 10:11 298:8
**repeated** 10:5
**repeatedly** 126:7
**repeating** 40:12 74:9 235:14
**report** 5:9,12 6:15 152:22 174:10 211:21 214:6 221:7 239:14 272:12 276:12 282:3 307:11
**reported** 1:22 72:14,15 73:17 124:13
**reporter** 116:17
**reporting** 11:11 65:2 222:17 294:8
**reports** 6:2 11:14 62:11,13 65:3,13 72:15 84:19 86:13
**representatives** 7:1
**request** 212:20 241:5 311:11
**requested** 306:13
**requests** 221:18 272:15
**require** 10:17 45:21 109:14 122:10 131:5,7 140:12 146:21 149:5 185:22 240:12 263:1 306:19
**required** 12:7 22:19 28:11 44:16 45:2 47:19,19 49:3 84:11 103:7 126:20 130:1,5 139:20 178:19 184:15 242:13
**requirement** 15:20 16:1,19 28:20 48:2 58:13,18 80:14 109:20 121:9 129:18 130:11 134:4,10 137:6 142:6 143:6 148:13 150:2 150:16 151:7 151:13 152:8 154:2,11 162:7 162:7 184:16 185:15 204:3 205:15 208:2 212:12 243:13 243:14 281:6,8
**requirements** 11:22 16:17 44:21 140:15 142:17 151:5 178:19 253:5 274:19 294:1,8
**requires** 22:7 52:16 84:19 126:19 131:20 148:7 224:21 240:5
**requiring** 35:1
**research** 241:18 275:14
**Researcher** 3:18 209:14
**reside** 217:19
**residence** 133:8 233:15
**resident** 8:3
**resides** 237:17
**resolution** 236:6 241:6,12,17 247:19 276:11
**resolved** 276:7
**resources** 64:20
**respect** 16:19 19:4 37:21 61:19 65:20 67:16 81:1,1 84:19 86:4 94:3 98:12,22 105:18,21 111:5 144:19 145:7 190:14 194:9 211:14 212:8 213:21 215:14 217:17 224:9 226:4 229:4,21 232:4 234:8 243:13 248:3,6,9,17 250:9 251:12 258:7 259:9 268:22 271:11 271:18 285:11 285:16 287:20 289:21 298:15 298:16 303:10
**respected** 185:16
**respectful** 217:11
**respecting** 247:20
**respective** 237:13
**respond** 132:13 142:20 149:16 305:3
**responded** 140:18 307:12
**responding** 225:5
**response** 8:16 64:3,4 83:14 99:5 102:16 111:15 154:12 238:11 284:8
**responses** 7:6 187:14
**responsibilities** 244:9
**responsibility** 6:13 291:1
**rest** 76:10

**restore** 208:14
**restraint** 187:17
**restricting** 194:16 242:12
**restriction** 133:8,12,15 162:9 194:4 195:15
**restrictions** 133:3,18 187:16 194:17 210:6 211:12 253:18
**restricts** 111:5
**result** 31:22 33:10 70:13 218:18 228:14
**resulting** 231:18
**results** 134:2 163:12 236:13 263:10
**resume** 113:5 209:3
**retain** 122:14
**retained** 17:20 44:4 81:10 93:21 119:1 120:5 135:21 146:4
**retains** 152:7 195:2
**retention** 9:20 17:7,17,19 47:6,9,11,14 79:21 81:4 94:19 95:21 103:21 104:17 116:12 117:6 117:21 118:21 120:15 201:2 229:9 253:19
**return** 31:18 79:10 113:12 153:21 171:10
**reunification** 263:14
**reveal** 153:14 155:13 156:11
**revealed** 240:8
**revealing** 13:11
**revelations** 226:21 238:16 247:18 269:6 272:1 276:6 286:21
**reverse** 40:15 89:2,10 90:4,6 90:10 91:1,3,6 91:17 92:11 97:19 123:14
**review** 9:8 11:7 15:13 22:12 23:13 31:1,5,7 31:11 61:19 68:19 72:7 74:2,4,5 78:14 81:20 83:21 103:19 116:3 124:17 135:1 141:6,14 156:16,20 157:19 172:8 172:14 192:14 200:20 201:12 202:21,22 203:1,9,20 205:8,9 228:8 242:14 294:16 312:12
**reviewed** 42:17 42:18 43:2,7 47:5 59:20 61:11 76:18,19 77:2 78:15 116:22 117:1 294:12
**reviewing** 75:12 76:14 101:17
**reviews** 18:14 22:4 62:9 68:22 310:5
**revised** 95:1
**revising** 206:19
**revisit** 42:12
**rewind** 124:16
**right** 18:7 32:10 38:8 39:14,17 53:13 55:1,3 57:9,10 58:21 61:17 73:5 75:3 81:16,17 91:12,22 96:11 100:18 101:2 101:13 102:15 110:2 112:18 112:22 114:20 117:3 137:20 138:3 142:13 143:4,20 144:6 146:17 149:3 157:8 161:9 163:1,22 164:7 170:1 180:1 181:9 183:5 184:15 189:19 192:16 194:5 196:16 203:12 206:21 207:20 210:19 217:6 225:16 226:4 227:14 229:4 236:7 246:6 247:20 248:17 249:19 251:3 254:11 263:3 266:5 268:2,13 270:21 280:15 280:16 281:2 282:1 283:19 287:6 289:22 297:4,22 299:2 299:4,17,17 304:10 305:22 306:5 307:17 311:4
**rightly** 185:20
**rights** 3:19 8:20 10:15 15:7,14 180:19 207:4 209:15 210:17 210:22 211:1 211:22 212:8 213:9,16,16,19 214:7,22 215:5 215:15,19 217:8 223:17 224:10 225:4 226:12,17 227:6,20 229:21 231:1 232:14 233:3 233:14,17,20 233:22 234:1 234:19 235:8 235:10,15,22 236:2,19 237:5 237:9 244:22 246:16,17 248:1,3,9 249:21 250:4,6 250:18,21,22 251:4,8,10 252:11 253:8 256:8 258:3 259:1,2,3,4 262:4 267:9 268:9 271:10 271:12,16,19 286:14 290:5 290:11,13,18 307:8 308:5,8
**ripe** 237:8
**rise** 184:22
**risk** 95:19 253:15 282:14
**risks** 258:15 282:8
**road** 300:1
**roamer** 73:7
**roamings** 72:1
**robbery** 186:15
**Robert** 2:17
**robust** 6:4 84:3 184:13 185:5 202:17,20 309:17,19
**robustly** 8:20
**role** 106:1 115:1 127:9 205:11 237:4
**rolls** 99:5
**Romania** 109:14
**room** 154:20 219:2,4 280:2 287:4
**Roosevelt** 212:21 247:12
**Rosetta** 76:2
**rough** 93:14
**round** 50:6 93:4 93:20 97:10 100:14 142:21 175:14 283:22 288:10,10 290:10 306:13
**rounds** 7:4
**route** 228:22
**routed** 144:13
**rubber** 299:22
**rule** 40:21 41:1 96:2 100:19 101:10,13,16 109:18 231:16 237:5
**ruled** 139:19
**rules** 5:20 12:21 17:17 54:1 56:15 81:14 101:5 102:11 104:22 105:2,4

105:6 107:18 112:20 229:9 259:12 309:14
**rulings** 205:19 290:17
**Rumanian** 109:15
**run** 225:8
**runs** 35:3
**rushing** 228:16 228:17
**Russia** 304:1

**S**

**s** 252:7
**sabotage** 285:5
**sacrifice** 228:12
**safe** 220:11 300:11
**safeguards** 160:1 237:14 275:22 284:11
**safer** 228:10 238:13 283:9
**safety** 228:11
**Sara** 252:6
**satisfied** 212:14
**satisfy** 173:2
**save** 175:13
**saw** 253:3 293:2
**saying** 25:9 32:10 37:2 53:4 56:18 64:10 70:6 76:7 145:14 148:22 164:8 167:22 171:22 176:7 191:3 197:10 199:11 217:4,7,10 262:19 265:16 265:17 286:6 287:22 294:17
**says** 53:21 89:8 91:11 111:4 156:1 161:2,20 165:2 212:7 224:8 230:7 247:4 258:9 285:10 290:16 305:11
**scale** 121:3 160:9 187:6,12 188:4 189:3 232:2 270:10
**scan** 147:20 148:1 189:21
**scanned** 192:13
**scanning** 189:1 192:16 197:8
**scans** 189:11
**scenario** 247:2
**schedule** 311:20
**scheme** 145:2 165:14 183:16
**Schmoe** 287:21
**scholar** 225:10
**scholarly** 118:12
**scholars** 210:17
**school** 3:5 113:11 302:14
**scientific** 240:16
**scope** 9:6 173:21 203:8 212:7 232:14 236:1 244:8
**score** 42:1
**screed** 221:5
**scrutinizes** 11:18
**sea** 158:2,9
**seal** 313:12
**search** 21:20 27:19,22 28:3 28:7,11 37:3 37:17 38:2,7 38:18,19 39:1 39:3,4,9,13,15 43:18 48:4 115:6 124:4 130:1,2,6 140:7 146:16 146:21 147:6 148:3 171:17 172:10 190:4 193:4 197:20 201:2 206:7
**searched** 115:11 198:11
**searches** 36:22 37:18 50:9 79:6 115:3 123:16,16 130:12 175:18 177:14 179:18 180:11 184:5,8 184:13 185:9 185:11 194:13
**searching** 38:20 78:10 137:22 174:14 175:17
**second** 6:16 10:13 26:4 29:19 39:9 48:13 58:22 74:18 106:18 110:14 112:4,8 113:5,9 114:7 114:21 122:17 126:4 129:1,16 130:4 133:9 134:21 145:17 188:21 203:13 222:1 250:13 251:21 273:12 278:8 305:5
**secondary** 37:16
**Secondly** 31:14 232:16 256:21 310:10
**seconds** 124:8 280:21
**secrecy** 84:9
**secret** 77:7 135:9 292:11 293:6
**secretly** 240:19
**section** 1:7 2:10 5:10,15 7:17 8:12,14,17,21 10:3,5,11,20 11:8,18,22 12:5,9,21 13:8 13:10 25:4,8 37:9 48:20 56:8 65:6,14 66:9 92:18 100:1 111:4 112:15 117:13 118:11 119:11 121:1 123:13 123:21 124:10 124:11 125:16 125:19 126:12 126:18 128:4 128:12 129:4 130:18,21 131:6,11 132:22 133:3 135:4,6 141:17 151:4,7,8 157:7,8 158:22 170:7,7 202:10 202:12 203:14 207:22 219:3,4 239:6 240:4 258:8 273:8 292:20
**sections** 177:4 208:5,7
**sector** 6:22
**secure** 238:17
**security** 2:15,20 3:10,18 35:18 93:1 113:16 119:20 139:19 139:20 140:16 141:2 142:7 198:6,7 209:14 210:11,12 218:10 219:10 228:4 230:6 232:18,21 236:18,20 240:12,17 241:20 242:5 242:12 253:11 253:14,15 254:14 255:17 272:11,16 273:9 275:20 277:12 286:2 287:9 300:2,9 300:15
**see** 27:6 35:5 36:15 45:10 48:5 54:4 56:13,14 62:21 65:12 74:2 87:2 118:1 154:22 155:7,9 162:4,5 172:9 173:5 178:5 198:5 201:6 204:15 252:10 256:6 266:5 271:20 277:2 291:21 295:1 303:20
**seeing** 220:2,9
**seek** 28:16 140:7 241:3
**seeking** 20:10
**seen** 93:6 236:5 254:5 279:13
**segregated** 34:4 95:19
**segue** 145:12
**seize** 12:18
**seized** 198:10

**seizure** 190:3 197:20
**selected** 155:2
**selection** 26:13 147:19
**selective** 50:2
**selector** 10:9 24:21 28:2 50:13,18 51:2 51:4,13,14,22 51:22 52:4 53:7,8,10 54:6 54:11 55:8,11 55:17 56:1 59:2 61:15 71:8 78:10 80:15 100:21 173:7 294:19
**selector-based** 25:9 26:9
**selectors** 9:4 10:7 23:20 25:11 26:1,12 26:13 36:21 37:3 47:21 56:10 57:12,17 63:8 71:5 123:17 135:15 161:15 163:3 189:6 295:2
**self-defense** 262:21
**self-executing** 236:21 306:15
**self-interest** 277:1
**self-restrain** 286:7
**semiannual** 62:12 72:15
**senate** 251:6,18 251:20 264:19 290:21,22 291:4
**send** 198:8 200:9
**sender** 229:3
**Senior** 3:18 209:14
**sense** 18:19 20:18 38:4 46:2 197:3 224:20 253:2 254:16 270:8 281:22 289:13 291:15 299:12 310:1
**sensible** 131:11
**sent** 181:15
**separate** 58:17 61:14 63:10 89:20 111:19 119:10 152:22 163:1 193:7
**separated** 257:16
**separating** 221:10
**separation** 256:22,22 257:3,11
**sequitur** 300:15
**series** 64:1 200:18
**serious** 232:10 232:13 257:5,6 289:7
**seriousness** 75:10
**serve** 204:17,17
**served** 210:8 252:15
**servers** 231:10 303:16
**service** 7:15 25:15 26:8 69:18,18 168:3 238:12 239:2
**set** 8:14 18:20 34:16 71:12 84:8 95:14 113:17 119:10 192:20 222:11 250:6 260:16 288:20 309:14
**sets** 72:17 220:18
**setting** 60:22 93:10 113:3 266:22 295:12
**severe** 136:13
**severely** 115:1
**sexual** 302:3
**shadows** 154:20
**shaking** 101:19
**sham** 145:1
**shape** 66:20
**share** 5:2 112:21 136:14 176:22 218:19 221:17 273:7,13,14 293:18
**shared** 112:8 136:5 291:3 310:19
**sharing** 112:4 239:1 242:1 276:8 283:11
**Sharon** 5:4
**shed** 135:3,12
**sheer** 65:9
**sheet** 61:7,7,14
**shift** 50:8,20 63:9 86:11
**short** 113:4 172:3 173:1
**shorter** 93:21 94:19 95:21
**shorthand** 25:21 26:5 41:5
**show** 164:19
**showed** 277:11
**showing** 198:21
**showings** 149:6
**shown** 275:8
**shows** 73:12
**side** 20:20 21:2 29:9 121:19 138:12 188:21 243:17 257:10
**Sieber** 3:20 209:15 215:10 230:10,11,12 254:21 255:5 255:14,18,21 260:8 261:14 262:18 266:3 301:16
**SIGAD** 191:5,5
**signals** 81:2 195:12 217:15
**significance** 137:15 143:15 185:12
**significant** 21:21 69:13 134:7,10 138:18 170:16 170:17 208:18 219:1,16,17 272:2 273:3
**significantly** 178:22
**silence** 194:2,21
**silent** 176:21 177:1 193:18 193:21 276:18
**silos** 220:5,14
**similar** 18:18 48:2 239:11 257:20
**similarities** 238:7
**Similarly** 223:5
**Simone** 5:6
**simply** 100:2 111:21 119:4 217:2 220:8 225:21 234:5
**single** 61:16 74:2 246:4 253:9
**site** 120:8
**sitting** 277:21
**situated** 229:6
**situation** 24:14 75:22 115:19 138:6 142:10 156:4 168:5 199:6,6 226:5 228:15 310:12
**situations** 150:19 234:17 247:6
**six** 98:6
**sixty-four** 211:15
**skepticism** 260:21 261:1,9
**skipped** 58:21
**Skype** 191:8
**slice** 68:8
**slide** 39:22
**slides** 191:6
**slightly** 18:17 278:11
**slip** 57:4
**slippage** 208:20
**slow** 116:14
**slowing** 116:17
**small** 48:20 131:21 190:21 254:8
**smaller** 270:15
**Smith** 108:5,7
**Smith's** 108:12
**Snowden** 226:21 238:10 238:15 269:6

276:6
**so-called** 123:15 173:6 210:19 242:4
**social** 299:21
**societal** 219:18
**societies** 237:6
**society** 157:13 175:2 299:20
**soil** 142:8
**solely** 69:12 174:13
**Solicitor** 167:6
**solution** 181:4 233:16 237:3,9
**solutions** 172:3 218:19 220:18 221:5 222:3,11
**solve** 247:13
**somebody** 80:7 114:8 161:6 167:22 171:5 177:3 302:4,12
**someone's** 12:18 226:6,8
**somewhat** 89:7 89:8 274:17 279:11 309:16
**soon** 239:12
**Sooner** 306:3
**sorry** 40:11 48:11 57:9 93:3 116:19 141:12 155:3 191:14 192:9 202:19 250:15 269:15
**sort** 11:3 24:8 24:10,10 32:21 34:10 54:10 64:11 72:7 76:1 80:17 84:22 133:20 138:7 139:9 143:5 144:13 144:15 148:20 162:4,6 163:12 166:10,12 170:4 181:9 185:5,17,22 193:5 194:6,14 199:3 202:22 203:9 205:15 207:21 243:12 244:7,17 264:10 281:14 296:1 299:12 299:13
**sorts** 81:13 171:9
**sounds** 299:11
**source** 65:4 198:15 250:18
**sources** 13:14 206:14 230:16 268:10
**sovereign** 231:4 262:3 264:15 264:22 304:18
**sovereignty** 231:7,14,18 261:21 262:1 265:5 305:8
**space** 154:17 298:17,18
**Spain** 239:11
**spatial** 234:18
**speak** 44:11 72:22 78:18 88:3 106:16 126:4 138:12 149:18 251:9 261:11 264:7
**speakers** 6:5,9 312:3
**speaking** 15:1 39:5 63:15 107:17 115:12 144:14 163:12
**speaks** 273:19
**special** 16:3 32:9 234:18 257:17
**specific** 8:5 13:10 14:22 25:22 47:12 61:4 66:14,15 71:5 81:8 88:15 122:9 137:1 141:15 191:16 216:17 231:1 235:21 252:17 253:4 278:9 294:16 294:19
**specifically** 24:16 80:4 100:17 107:12 117:13 229:13 239:5 266:9 291:22
**specificity** 194:22
**specifics** 88:18 95:11
**spectrum** 153:19
**speech** 277:10
**spend** 85:16,16 215:17
**spending** 84:21 113:1
**spent** 36:1 98:6
**sphere** 184:19
**spirit** 132:21
**split** 243:12 263:4
**spoke** 147:10 203:20 308:15
**sponsored** 247:19
**spot** 33:21 62:7
**spy** 265:16
**spying** 215:17 264:20 265:8
**square** 191:10
**stab** 50:22 244:10
**staff** 5:4 312:3
**staffs** 99:13
**stage** 8:14 37:1 87:20 118:18 146:11
**stages** 103:22 146:11 188:22
**stake** 27:5 240:17
**stakes** 124:21
**stance** 224:15
**stand** 264:4
**standard** 72:12 72:20 79:9 86:8 105:17 137:7 180:13 180:14 199:21 204:1 206:19 206:19 207:17 208:4 280:6 281:15 305:21 306:6,10,11
**standards** 18:11 21:14 25:17 31:15 136:12 222:18,20 223:3 278:17
**standing** 185:21
**standpoint** 228:20
**start** 13:22 51:2 54:11 64:9,10 113:18 144:4,6 209:22 223:17 230:21 243:6
**started** 98:19 289:1
**starting** 118:1 149:22 155:5 198:5
**state** 129:10 181:3 210:9 212:7 215:4 224:16 231:6,9 232:20,22 233:2 234:7,14 252:16 261:20 264:9 313:5
**state's** 225:22 227:13 230:19 241:13 248:2 262:3
**stated** 146:3 187:11
**statement** 8:9 13:21 140:19 152:22 209:20 213:8 222:22 223:12 264:14 271:22 304:10 308:14 309:1
**statements** 70:5 71:2 93:7 136:21 153:13 159:11 213:19 216:22 222:14 250:7 251:11
**states** 8:4,19 9:12,15 10:15 10:21 29:8 39:21 40:4 67:9,11 71:18 71:20 72:3 73:11 86:20 89:5,10,11,13 89:15,17,22 90:2,13,15 91:10 97:17,21 97:21 103:10 104:18 114:19 115:13 128:3 129:9,13,20,22

130:14,22 131:2 133:7 137:10,12,13 138:7 140:14 147:6 151:17 159:18,19 162:2,18 176:20 180:19 182:3 210:7 211:15,18 212:5,5,15,16 212:18 213:4 213:20 214:9 215:8 216:5,6 216:8 217:7,15 224:8 229:6 230:17 231:5 231:14 232:2,6 232:18 235:17 239:16,20 241:8,10 243:20 245:6,9 245:12,14 246:3,11 248:5 248:10,12 250:2,8 251:13 251:15 253:11 254:7 261:19 264:16 267:9 268:17 269:14 270:8 274:4 276:5 277:14 279:9 281:9 285:3,13,22 287:11,18 288:1,2,4 290:8 291:6,16 292:8 294:17 297:13 305:8 306:8 307:3,12 309:18,18
**status** 41:13 262:3
**statute** 12:6 13:1 22:10,18 23:16 40:8,13 43:5 52:16 54:22 55:10,12 59:6 60:11 84:11 89:8 91:11 96:1 97:14 109:2 121:2,8,13,19 121:21 122:1 122:17 123:2 133:1 134:1,4 134:11,20 148:12 151:8 155:1 159:10 159:13,14,15 160:14,22 161:2,10,19 162:13 163:22 164:9,19 166:9 166:20 167:5,8 167:13 176:21 177:1,2 187:18 187:22 188:1 194:19 195:5 195:15 200:22 202:15 203:8 203:15 247:4 270:3 293:10 293:16
**statute's** 123:3
**statutes** 121:16 232:8 287:5
**statutory** 6:18 25:17 54:6,13 58:17 69:4 90:7 104:14 114:2 127:18 130:16 148:13 161:17 164:13 164:13 165:13 170:22 176:15 183:13,16 187:16 310:5
**stay** 259:14
**steal** 197:15
**stems** 224:6
**stenographica...** 313:7
**step** 25:2 44:8 58:22 273:3
**steps** 103:18 222:17,19 223:1,5 256:9 272:5 273:4 274:3 275:1
**stolen** 197:18
**Stone** 76:2
**stop** 66:22 227:18 304:8
**storage** 238:12 238:14 239:4 282:13
**stored** 228:19
**stories** 64:1,12
**storing** 235:12
**straightforward** 239:19
**strategic** 301:7 310:7
**stream** 190:3 192:14
**strength** 42:6
**strict** 129:3 225:13 269:16
**stricter** 257:8
**strictly** 224:15
**strikes** 178:13 178:14 187:12
**strong** 135:19 174:8 256:6,22 257:11
**strongest** 160:22 161:17
**strongly** 185:10 206:18
**struck** 288:15
**structural** 193:20
**structure** 132:22 133:22 134:20 164:13 309:17 310:5
**structures** 309:16
**structuring** 309:12
**struggle** 304:1
**struggling** 157:20 288:17
**studies** 64:22
**study** 110:18
**stuff** 200:20
**sub-questions** 44:7
**subject** 6:15 11:4 19:13,17 19:19,22 25:17 86:12 133:16 212:10 213:3 214:20 215:1,6 224:10 243:14 244:18 247:11 292:4,5 296:5 296:6
**subjected** 18:10 211:4
**subjects** 36:17
**submission** 132:18 159:5 161:11 246:15
**submit** 312:7,8
**submitted** 7:11 8:22 19:15 22:10,20 117:2 211:21 312:11
**submitting** 116:21 117:4 182:16 312:10
**subpart** 109:9 161:21
**subpoena** 153:12 156:18
**subsequent** 27:18 77:1 191:22 193:3 193:11 201:13 213:7
**subsequently** 27:16 28:6 44:2,3 196:14 198:1 199:20
**subset** 56:9 82:16
**substantial** 99:13 241:19
**substantive** 78:9 78:12,17 79:1 236:1 243:2
**substituting** 106:18
**subterfuge** 9:16
**succeed** 205:5
**success** 64:1,11
**successful** 263:7
**succinct** 309:4
**Sue** 5:4
**sufficient** 41:1 42:2,4 160:1 173:11 174:3 177:13 179:7 198:13 272:21
**suggest** 41:12 45:11 72:10 77:9 83:15 148:14 195:1 215:20 216:14 274:21
**suggested** 28:14 68:9 162:21 252:14 275:1 278:21
**suggesting** 34:3 137:5 148:18 167:3 199:9 215:6,22

**suggestion** 135:18,19 244:18 275:1
**suggests** 41:21 41:22 166:16 245:18
**sui** 207:22
**sum** 237:2
**summary** 54:3
**sunset** 69:3 100:12
**supervised** 83:9
**supervision** 7:16
**supplanted** 184:21
**supply** 295:22
**support** 123:2 218:14 238:16
**supported** 233:17
**suppose** 49:4 109:13
**supposed** 285:15
**Supreme** 15:8 129:9 167:6 249:10
**sure** 15:4 24:1 24:22 28:22 33:6 36:7,8 40:6,22 44:8 52:20 56:17 58:20 74:13 85:13 92:7 94:7,20 96:18 100:13 105:11 111:14 113:19 127:5 149:1 153:21 154:5 168:10,21 169:14,17 178:5 181:8 182:1,4,19 185:20 187:6 189:14,15 199:22 207:14 216:14 222:6 222:20 245:16 248:13 270:1 301:22 311:17
**surprised** 119:8 246:9
**surveil** 123:10 123:11 151:16 172:22
**surveillance** 1:6 1:8 2:11 3:3 6:14 7:18 11:13,17 29:11 43:3 44:22 45:4 49:2 116:2 121:4,10 121:15 123:9 124:14 125:16 126:2,6,9 127:15,19 128:1,7,9 129:12,18,20 131:15 133:14 133:17 139:1 139:16 140:17 141:5,16 150:11,21 151:2 158:8,8 158:10,11,17 160:7,9 161:1 164:10,11,14 165:2,5,6,9,11 166:8,11,13,17 166:19,21 167:3 169:1,11 170:13 171:11 181:22 182:21 183:14 188:8 188:14,18 195:17 196:22 196:22 197:2 206:6,10 210:6 210:18 211:7 214:19 215:7 215:11 216:20 221:4 225:15 225:21 226:19 227:11,18,19 227:21 230:15 231:15 232:3 232:16 233:12 235:1 238:13 238:17 239:6 239:17,21 240:2,4,5,7,13 240:15 241:7 242:3,6,8,12 244:19 245:2,5 246:7,11,18 252:12,19 253:3,7,20 255:3,8 257:17 261:21 262:7,8 264:10,17 265:7,19 268:22 269:3 270:6,9,16 271:1 272:1,15 274:12 275:12 277:1,4 278:3 279:4 280:1,8 283:9,10,11 289:21 290:1 291:11,17 293:15 295:11 296:14 300:2,9 300:15,21 301:12 302:8 304:13 306:7 307:18 308:2 308:17 310:7
**surveilled** 269:20
**surveilling** 151:14 175:7 197:4 235:17 277:19
**survive** 125:2
**survived** 187:1
**suspect** 49:1 156:1 302:4
**suspected** 151:16 198:14
**suspicion** 48:19 199:2 302:9
**suspicionless** 281:14
**swath** 192:6
**switch** 189:8 303:16
**synthesizes** 239:9
**system** 33:9 42:14 80:10 119:18 124:14 125:2 130:17 184:22,22 185:4,5 233:5 233:10 256:3,5 309:12,19 310:1
**systemically** 292:7
**systems** 44:18 45:2 72:21 154:17 231:8 232:21 241:8 258:18 259:8

**T**

**table** 44:13 105:20
**tail-end** 44:12
**tailored** 30:17 47:12 88:18 228:6
**take** 15:4 41:10 42:6 50:22 53:9 77:6 92:17,17 109:10 113:4 119:12 124:18 151:20 156:6 156:17 157:6 166:20 168:5 171:4 174:11 187:10 190:14 193:3 196:3 197:15 209:2 217:16,22 223:1 224:1 225:13 227:19 232:17 244:10 289:17 291:3 296:12 306:17 311:19
**taken** 22:1 145:14 190:10 211:16 222:18 247:17 249:9 252:3 270:8 273:5 274:3,4
**takes** 156:4 224:15 269:1
**talk** 8:12 20:14 24:2 25:1,3 28:19 29:1 39:18,21 89:1 98:20 120:12 174:9 182:20 191:15,15 213:15 223:15 265:10
**talked** 23:17,20 27:13,14 61:2 105:21 137:3 168:18 204:11 260:20 261:18 278:7 310:3
**talking** 30:12 31:17 36:11,16 38:2 52:19 58:7 68:2 72:1

72:2 76:1 81:21 86:2 90:11 98:6 99:21 103:20 112:14,19 137:9 146:12 168:1 189:16 205:22 216:16 249:20 270:16 284:1 287:16 287:19 292:19
**talks** 161:19 270:3
**target** 8:2,6 9:4 9:10,14,16 10:17 12:3 14:3 29:7 40:13,14,19 50:17 51:1,14 52:14,17,20 54:5,14 55:15 55:19 58:14 61:10 71:2 80:15 82:9,10 89:2,9,11,12 90:1,12,21 91:8,16,17 92:1,6,8,13 97:1,18 116:6 116:9 131:8 133:5,20 137:12 141:12 141:12,15,19 147:12,13,14 150:21 154:8 154:22 155:2 161:12,15 163:22 164:20 165:15 166:2 166:21 167:4 201:11 206:22 207:7 281:16
**targeted** 10:7 24:16 25:8 43:19 48:8 52:12 60:7 124:5 149:9 167:18,18 169:22 229:14 253:4 279:5,21
**targeting** 9:9,10 10:20 13:12 15:6 16:11,13 17:1,6 21:13 22:9 24:9 37:10 40:9,16 42:15,22 49:20 51:5,22 52:8 54:21 55:3,4 55:10,11,12,14 55:21 59:18 81:18 89:2,14 89:21 90:4,6,8 90:10,21,22 91:1,2,3,4,6,7 92:11 97:20 101:2 103:14 114:3,14,22 117:14 119:13 120:14 122:4 123:14 130:22 133:17 147:11 161:2,7 162:1 162:6,14 163:7 177:6,7 200:21 203:11 204:5,6 205:9,11 206:19 281:11 294:1,12,16 310:7
**targets** 8:18 12:4,12,18,20 37:14 60:15 114:6,6 120:3 122:8,20,22 123:7 134:6 135:14 151:15 163:2 167:9 176:18
**task** 53:2,4,7,8
**tasked** 95:4
**tasking** 50:17 53:2,3,19 54:9 61:7,21 100:20 188:16,17 189:4,5
**taskings** 53:22
**technical** 34:2,6 45:1 46:2 89:7 119:3,3 227:15
**technically** 137:9 144:14
**technological** 204:19 228:20
**technologies** 219:7,11
**technology** 3:17 137:18 182:2 209:13 227:9 270:9
**telecommunic...** 235:7,9 282:9
**telephone** 9:4 10:8 14:5 47:22 48:18 190:11,15,19 190:19
**telephony** 66:11
**tell** 60:21 65:21 80:3 93:9 107:11 260:4
**telling** 168:2
**tells** 293:10,17
**temporarily** 47:21 229:13
**tendency** 266:10
**tends** 154:19
**tens** 134:15 163:5 219:14
**term** 38:18,19 39:6,7,12 50:13 51:3 52:5 54:6,6,7 54:10 55:10 70:13,14 82:7 95:4 96:15 97:3,5,8 99:17 106:21 159:7 230:5
**terms** 19:5,9 21:22 33:21 38:3 50:15,19 50:20 58:3 66:18 69:17 71:15 83:3 102:1 106:1 110:13 117:9 118:18 147:19 196:10 202:21 208:20 228:12 244:3,8 264:9 272:13 275:11 295:4
**terrible** 167:16
**territorial** 138:17 139:3 139:10 143:16 224:15 231:5,6 232:1,5 243:10 243:15 264:15 264:22 265:5 278:16 295:12 305:8
**territoriality** 258:8 303:11 303:19 304:14 304:18,20
**territorially** 271:11 297:11
**territories** 220:12
**territory** 129:8 212:9,16,19 213:3,13 214:11 215:5 224:9,17,19 230:19 231:11 232:17 233:3 234:18 235:16 235:19 246:7 246:22 247:3,5 247:10 248:2,4 248:5 270:3,5 285:11 296:5 303:14,15
**terrorism** 13:14 34:17 172:18 285:6
**terrorist** 51:10 53:12 57:13 103:9 151:17 169:2,7 297:14
**terrorists** 51:6 60:19
**test** 42:5,5 156:3 243:1,2
**testify** 218:8
**testimony** 121:13 218:16 222:3 239:9 252:9 279:11 282:2 294:5
**tests** 178:12
**text** 161:7 164:13,17 167:12
**textual** 160:22 164:5 176:22 194:7
**thank** 4:22 5:3 8:10,10 13:20 27:7 35:5,19 43:15 113:1,6 113:19 116:15 117:1 120:17 125:5,6,7 132:8,10 136:18,20 145:11 152:13 167:14 172:6

182:6,7,15 208:22 209:4 210:3 218:3,4 218:5,5,8,9 223:9,10,11 230:10,12 237:22 238:1,2 242:17,20 248:19 252:20 260:6,14 266:7 266:15 273:1 291:13 295:6 311:9,21,22 312:20
**thanks** 20:2 35:20,20 120:19,20 125:7 160:18 160:18 209:6 247:15 288:21 307:15 312:2
**theoretical** 48:7
**theoretically** 247:9
**theories** 38:13
**theory** 39:19 195:17 206:1
**thing** 38:17 65:8 71:1 77:17 138:10 145:2 167:16 168:4 179:16 182:5 201:16 206:2 208:12 226:9 253:19 305:12
**things** 25:11 26:1,11 34:7 34:11 36:16 38:9 45:10 52:7 57:14 59:11 63:10 71:5 85:18,22 95:18 104:7 105:8,12 135:8 136:11 161:10 182:14 200:18 202:17 244:11 245:15,20 253:22 257:13 258:1 259:16 265:14 266:8 279:7 287:8 289:9 296:20 302:21 303:1 306:4 307:10
**think** 13:18 15:19 19:1,7 19:14 20:1 23:14,21 24:1 25:4 28:9,14 31:4 32:7,8,8 33:8 34:1,2,5 35:22 36:12,13 36:15,17 39:5 40:6 43:15 46:15,22 47:19 48:6,10,11,14 49:9,10,13,15 56:4 57:3,21 58:6 60:2 61:7 61:18,19 62:17 63:19 64:3 65:21 66:21 67:3,5,10,13 67:15,19 68:1 68:2,5,8,10,18 69:2 72:22 73:20 74:1,5 75:4 76:6,13 76:21 77:5,8,9 77:11 80:6,21 82:5 83:8,15 83:17 84:2,5 85:9 87:10,13 87:18,19 88:5 91:6,16 93:2 93:11 94:9 96:14 97:5,12 98:18 99:5 102:17,18 103:20 106:9 107:2,3,18 108:20 110:5 110:15 111:3,4 112:11 118:16 119:12 120:9 125:10,15 131:20 132:7 134:18,22 135:1,16 136:9 137:14,17 138:9,13,20 139:5,10 143:1 143:3,17 144:3 144:17 145:19 148:19 151:11 152:21 156:3 157:13 158:1,4 158:9,19 159:6 161:8,15,17 162:5,21,22 163:9,21 164:8 164:8,10,12,19 165:7,12 166:4 166:7 167:10 168:19 169:12 170:3,5,12,13 170:19,20,21 172:13,19 173:10,11,18 173:21 174:2,7 174:8 176:4 177:1 178:2,3 179:15,19 180:11,16 181:4,8 182:1 182:2,12,12,13 183:5 184:1,3 184:10,11 185:6,10,11,13 185:19 186:4,7 186:11,17 187:4,15 188:4 189:19 190:6 192:13 193:18 194:5,7,14,17 195:1,18 196:7 196:16,20 197:16 198:18 200:5 202:9,14 203:6,13 205:7 205:18,21 206:1,3 207:5 208:8,12 210:8 210:16 221:9 222:10 223:7 244:20,22 245:7,9 246:3 247:13 248:16 248:21,21 249:10,19 253:14,21 254:13 260:3 260:17,22 261:3,12 262:6 262:9 263:21 264:12 266:3 266:19 267:3 269:7 274:15 274:17 276:18 279:2,15 280:1 280:12 282:18 283:6,19 285:9 285:19 286:15 287:3,7 288:13 288:22 289:5 291:15 292:11 294:4 296:10 298:2 299:18 300:6,8 301:13 305:5,11 307:20 309:13 310:22 311:10 311:15
**thinking** 162:14 203:13 208:2 208:14
**thinks** 288:1
**third** 11:4 66:17 72:17 114:9 116:12 117:6 140:8 203:22 209:3,8 288:10 296:3
**thirdly** 31:14
**thirty** 124:8
**thirty-five** 150:9 187:1
**thought** 58:1 72:2,4 110:2 146:7 170:20 183:15,17,21 188:20,21 252:22 275:17 310:16
**thoughts** 272:9 298:7 310:10 311:3,5
**thousand** 43:11 74:6
**thousands** 134:15 163:5,5
**threat** 32:16 108:8 232:10 253:11 300:11
**threats** 13:15 60:19 103:6 236:9,10 282:10 283:1
**three** 6:11 11:5 63:21 121:22 139:22 202:17 220:18 243:7
**threshold** 104:2 116:10 198:3
**throwing** 173:3
**time** 12:14 20:1 20:4 27:6,8,22 28:3 29:19 30:2,5 35:6

36:6,10 40:3 50:4,5 51:18 56:13 62:22 65:12 67:5 72:9 75:1 82:2 82:20,21 85:16 85:17 87:15 92:17 93:22 100:14,15 113:2 125:12 175:13 195:13 212:2,12,21 215:17 237:8 247:13 266:18 271:20 278:13 283:17 286:19 295:6 300:8 306:12 311:20 312:1,19
**timekeeper** 269:16
**timely** 67:19
**times** 14:4 48:21 284:21 307:18
**tiny** 44:11
**tip** 118:7
**tipping** 157:6
**title** 12:16 29:4 29:10 111:3 116:4 121:16 141:10 155:21 171:17 179:2 194:3 197:18 206:7
**today** 5:15,20 6:11 98:10 99:21 113:2,20 121:18 124:9 124:21,22 125:8 196:17 200:17 209:1 218:8 220:6 236:15 239:9 239:18 243:17 260:17,20 261:16 264:4 266:7 273:19 292:12 312:5
**today's** 5:1 7:13 109:18 312:12
**told** 214:8
**tool** 65:22 66:4,7 66:13,22 67:1
**tools** 13:9 66:1,2
**top** 87:12 95:12 101:15 185:18 189:19
**topic** 37:13 50:8 63:10 232:4 312:8
**topics** 79:5
**torture** 225:20 270:14
**tortured** 270:18
**torturing** 270:20
**total** 144:22 234:17
**totality** 41:7 42:5 178:12
**totally** 9:13 104:5 196:5
**touch** 6:1 245:2
**trace** 156:8,8,10 157:10
**traces** 118:9
**track** 71:13,21 72:9 81:5 192:10
**trade** 300:13
**tradition** 125:21 128:21 130:14 130:17 185:16
**traditional** 14:16,17 153:8 153:12 155:6,8 156:10 158:2 206:7
**traditionally** 84:6
**trail** 118:6
**training** 34:6 41:18 62:4 86:6
**transatlantic** 300:12
**transcript** 7:9 312:12 313:8
**transfer** 229:1
**transfers** 241:3
**transformed** 219:22
**transiting** 138:7
**transmission** 235:10
**transmissions** 235:13
**transnational** 3:14 7:1 209:9 232:16,19 233:12 235:21 236:19
**transparency** 221:6,8,21 239:16 241:19 272:8,9,13 273:16,20 276:1 277:8 279:14,16 284:13 291:18 292:16 293:19 294:20,21 301:2
**transparent** 98:16 293:9
**trap** 156:7,8,10 157:9
**travel** 119:19 228:22
**treat** 280:7
**treated** 34:4 95:16 217:17
**treaties** 238:22 249:5 251:4,17 251:17 290:15
**treatment** 79:19 253:18
**treaty** 210:22 211:19 212:13 212:18 214:18 224:5,21,22 225:3,7,14 227:6 243:9 245:19 246:1 247:4 249:13 249:15 250:11 250:21 251:12 251:18 267:17 267:18,20 268:2,3,4,7,16 271:4 286:17 286:19 289:10 290:3,11 291:2 291:5 299:6 306:14
**tried** 205:1 223:22
**trigger** 15:12
**true** 135:22 181:12 187:11 213:14 289:16 313:8
**trust** 219:6,7 222:12 228:13 232:11 237:6 292:9
**try** 32:15,17 64:19,22 253:16
**trying** 52:9 60:9 61:9 69:16 88:14 90:1 108:15 144:18 146:8 164:1 165:13 172:1 186:11 191:17 199:6 247:12 267:1 286:8
**turn** 8:7 30:9 32:5 58:10 77:16 233:18 242:21
**turning** 230:22
**turns** 41:17 73:22,22 189:14
**twice** 69:5
**two** 5:9 6:19 25:7 30:13 39:1 41:22 42:1 47:14 53:1 54:16,17 65:16 73:6 82:8 94:22 101:11 110:5 125:13 126:10 127:4 129:5 132:17 133:2 146:2 162:6 168:6,17 171:19 175:18 176:2,11 178:13 180:17 182:14 187:14 188:22 201:5 218:12,16 225:3 230:16 230:18 232:3 243:1 248:20 249:16,16 263:9,15 271:5 277:16 278:4 282:17 289:15
**type** 10:19 25:19 25:21 26:4,15 32:22 33:17,20 57:7 58:19 59:5 66:7 105:18 132:3 157:10 178:12

183:17 260:18 288:7
**types** 25:3,7,14 25:16 27:2 29:3 30:13,18 33:11,19 34:10 66:8 73:6 139:11
**typical** 21:17 55:2
**typically** 39:13 51:4

**U**

**U.K** 240:21 310:8
**U.N** 211:22 231:4 234:1 236:5 247:19 251:6,20 252:7 264:14,20 265:1,15,15 290:16 304:21 305:7,11 307:8
**U.S** 9:17,21 10:14 12:2,11 14:6,9,13 15:10 16:5,10 16:20 17:8,10 17:13,21 19:4 19:21 28:17 30:12,14 31:21 36:20 37:2,19 40:13,15 43:17 43:20 45:13,14 47:22 48:3 54:17 71:20 74:2 78:10 79:22 80:12,12 81:6,9 82:14 82:16 89:4,16 89:21 90:1,8,9 90:12,14,22 91:9,14,19 92:2,9 94:12 96:8,10 97:19 101:3,8,18 102:12 103:11 103:13 106:3 106:19,20,21 107:1,19 108:16,19 109:17,19,22 111:5 112:17 114:8,14,18 125:15 126:8,9 127:6 128:9 129:19 130:1 130:17 131:8 133:5 138:2 139:21,21 142:7,8,8,8,17 143:20 149:3 152:5 172:11 172:21 175:17 176:5,18 177:3 177:7,9 178:6 180:2 183:12 183:22 184:2 193:4 194:12 194:17 201:1,2 211:2,18 212:20 213:18 214:14,20 219:7 223:15 224:2,5,14 225:12,13 226:6 227:3,7 227:8 228:4,19 229:5,11,18 230:1,5,15 232:11 233:6 234:7 236:18 237:1,4,13 238:14 240:1 241:2,21 242:8 242:10 244:12 244:19 245:3 248:13 250:20 251:10,16 256:3,11 260:21,22 265:19 267:12 267:15 268:2,6 268:7 272:4,15 278:3,14,16 279:17 280:7 282:9,16 283:1 283:15 284:14 295:11,21 297:12 300:6 304:1,5 310:18
**U.S.A** 219:8 236:22
**ubiquitous** 220:4
**Ukraine** 236:15
**Ulrich** 3:20 209:15
**ultimate** 49:4,8
**ultimately** 72:15 185:13 245:6
**unable** 98:8
**unanimous** 4:20 312:18
**unanswered** 135:10
**unavoidable** 96:17
**unclassified** 5:21 60:22 75:18
**unclear** 181:17
**unconsenting** 104:18
**unconstitutio...** 121:1,9 153:6 153:10,17
**unconstitutio...** 169:6
**unconstrained** 129:14
**uncontroversi...** 127:9
**uncovered** 201:12
**under-empha...** 125:14
**underlying** 49:14
**undermine** 134:10 222:18 223:2,3
**undermined** 150:8
**undermines** 163:9 230:5
**underscores** 247:19
**understand** 8:8 17:15 18:3 20:14 25:5 31:10 32:1 33:1 50:16 52:6 58:6 67:14 68:3 79:18 80:7 82:17 86:17 107:21 108:7 109:3 119:9 124:11 143:2 145:13 146:12 148:21 157:20 158:12 168:21 182:19 184:1 191:17 194:9 194:11 242:22 262:16 286:8 296:1
**understanding** 50:11 98:5 106:1 108:8 125:15 164:2 179:17 184:21 194:1 197:1 213:11 244:3 264:19 291:4 311:1
**understands** 56:18
**understood** 111:14,16 125:20 131:11 261:19
**undertake** 290:17,19
**undertakes** 69:6
**underwear** 34:18
**undisputed** 127:15 304:19
**undoubtedly** 235:16
**unequivocal** 222:13
**unexpected** 12:4
**unfair** 200:15
**unfortunate** 77:5
**unfriendly** 244:8
**unhappiness** 49:7
**unhappy** 49:2 215:11,18
**unilaterally** 278:1,1
**unintentional** 96:20
**Union** 3:7
**unique** 12:5 18:14 26:19 47:15 229:19
**United** 8:4,19 9:12,15 10:15 10:21 29:8 39:20 40:4 67:8,11 71:18 71:20 72:3 73:11 86:20

89:5,11,13,15 89:17,22 90:2 90:13,15 91:10 97:17,20,21 103:10 104:18 114:19 115:12 128:3 129:8,10 129:13,19,22 130:14,22 131:2 133:6 137:10,12,13 138:7 140:14 147:6 151:17 159:18,19 162:2,18 176:19 180:19 210:7 211:15 211:18 212:5,5 212:15,16,18 213:20 214:8 215:8 216:5,6 216:7 217:7 239:8,20 240:11 243:20 245:6,9,12,14 246:2,11 248:5 248:10,12 250:2,8 251:13 251:15 253:11 254:6 267:9 268:17 269:13 270:8 274:4 276:5 277:14 279:9 281:9 285:3,13,22 287:11,17,22 288:2,4 290:8 291:6,16 292:8 294:17 297:13 306:8 307:3,12 309:17,18
**Unites** 89:10
**universal** 210:19 217:6
**universally** 225:4 295:15 295:19 296:18
**universe** 197:3,9
**University** 3:5,8 113:11,14
**unknown** 83:8 233:1
**unlawful** 199:10 211:4 216:9,12 216:15,20 296:16 298:4 298:14
**unreasonable** 121:11
**unregulated** 144:8
**unsupervised** 130:15 144:12
**upheld** 126:7
**upholding** 121:15
**upset** 246:10
**upstream** 26:5,6 26:15,19 30:15 30:19 36:21,22 37:6,10,21 47:13,15 56:9 56:10 57:19 63:6 93:6,8,16 93:20,21 94:3 94:6 95:16 101:12 187:7 248:14
**Ur** 76:2
**urged** 7:5
**Uruguayans** 246:18
**USA** 5:11
**usable** 176:12
**USC** 111:2
**USD** 188:10 196:6
**use** 13:4 34:21 39:6,7,9,13 78:10 81:20 91:15 96:5,15 97:18 98:12 106:13 111:7 142:11 147:18 159:7 171:6 172:5 176:7 181:17 199:14 201:1,2 203:17 206:16 253:18 265:6,17
**useful** 67:15 85:22 103:4 106:9 170:10 206:2 283:13
**uses** 55:10 66:17 99:16 119:11
**usually** 106:8 128:3 162:14 303:18
**utility** 64:13 65:10 69:13,14
**utilized** 66:1

**V**

**vague** 286:12
**valid** 12:3,12 13:5 59:6,8,15 92:6 253:12 303:4
**validity** 6:10
**valuable** 13:9 66:6 67:8,11 102:17,18
**value** 43:21 44:6 44:15 45:11,22 46:8,18 47:2 65:17 80:2,16 82:3 102:14 103:2 110:8 163:8,11 164:3 191:12 230:4
**values** 310:19
**variety** 13:15 23:5,10 34:17 65:10 75:14 84:4 94:16
**various** 22:9 46:20 67:7 69:3 153:15 238:8
**varying** 6:13 277:18
**vast** 150:5 279:18 286:1 293:5
**vastness** 227:1 269:10
**veneer** 142:11
**venue** 301:6,11
**Verdugo-Urq...** 129:11 147:5
**versus** 71:14 129:10
**viability** 220:11
**Vienna** 231:21 249:4
**view** 10:13 50:16 67:6 83:3 89:3 91:2 97:17 98:21 120:22 121:8 123:1 125:10 145:22 154:17 159:16 182:22 184:2 185:17 190:5,18 191:18 192:18 193:9,22 211:9 218:12 246:2 246:20 250:2 251:9 263:12 277:6 291:7 296:11 310:13
**viewed** 10:22 24:10 273:3
**viewing** 88:12
**views** 5:2 7:7 182:9 250:4 268:21
**vigorous** 276:15
**VII** 194:3
**violate** 11:21 156:14,20 224:18 232:6 264:21 265:20
**violated** 227:14
**violates** 121:2 210:19 211:8 231:6,20 296:21
**violating** 158:3 217:1 231:13
**violation** 158:1 215:22 253:8 261:22 262:3 263:21 264:8 265:21 267:7 286:13,17 296:17 297:6
**violations** 153:20 232:10 232:13 233:1
**virtual** 234:20 234:22
**virtue** 135:21
**vis-a-vis** 80:5 93:8 293:14
**visit** 120:1
**vocabulary** 158:13 188:20 189:15
**voice** 191:9
**voicemail** 190:19
**volume** 93:7,8
**volumes** 180:20 199:1
**voluntarily** 240:22
**voluntary**

197:20 241:3
**vote** 213:5
**voted** 100:11
**vs** 139:21 142:8
**vulnerability** 229:6

**W**

**wait** 175:14
**Wald** 2:5 4:15 43:14,15 44:11 44:19 45:5,20 46:6,10 47:18 48:10 49:4 50:2 78:7,8,20 79:12,15 81:16 82:17,20 106:2 106:3 107:5,11 109:9 110:1,9 110:12,19 111:12 112:16 112:19 167:14 167:15 168:12 168:15,17 169:16 171:1 171:19 173:13 173:17 175:13 200:14,15 201:15,22 202:4,19 203:3 203:11 204:5,8 205:12 207:8 248:19,20 249:22 250:13 250:16 251:21 253:1,13 265:12 277:15 277:16 279:1 280:5,20 281:4 281:21 282:1 282:21 283:15 283:19 289:1 289:15 300:5 307:15,16 308:12 309:4
**Wald's** 77:13,16 111:14 117:8
**walk** 145:16 153:18
**wall** 141:9
**walled** 220:5,7 220:14
**want** 4:22 10:2 10:11 13:7 20:6 23:12 24:13,15 50:8 50:20 53:4,5 59:16 60:5 64:10 68:5 69:10 76:20 77:4 85:4 86:16 89:1 91:9 96:5 100:8,13 103:11,15 112:22 113:18 125:9,13 132:6 145:13 149:19 149:21 154:5 172:7 174:6 175:16 179:14 182:10,11,18 207:11 208:22 209:7 215:9 218:14 233:16 242:21 243:6 243:16 260:11 269:17 283:3 301:3 311:4,21
**wanted** 5:3 13:22 27:11 35:10 63:1,9 85:5,8 86:3,11 87:2 92:21 93:5 96:4,17 98:3 111:13 148:21 149:16 172:9 192:20 247:1 260:14 261:13 266:21 272:5 284:4,4 291:12 311:8
**wants** 59:1 201:7 295:8
**War** 225:2
**warrant** 8:5 15:20 16:1,6 16:17 21:20 28:11 115:16 121:9 128:3 129:18 130:1,5 136:15 137:6 139:20 140:12 142:5,9 143:6 146:21 147:2 150:2,16 151:6 151:12,14,18 152:8,10,10 154:2,10 160:8 172:9,10,16 173:1,11,13,15 177:11 180:8 184:15,16 185:14 205:15 206:4,7 281:5 281:8
**warrantless** 14:12 115:2 121:4 126:8 128:7
**warrants** 10:17 141:7 151:22 157:4,5 173:14 256:15
**Warren** 299:16
**Washington** 1:17 4:8 124:13 174:10
**wasn't** 158:16
**wasting** 85:17
**Watch** 3:19 209:15 251:5,8
**way** 16:16 20:22 31:4,4,12 34:4 34:9 35:7 44:18 57:20 64:12,14 78:2 85:1 99:2,7,19 101:22 104:5 137:18 138:13 143:2,2 144:13 153:2 154:21 157:12 158:16 169:12 175:2,3 175:4 180:9,10 184:4 197:1,5 198:19 199:3 203:3 208:4,9 208:10 219:22 222:16 225:8 246:1 257:5 268:4,7 271:8 278:20 280:1 287:12 309:11 313:10
**ways** 19:3 65:5 65:16 68:9 95:19 135:3 188:6 228:6 271:6 287:11 306:22
**we'll** 8:14 32:13 32:14 50:5 77:21 113:4,5 132:12 174:13 174:20 260:7 260:12 266:1,2
**we're** 13:12,12 13:18 31:17 36:16 43:11 51:15,15,18 52:19 58:7 73:9,14 76:14 84:11 96:18,20 99:21 103:13 103:13,20 110:21 112:14 113:8 115:2 118:1 124:10 124:22 126:14 137:9 142:11 177:6,7 189:15 194:9 198:5 199:5 207:21 209:2 215:18 216:16 218:17 218:20 219:5 219:19 220:2,9 228:15 254:9 287:3 295:6
**we've** 11:15 23:8 27:13,14 29:15,16,19,20 30:11 36:1 58:5 61:2 65:6 70:7 84:8,8 85:1 172:12 176:7 188:21 189:19,20 193:17 223:12 252:3 254:15 260:20 278:7 278:17 279:13 291:14
**weapons** 59:13 285:6
**website** 312:9
**websites** 175:10
**week** 276:11 307:11
**week's** 239:14 241:6
**weeks** 86:14
**weigh** 179:14
**weighed** 16:4
**weird** 138:5
**welcome** 4:2 7:10 200:12 237:12
**welcomed** 110:21 112:14 113:8 115:2 118:1 124:10 124:22 126:14 137:9 142:11 177:6,7 189:15 194:9 198:5 199:5 207:21 209:2 215:18 216:16 218:17 218:20 219:5 219:19 220:2,9 228:15 254:9 287:3 295:6
**we've** 11:15 23:8 27:13,14 29:15,16,19,20 30:11 36:1 58:5 61:2 65:6 70:7 84:8,8 85:1 172:12 176:7 188:21 189:19,20 193:17 223:12 252:3 254:15 260:20 278:7 278:17 279:13 291:14
**weapons** 59:13 285:6
**website** 312:9
**websites** 175:10
**week** 276:11 307:11
**week's** 239:14 241:6
**weeks** 86:14
**weigh** 179:14
**weighed** 16:4
**weird** 138:5
**welcome** 4:2 7:10 200:12 237:12
**welcomed**

311:18
**well-founded** 234:5
**well-known** 35:22 274:2
**well-recognized** 119:17
**went** 47:20 140:11
**weren't** 166:4 188:7 274:21
**Westphalia** 305:1
**whatsoever** 134:9
**white** 140:10 217:10 238:7 238:19 239:5 239:10,13,19 240:8 241:16 242:18 275:13 277:8 282:19
**who've** 168:17 276:15
**wholly** 40:17 94:13 95:5,20 95:22 134:15 163:7
**wide** 13:15 192:6
**wide-ranging** 126:8
**widely** 277:18
**Wiegmann** 2:19 15:4 17:5 18:7 18:12 19:1,21 20:16 27:21 28:22 35:16 43:6 50:22 53:3,8,17 55:1 56:1 60:1 61:5 61:16 73:5 75:4 76:13 77:17 89:18,20 90:5,17,20 91:5,13,18,22 92:4 103:8 105:14 107:17 108:2
**willfully** 224:18
**William** 140:19 140:20
**willing** 58:3
**willy-nilly** 297:19
**wind** 216:3
**Winn** 5:5
**winners** 275:15
**wire** 165:3
**wire-brushing** 99:17
**wiretap** 12:16 12:16 14:16,18 21:19 29:10 115:16 146:20 153:9 155:8
**wish** 104:4 132:6 208:13 245:16 290:6
**withdraw** 300:11
**witness** 256:4 313:12
**witnesses** 35:21 160:19 284:20 309:10 310:12
**WMDs** 59:12
**Wolf** 3:22 209:18 238:1,2 254:22 275:7 275:13 277:5 278:20 282:2 282:18 283:5 299:15
**Wolf's** 274:1
**won** 233:10
**wonder** 45:16
**wondered** 249:2 308:19
**wonderful** 168:2
**wondering** 172:2 252:15
**word** 56:6 96:5 160:2 224:12 249:3,16
**wording** 213:11
**words** 26:14 38:6 45:12 57:13 107:22 108:4 127:17 135:15 147:20 160:21 171:1 188:5 204:16 213:10 255:10 260:9 278:11
**work** 238:10 266:6 282:19 302:18
**working** 46:11 79:15 110:20 220:20 222:12 266:12
**works** 20:15 108:20
**world** 83:10 182:8 218:8 219:12 234:15 234:21,22 246:4 250:3 252:2 254:8 262:16 264:2,3 275:21 283:12 289:19 293:11 305:6 307:6 310:17
**world's** 229:19
**world-wide** 231:14
**worse** 260:5
**worth** 68:3 74:8 88:6 126:7 228:11,14
**wouldn't** 23:14 48:2 52:5 90:3 92:10 168:7 171:2,16
**writ** 295:17
**write** 290:15,15
**writing** 245:19 311:6
**written** 7:9,20 87:8 88:4 116:21 121:13 132:18 159:5 161:11 182:17 200:20 239:8 246:2 252:9 312:8
**wrong** 40:3 66:21 67:2 71:19 72:3,5 73:20,22 100:21 110:3 160:2
**www.regulati...** 312:9

**X**

**Y**

**Yahoo** 191:7
**Yahoo.com** 207:3,4,5
**yeah** 75:9 84:7 104:4 107:15 109:1 146:13 155:7 164:17 248:15 249:22 249:22 255:10 288:21 296:2
**year** 5:8 17:19 22:8,14,16 23:1,4,7,15,16 47:8 74:20 219:20 220:20
**years** 11:20 47:14 69:5 94:22 99:9 101:9,11,11,12 101:12 104:9 150:9 187:1 211:15 214:14 301:8
**yesterday** 124:13 174:10
**yield** 162:19 288:9,11
**YouTube** 191:8

**Z**

**0**

**1**

**1** 43:9 258:8
**1:45** 209:3
**10** 93:16 313:17
**10th** 4:10
**1127** 1:16 4:8
**11th** 93:12
**12333** 81:7,12 109:6,8
**17** 210:21 211:3 211:8 216:8 217:1 233:20 246:12 260:10 261:17 267:7 289:22
**18** 188:10 196:6
**1806** 111:2
**1881** 161:21
**1890** 299:19
**19** 1:10
**1950** 211:19 212:21 213:6
**1967** 140:9
**1970s** 15:21
**1972** 139:22
**1973** 195:10

150:13
**1990** 129:10
**1992** 211:2
**1995** 211:20
213:9
**19th** 4:6

**2**

**2** 92:18 212:6
213:6 231:3
304:21 305:7
**2001** 210:11
**2002** 116:2
141:10
**20036** 1:17
**2005** 210:9,11
**2008** 75:15
77:15 247:17
**2009** 210:10
**2010** 234:7
**2011** 93:13 94:9
134:13 135:19
**2012** 69:6 100:1
**2013** 234:8
238:6 239:5
313:13
**2014** 1:10 4:6,10
5:14 313:17
**215** 5:10,13
47:20,21 48:16
48:20 49:16,21
50:3 69:1,4
152:22 157:7
170:7 204:11
204:18 219:3
221:18 272:12
273:8 292:18
293:2
**23rd** 5:13
**25th** 219:20
**28** 237:13
**28th** 7:12
312:10

**3**

**3** 231:21
**3:40** 312:20,21
**30** 61:20
**31** 234:2 249:4
249:20
**32** 303:22 304:4

**4**

**402** 157:8
**49** 40:2

**5**

**50** 111:2
**51** 39:19 40:2,21
40:21

**6**

**60** 42:18 59:21
62:8
**68167** 236:6

**7**

**701** 252:18
**702** 1:7 2:10 3:2
4:4 5:11,16
7:17 8:12,14
8:17,21 10:3,5
10:11,20 11:4
11:8,22 12:5,9
12:22 13:8,10
19:12,19 21:3
21:12 22:6
23:18 25:4,8
25:16 30:22
36:14 37:9
38:6 40:5
43:18 48:3,12
48:15,22 49:16
56:8 65:6,15
66:10 67:7
69:6,19,19,20
70:9 71:2,4
75:17 77:18,20
78:3 79:2 80:5
81:1 88:15
90:9 91:15
97:18 99:21
100:1,10 107:8
111:4 112:15
113:21 117:13
118:11 119:12
121:1 123:13
123:21 124:10
124:11 125:17
125:19 126:12
126:15,18
128:5,12 129:4
130:19,21
131:6,11
132:22 133:3
135:4,6 137:9
141:17 145:22
148:7 151:4,8
151:8 152:20
158:22 160:14
165:5,10,10
170:7 186:9
187:5 193:1,18
194:3,13 196:7
200:17 201:6
202:12 203:14
204:15,17,21
205:12 207:22
219:4 221:12
221:17 223:6
228:2,3 239:6
240:4,7 243:3
243:19 267:2
267:16 272:2
273:9,20
274:10 277:22
280:22 281:6
281:11 291:20
292:20,22
293:21
**703** 177:4
**704** 92:18 177:4

**8**

**8** 213:6

**9**

**9/11** 34:17 257:2
257:13
**9:00** 1:17
**9:05** 4:6

DECLARATION OF SCOTT BRADNER

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

# Appendix R

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

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

Follow-up Questions Regarding Section 702 Certifications
June 17, 2011

1. The government's Response to the Court's Briefing Order of May 9, 2011 ("June 1 Submission") states that Internet transactions acquired by NSA in its upstream collection may contain not only multiple discrete communications (some of which are neither to, from, nor about a tasked selector), but also [redacted] June 1 Submission at 25.

a. Please provide some examples of the [redacted] For instance, could such acquisitions include [redacted]

b. What is the likelihood that such [redacted] pertain to persons other than the users of tasked selectors, including persons in the United States or U.S. persons?

2. The June 1 Submission states that "no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication." June 1 Submission at 9.

a. What is meant by "wholly domestic communication" in this statement? Does the term include the discrete communications that might be embedded within acquired transactions?

b. What is the likelihood that an analyst viewing information obtained through a transactional acquisition would have a basis for determining that a discrete communication embedded within the transaction is purely domestic?

3. a. Might the non-targeted portion of a transaction ever be the sole basis for that transaction being responsive to an analyst's query?

b. Upon retrieving information in response to a query, can an analyst readily distinguish that portion of a transaction that contains the targeted selector from other portions of a transaction?

4. a. Please describe the manner in which the government minimizes discrete communications and other information that is contained within acquired Internet transactions but that is neither to, from, nor about the user of a targeted selector.

b. In particular, please explain how the government applies the provisions of NSA's minimization procedures that use the term "communication" to the discrete communications and other non-target information contained within the transactions that are acquired. See, e.g., NSA Minimization Procedures § 2(c) (defining "[c]ommunications of a United States person"); § 2(e) (defining "foreign communication" and "domestic communication[]"), § 3(b)(4) (discussing determination whether a communication is "foreign" or "domestic"), and § 5 (discussing handling of domestic communications).

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


NYT v DOJ, 16 CIV 7020_000408

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



c. Would all communications and [redacted] within a transaction be treated the same when the minimization procedures are applied, or would there be different treatment?

5. a. Once NSA has identified a portion of a transaction that does not contain targeted information, is it possible to mask or otherwise minimize the non-target information contained within the transaction?
b. Why is NSA unable to delete and replace, or alter, an original transaction that contains non-target information? See June 1 Submission at 27-28.

6. The government states that an Internet transaction that is acquired "is . . . not divisible into the discrete communications within it even once it resides in an NSA corporate store." June 1 Submission at 22. Please reconcile that statement with the government's acknowledgment that "an analyst would . . . be able to copy a portion of the rendered view of a transaction contained in a NSA corporate store and then paste it into a new record on a different system." Id. at 27 n.25.

7. Please reconcile the government's statement that the "communicants" of to/from communications are "the individual users of particular selectors" (see June 1 Submission at 30) with [redacted] elsewhere in its response to the Court's questions (see, e.g., id. at 6 (discussing application of IP filtering)).

8. What is the factual basis for NSA's assertions that "a United States person would use [redacted] only in a minute percentage of cases" and that "[redacted] See June 1 Submission at 11, 12.

9. What is the factual basis for NSA's suggestion that [redacted] See June 1 Submission at 8 n.9

10. The government repeatedly characterizes as "unintentional" NSA's collection of discrete non-target communications as part of transactional acquisitions, [redacted] Assuming arguendo that such collection can fairly be characterized as unintentional, please explain how 50 U.S.C. § 1806(i) applies to the discrete, wholly domestic communications that might be contained within a particular transaction.

11. Please provide a thorough legal analysis supporting your view that the knowing and intentional acquisition of large volumes of Internet transactions containing discrete communications that are neither to, from, nor about a targeted selector (as well as other information not pertaining to the users of targeted selectors) is merely "incidental" to the authorized purpose of the collection as a whole, and therefore reasonable under the Fourth Amendment.

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



12. The statute requires the targeting procedures to "be reasonably designed to ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States and [to] prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). How can procedures that contemplate the knowing acquisition of huge volumes of transactions that will include quantifiable amounts of information relating to non-targets, including information of or about U.S. persons abroad or persons located in the United States, meet this statutory requirement?

13. In its discussion of the Fourth Amendment, the government asserts that "upstream collection" in general is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs." June 1 Submission at 16.

a. To what extent can the same be said for the acquisition of Internet transactions [redacted] in particular?

b. Is the acquisition of Internet transactions via upstream collection the only source for certain categories of foreign intelligence information? If so, what categories?

c. Please describe with particularity what information NSA would acquire, and what information NSA would not acquire, if NSA were, in comparison to its current collection, to limit its acquisition of Internet communications to: (1) acquisitions conducted with the assistance of [redacted]; and (2) the upstream collection of discrete communications to, from, or about tasked selectors that are [redacted] (id. at 2, n.2).

14. The Fourth Amendment also requires the Court to examine the nature and scope of the intrusion upon protected privacy interests. How can the Court conduct such an assessment if the government itself is unable to describe the nature and scope of the information that is acquired or the degree to which the collection includes information pertaining to U.S. persons or persons located in the United States?

15. In light of the government's emphasis on the limited querying of Section 702 acquisitions that is currently permitted (see June 1 Submission at 23), why is it reasonable and appropriate to broaden the targeting procedures to permit querying using U.S.-person identifiers?

16. The government acknowledges that it previously "did not fully explain all of the means by which . . . communications are acquired through NSA's upstream collection techniques" (June 1 Submission at 2), yet states that the "[Attorney General] and [Director of National Intelligence] have confirmed that their prior authorizations remain valid" (id. at 35). At the time of each previous Certification under Section 702, were the Attorney General and the Director of National Intelligence aware that the acquisitions being approved included Internet "transactions" [redacted]? If so, why was the Court not informed. If not, why are the prior Certifications and collections still valid?

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

~~SECRET//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

2011 JUN 28 PM 4:51

WASHINGTON, D.C.

[redacted]

NOTICE OF FILING OF GOVERNMENT'S RESPONSE
TO THE COURT'S SUPPLEMENTAL QUESTIONS OF JUNE 17, 2011

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits the attached factual and legal response to the

~~SECRET//ORCON,NOFORN~~

Classified by: Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: 28 June 2036


NYT v DOJ, 16 CIV 7020_000411

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



supplemental questions provided by this Court to the Government on June 17, 2011, concerning the above-referenced matters. Given the complex nature of the Court's questions and the Government's responses, the United States is prepared to provide any additional/supplemental information the Court believes would aid it in reviewing these matters. The Government may also seek to supplement and/or modify its response as appropriate during any hearing that the Court may hold in the above-captioned matters. ~~(S//OC,NF)~~

Respectfully submitted,

[redacted]

[redacted]
National Security Division
United States Department of Justice

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

~~SECRET//ORCON,NOFORN~~

## VERIFICATION

I declare under penalty of perjury that the facts set forth in the attached Government's Response to the Court's Supplemental Questions of June 17, 2011, are true and correct based upon my best information, knowledge and belief. Executed pursuant to Title 28, United States Code, § 1746, on this 28th day of June, 2011. ~~(S)~~

[redacted]

Signals Intelligence Directorate Compliance Architect
National Security Agency

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

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

# GOVERNMENT'S RESPONSE TO THE COURT'S FOLLOW-UP QUESTIONS OF JUNE 17, 2011

**1. The government's Response to the Court's Briefing Order of May 9, 2011 ("June 1 Submission") states that Internet transactions acquired by NSA in its upstream collection may contain not only multiple discrete communications (some of which are neither to, from, nor about a tasked selector), but also [redacted] June 1 Submission at 25.**

**a. Please provide some examples of the [redacted] For instance, could such acquisitions include [redacted]**

**b. What is the likelihood that such [redacted] pertain to persons other than the users of tasked selectors, including persons in the United States or U.S. persons?**

As was more fully explained in the Government's June 1 Submission, the presence of a tasked selector is required in order for the National Security Agency's (NSA) upstream Internet collection devices to identify and then acquire Internet communications in the form of transactions. *See* June 1 Submission at 1, 24-26. The Court's question in 1.a. further asks whether such transactions could include [redacted]. Personal information, including that of persons other than a user of a tasked selector, could be acquired by NSA in relation to any one or more of these communication services to the extent it is included within a transaction. This, however, is true even with respect to discrete communications to,

[1] [redacted] (S)

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

Classified by: Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ
Reason: 1.4(c)
Declassify on: 28 June 2036

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


from, or about a tasked selector, depending on what the communicants chose to include within, the communication. [redacted] ~~(TS//SI//NF)~~

Although personal information may be included in a transaction, the manner in which NSA conducts its upstream collection significantly diminishes the likelihood that such information would pertain to U.S. persons or persons in the United States. As discussed more fully in the Government's response to question 14 below, NSA acquires certain transactions because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's targeting procedures, is a non-United States person reasonably believed to be located outside the United States. NSA acquires transactions that contain a discrete communication about a tasked selector using technical means that are designed to ensure that such acquisition is directed at a person reasonably believed to be located outside the United States. The Court has previously recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, Docket No. 105B(g):07-01, Mem. Op. at 87 (USFISC April 25, 2008) (footnote omitted) (hereinafter "*In re Directives to Yahoo!* Mem. Op."). Thus, it is reasonable to presume that most of the discrete communications that may be within an acquired transaction are between non-United States persons located outside the United States. ~~(TS//SI//OC/NF)~~

**2. The June 1 Submission states that "no NSA analyst has yet discovered in NSA's repositories a wholly domestic communication." June 1 Submission at 9.**

**a. What is meant by "wholly domestic communication" in this statement? Does the term include the discrete communications that might be embedded within acquired transactions?**

By "wholly domestic communication" the Government means a communication as to which the sender and all intended recipients are located within the United States. The Government includes within this term any discrete communication within a transaction where the sender and all intended recipients of the discrete communication were located in the United States at the time the communication was acquired. With the previously described limited exception involving [redacted] NSA analysts have yet to identify a wholly domestic communication in any transaction acquired through NSA's upstream collection systems. ~~(TS//SI//NF)~~

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


**b. What is the likelihood that an analyst viewing information obtained through a transactional acquisition would have a basis for determining that a discrete communication embedded within the transaction is purely domestic?**

The likelihood that an NSA analyst would recognize that a transaction containing either a discrete communication (e.g., an e-mail message) or multiple discrete communications [redacted] contains a wholly domestic communication depends on a number of factors, including: [redacted] ~~(TS//SI//OC/NF)~~

**3.a. Might the non-targeted portion of a transaction ever be the sole basis for that transaction being responsive to an analyst's query?**

Yes. All information acquired by NSA as a result of tasking the targeted foreign person's selector -- whether initially determined to be foreign intelligence information to, from, or about that targeted foreign person (or foreign intelligence information concerning other foreign persons or organizations) or incidentally acquired information concerning other currently non-targeted persons -- can be queried by analysts for foreign intelligence information. As a result, it is possible that any portion of a transaction could be the sole basis for that transaction being responsive to an analyst's foreign intelligence query of NSA databases. Such queries (which are subject to review), however, must be formulated by an analyst in accordance with NSA minimization procedures which require that computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, be limited to those selection terms reasonably likely to return foreign intelligence information. *See, e.g.,* Amendment 1 to

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

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


DNI/AG 702(g) Certification [redacted] Ex. B, filed Aug. 12, 2010, § 3(b)(5) (hereinafter "Current NSA Minimization Procedures").[3] ~~(TS//SI//NF)~~

**3.b. Upon retrieving information in response to a query, can an analyst readily distinguish that portion of a transaction that contains the targeted selector from other portions of a transaction?**

Yes. The tasked selector that resulted in NSA's acquisition of any particular transaction is discernable by analysts reviewing information in response to a query. The analytic tools used to display an acquired transaction allow NSA analysts to identify the tasked selectors that resulted in the acquisition of the transaction, thereby enabling analysts to determine the portion(s) of the transaction in which that selector appears. In some instances, the analyst may need to review the entirety of the transaction (including the underlying metadata or raw data) to identify where the tasked selector appears, but even in these situations, the tasked selector is included and identifiable. [redacted] ~~(TS//SI//NF)~~

**4.a. Please describe the manner in which the government minimizes discrete communications and other information that is contained within acquired Internet transactions but that is neither to, from, nor about the user of a targeted selector.**

**4.b. In particular, please explain how the government applies the provisions of NSA's minimization procedures that use the term "communication" to the discrete communications and other non-target information contained within the transactions that are acquired. See, e.g., NSA Minimization Procedures § 2(c) (defining "[c]ommunications of a United States person"); § 2(e) (defining "foreign communication" and "domestic communication[]"), § 3(b)(4) (discussing determination whether a communication is "foreign" or "domestic"), and § 5 (discussing handling of domestic communications).**

**4.c. Would all communications [redacted] within a transaction be treated the same when the minimization procedures are applied, or would there be different treatment?**

---

[3] The Government seeks the Court's approval of revised NSA Section 702 minimization procedures that would enable NSA analysts to use United States person identifiers as selection terms if those selection terms are reasonably likely to return foreign intelligence information. *See, e.g.*, DNI/AG 702(g) Certification [redacted], Ex. B, filed Apr. 20, 2011, § 3(b)(5) (hereinafter "Proposed NSA Minimization Procedures"). Under these revised NSA Section 702 minimization procedures, the use of such selection terms must be approved in accordance with NSA procedures designed to ensure that the selection terms are reasonably likely to return foreign intelligence information. *Id.* The Government is still in the process of developing the NSA procedures governing the use of United States person identifiers as selection terms. Until those procedures are completed, NSA analysts will not begin using United States person identifiers as selection terms. ~~(TS//SI//NF)~~

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


As required by FISA, *see* 50 U.S.C. §§ 1881a(e), 1801(h), and 1821(h), NSA's minimization procedures address the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons. *See* Current Minimization Procedures, § 1.[4] When NSA acquires an Internet transaction that contains multiple discrete communications, NSA considers each of those communications to be separate "communications" under its minimization procedures. Thus, for example, an NSA analyst would consider each discrete communication within a larger Internet transaction as a separate communication for purposes of determining whether the communication is a foreign or domestic communication under NSA's minimization procedures. *See, e.g.,* Current and Proposed NSA Minimization Procedures, § 2(e). ~~(TS//SI//OC/NF)~~

The manner in which acquisitions are conducted under Section 702 operates to minimize the acquisition of information about United States persons. First, certain transactions are acquired because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's FISC-approved targeting procedures, is a non-United States person reasonably believed to be located outside the United States. This Court has recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!* Mem. Op. at 87 (footnote omitted). Accordingly, it is reasonable to presume that most of the discrete communications that may be within the acquired transaction -- even those that are not to or from a tasked selector -- are between non-United States persons located outside the United States. Second, with respect to transactions that contain a discrete communication about a tasked selector, the technical means by which NSA prevents the intentional acquisition of wholly domestic communications are designed to ensure that the acquisition of transactions is directed at persons reasonably believed to be located outside the United States. As a result, these persons reasonably also can be presumed to be non-United States persons, and most of their communications -- including those that are not about a tasked selector -- can be presumed to be with other non-United States persons located outside the United States. *Id.* This combination of targeting non-United States persons located outside the United States and directing acquisitions at persons located outside the United States operates to significantly diminish the amount of information pertaining to United States persons or persons in the United States that NSA acquires through its upstream collection. *See* [redacted] Mem. Op. at 23 (recognizing that "[t]he targeting of communications pursuant to Section 702 is designed in a manner that diminishes the likelihood that U.S. person information will be obtained"). ~~(TS//SI//OC/NF)~~

To be sure, it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain U.S. person information. The acquisition of such information is an unavoidable by-product of the acquisition of the foreign intelligence information (i.e., the communication to, from, or about a tasked selector) within the transaction. Yet it is important to note that, for purposes of the application of NSA's current and proposed minimization procedures, the Government does not consider its acquisition

[4] NSA's proposed minimization procedures currently before the Court address these same issues. *See* Proposed NSA Minimization Procedures § 1. ~~(S)~~

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


of a discrete communication within a transaction that is not to, from, or about a tasked selector to be "inadvertent." Subsection 3(b)(1) of NSA's current and proposed minimization procedures require inadvertently acquired communications to be destroyed if they are "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 not be disseminated under these procedures." Current and Proposed NSA Minimization Procedures, § 3(b)(1). ~~(TS//SI//NF)~~

As described below in the Government's response to question 10, the Government considers a discrete communication that is not to, from, or about a tasked selector within a transaction to be acquired "incidentally," rather than "inadvertently." In the context of minimization, "incidental" and "inadvertent" should not be considered synonymous. Given that the acquisition of the transaction is intentional, and given the Government's knowledge that such transactions may also include information that is not to, from, or about a tasked selector, the acquisition of this additional information is not "inadvertent." By contrast, the additionally acquired information is "incidental" in that it is not the basis for the collection but is rather a necessary yet unavoidable consequence of acquiring foreign communications to, from, or about a tasked selector. *See* [redacted] Mem. Op. at 40 (concluding that the Government's minimization procedures "constitute a safeguard against improper use of information about U.S. persons that is inadvertently *or* incidentally acquired") (emphasis added).[5] Otherwise, subsection 3(b)(1) of NSA's current and proposed minimization procedures would require the destruction of the *entire* transaction -- even the very foreign intelligence information that resulted in the transaction's acquisition in the first place -- if any discrete communication therein contained United States person information and was not to, from, or about a tasked selector. ~~(TS//SI//OC/NF)~~

Such an absurd result simply cannot be squared with Congress's explicit intent that non-pertinent information should be destroyed only if "feasible." *See* H.R. Rep. No. 95-1283, pt. 1, at 56 ("By minimizing retention, the committee intends that information acquired, which is not necessary for obtaining[,] producing, or disseminating foreign intelligence information, be destroyed *where feasible*." (emphasis added)). Congress recognized that in some cases, pertinent and non-pertinent information may be co-mingled in such a way as to make it technologically infeasible to segregate the pertinent information from the non-pertinent information and then

[5] The Government notes that at a single point in its June 1 Submission, it incorrectly described the acquisition of a discrete communication that is not to, from, or about a tasked selector within a transaction to be acquired "inadvertently." *See* June 1 Submission at 13 ("The issue for the Court in light of the above-described nature and scope of NSA's upstream collection is whether, in light of a governmental interest 'of the highest order of magnitude,' NSA's targeting and minimization procedures sufficiently protect the individual privacy interests of United States persons whose communications are inadvertently acquired."). However, the Government otherwise consistently described the acquisition of such communications as "incidental," *see, e.g., id.* at 15 ("NSA's upstream collection may incidentally acquire information concerning United States persons within transactions containing multiple discrete communications, only one of which is to, from, or about a person targeted under Section 702."); *id.* at 19 ("The fact that other, non-pertinent information within the transaction may also be incidentally and unavoidably acquired simply cannot render the acquisition of the transaction unreasonable."); *id.* ("[T]o the extent that United States person information is incidentally acquired in the acquisition of a whole transaction by NSA's upstream collection, such information will be handled in accordance with strict minimization procedures."). ~~(TS//SI//NF)~~

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


destroy the latter. *See id.* ("The committee recognizes that it may not be feasible to cut and paste files or erase part of tapes where some information is relevant and some is not."). Here, it is not technologically feasible for NSA to extract, post-acquisition, only the discrete communication that is to, from, or about a tasked selector within a transaction. Thus, in order for NSA to retain the foreign intelligence information within a transaction, it must retain the entire transaction, including any incidentally acquired information about U.S. persons or persons in the United States contained therein. ~~(TS//SI//NF)~~

This incidentally acquired information in transactions is subjected to the same restrictions on use and dissemination that govern information obtained through other means pursuant to Section 702 (such as through collection at Internet Service Providers).[6] The Court has previously found these restrictions on use and dissemination in NSA's current minimization procedures to be consistent with the Act and the Fourth Amendment. *See, e.g, In re DNI/AG Certification* [redacted] Mem. Op. at 8-12 (USFISC [redacted] 2010); *In re DNI/AG Certification* [redacted] Mem. Op. at 8-15 (USFISC [redacted] 2009). Of course, the Government seeks the Court's approval of revised NSA Section 702 minimization procedures that would enable NSA analysts to use United States person identifiers as selection terms if those selection terms are reasonably likely to return foreign intelligence information. As discussed in its response to question 14 below, the Government respectfully suggests that these revised NSA minimization procedures are also consistent with the Act and the Fourth Amendment. ~~(TS//SI//OC/NF)~~

In sum, NSA treats each discrete communication contained within a larger Internet transaction as a separate communication for purposes of its minimization procedures. Although it is possible that certain discrete communications containing United States person information will be retained, as described above, they remain subject to the same restrictions on use and dissemination imposed by NSA's minimization procedures. ~~(TS//SI//OC/NF)~~

**5.a. Once NSA has identified a portion of a transaction that does not contain targeted information, is it possible to mask or otherwise minimize the non-target information contained within the transaction?**

No. The analytic tools used to display the acquired data to NSA analysts do not have a capability to mask information or otherwise minimize the non-target information contained within a transaction. See additional details provided in response to question 6 below. ~~(TS//SI//NF)~~

[6] Moreover, as discussed in response to question 3.b. above, NSA's inability to separate the discrete communications post-acquisition also means that the discrete communications are not displayed in NSA's SC-SSRs as separate communications, but rather clearly retain their connection to the entirety of the original transaction, making it more apparent to NSA analysts the discrete communication's relationship to a tasked selector. ~~(TS//SI//OC/NF)~~

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



**5.b. Why is NSA unable to delete and replace, or alter, an original transaction that contains non-target information? See June 1 Submission at 27-28.**

The answer to this question is included in the response to question 6 below. ~~(TS//SI//NF)~~

**6. The government states that an Internet transaction that is acquired "is... not divisible into the discrete communications within it even once it resides in an NSA corporate store." June 1 Submission at 22. Please reconcile that statement with the government's acknowledgment that "an analyst would . . . be able to copy a portion of the rendered view of a transaction contained in a NSA corporate store and then paste it into a new record on a different system." Id. at 27 n.25.**

As discussed in the example of [redacted] information on pages 27-28 of the June 1 Submission, the data within such transactions is organized in a fashion meant to be displayed using [redacted], which is not necessarily a format in which discrete communications that may be contained within the transaction are distinguishable. In order for NSA to identify and separate a transaction containing multiple communications into those component parts, the transaction would require processing, parsing, and reformatting for those components intended for subsequent retention as separate communications. This is true at the point of acquisition and at any point post-acquisition, including at the point of display to the analyst, whether the intent is to separate out a particular communication from the transaction for the purpose of deleting it, replacing it, masking it, or otherwise altering it. [redacted] ~~(TS//SI//OC/NF)~~

Absent [redacted] capabilities as discussed above, attempts by NSA analysts to delete, replace or otherwise alter (e.g., mask or otherwise minimize the non-target information contained within the transaction) a portion of a transaction intercepted through NSA's upstream collection techniques could similarly corrupt the integrity of the collection, destabilizing -- and potentially rendering unusable -- some or all of the collected transaction, including any particular communication therein for analytic or other purposes. Maintaining the integrity of original transactions is paramount to NSA's retention and dissemination processes. Specifically, NSA has developed and implemented a comprehensive purge process designed to improve the completeness of data purges. The efficacy of this process depends in large measure on NSA's ability to trace data back to the original object (such as a transaction) in a SIGINT Collection - Source Systems of Record (SC-SSR). Maintaining the integrity of original transactions is also important for ensuring quality control of NSA's foreign intelligence analysis of Internet communications, which frequently may contain more than one tasked selector or could be used by more than one analyst, depending on the target, mission, or specific foreign intelligence need to which it pertains. Thus, preserving the integrity of the data is dependent upon the retention of the original transaction in its original form as stored in the SC-SSR. ~~(TS//SI//OC/NF)~~

The government's representation that an Internet transaction that is acquired "is... not divisible into the discrete communications within it even once it resides in an NSA corporate store" was intended to convey that it is not technologically feasible for NSA to create [redacted] processes to divide transactions into discrete communications. Footnote 25 on page 27 of the June 1 Submission refers to the fact that it is possible for individual analysts to copy some of the information from a transaction in NSA corporate stores into a new document or file stored on a separate system, such as a [redacted] *See, e.g.*, DNI/AG 702(g) Certification [redacted] Trans. of Proceedings at 20-21 ([redacted] 2010) (for a discussion of [redacted]). The fact that such a copy or extract can be made, however, does not mean that the underlying transaction can then be altered in the corporate store. For example, if an analyst copied a portion of a transaction from an SC-SSR into a [redacted] and then purged the transaction from the SC-SSR, the data copied into the [redacted] would likewise have to be purged -- even if it contained foreign intelligence information copied from a communication to, from, or about a tasked selector -- because it could no longer be traced back to an object present in an SC-SSR. ~~(TS//SI//OC/NF)~~

**7. Please reconcile the government's statement that the "communicants" of to/from communications are "the individual users of particular selectors" (see June 1 Submission at 30) with [redacted] elsewhere in its response to the Court's questions (see, e.g., id. at 6 (discussing application of IP filtering)).**

The Government believes its statement that [redacted] in the case of to/from communications is fully consistent with the Government's description of how NSA [redacted] to determine if one end of a to/from communication is outside of the United States. As stated on page 30 of the June 1 Submission, the communicants in to/from communications are the individual users who are the senders and intended recipients of those communications, rather than [redacted] ~~(TS//SI//OC/NF)~~

With respect to IP filtering, however, in many instances it is not possible for NSA to [redacted]. *See* June 1 Submission at 6-7. [redacted] *See, e.g., id.* at 11. ~~(TS//SI//OC/NF)~~.

As described in the June 1 Submission, there are scenarios under which NSA could unknowingly and unintentionally acquire a to/from communication in which the sender and all intended recipients are in the United States at the time of acquisition -- for example, if that

communication [redacted][7] In the unlikely event that NSA does unintentionally acquire such a communication, NSA will purge the communication unless its continued retention is authorized by the Attorney General in accordance with 50 U.S.C. § 1806(i). If the communication is itself contained within a transaction that contains other discrete communications, the whole transaction will be purged unless its continued retention is authorized by the Attorney General in accordance with 50 U.S.C. § 1806(i), regardless of whether those other discrete communications are foreign. ~~(TS//SI//OC/NF)~~

**8. What is the factual basis for NSA's assertions that "a United States person would [redacted] only in a minute percentage of cases" and that [redacted]? See June 1 Submission at 11, 12.**

These factual assertions by NSA are based upon the assessments of NSA Signals Intelligence (SIGINT) personnel, who have been involved in NSA's Section 702 acquisitions since the initiation of that collection, and many of whom have experience [redacted] NSA's factual assertions in the June 1 Submission are also based on its review of a sampling of Section 702-acquired communications, which is described on page 9 of the June 1 Submission. As is more fully discussed in that filing, NSA's review of [redacted] records between these two tests revealed only [redacted] records indicative of a non-targeted user [redacted] in the United States. Further research revealed that these [redacted] records were actually copies of the same transaction, and NSA found no indication that any wholly domestic communications were within this transaction. NSA assesses that the results of these tests are consistent with the assessments made by NSA's SIGINT personnel in the June 1 Submission. ~~(TS//SI//OC//NF)~~

**9. What is the factual basis for NSA's suggestion that [redacted]? See June 1 Submission at 8 n.9.**

[redacted]

[7] As previously described, it would be very unlikely for [redacted] in which the sender and all intended recipients are located inside the United States. See June 1 Submission at 11. Moreover, with the previously described limited exception [redacted] *see id.* at 6 & n.5, NSA analysts have yet to identify a wholly domestic communication acquired through NSA's upstream collection systems. *See id.* at 9 (noting NSA's experience to date and describing NSA's test samples, stating that the only records possibly indicative of a United States-based user [redacted] did not reveal that any wholly domestic communications had been acquired). ~~(TS//SI//OC/NF)~~

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



[redacted]

**10. The government repeatedly characterizes as "unintentional" NSA's collection of discrete non-target communications as part of transactional acquisitions, [redacted] Assuming arguendo that such collection can fairly be characterized as unintentional, please explain how 50 U.S.C. § 1806(i) applies to the discrete, wholly domestic communications that might be contained within a particular transaction.**

Subsection 1806(i) provides that "[i]n circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication,[8] under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located in the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicates a threat of death or serious bodily harm to any person." (U)

The Government's June 1 Submission described for the Court that at the time of acquisition, NSA's Section 702 upstream Internet collection devices are generally not capable of distinguishing transactions containing only a single discrete communication to, from, or about a tasked selector from transactions containing multiple discrete communications, not all of which

[8] Subsection 1806(i) originally covered only radio communications, but was amended in 2008 to cover all communications to make it technology neutral. *See* 154 Cong. Rec. S6133 (daily ed. June 25, 2008). (U)

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


may be to, from, or about a tasked selector at the time of acquisition.[9] *See* June 1 Submission at 7, 27-28. The Government considers the acquisition of communications within a transaction that are not to, from, or about a tasked selector to be incidentally acquired communications. However, the Government does not intend to acquire transactions containing communications that are wholly domestic in nature and in fact has implemented [redacted] means to prevent the acquisition of such transactions. While those [redacted] means could fail (as was the case involving the previously reported [redacted], or be circumvented [redacted] NSA is nevertheless not intending to acquire wholly domestic communications. Thus, in the context of acquiring Internet transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector, the Government recognizes that subsection 1806(i) could potentially be implicated to the extent that one of those discrete communications is a communication in which the sender and all intended recipients were located in the United States at the time of acquisition. Accordingly, in the event NSA recognizes a wholly domestic communication which is not to, from, or about a tasked selector which it has unintentionally acquired in the course of conducting its Section 702 upstream Internet collection, NSA would handle the entire transaction in accordance with subsection 1806(i) and either purge it or, if appropriate, seek authorization from the Attorney General to retain it. ~~(TS//SI//OC/NF)~~

NSA's minimization procedures, adopted by the Attorney General in consultation with the Director of National Intelligence, allow the Director of NSA to execute a waiver permitting the retention of wholly domestic communications. *See* Current and Proposed NSA Minimization Procedures, § 5. However, this provision applies to the acquisition of domestic communications when the Government has a reasonable, but mistaken, belief that the target is a non-United States person located outside the United States because NSA is intentionally but mistakenly acquiring such communications.[10] This domestic communications carve-out does not apply to an unintentionally acquired transaction that contains a wholly domestic communication (when recognized as such by NSA) along with other discrete communications, which is not to, from, or about a tasked selector. As described previously, NSA's Section 702 upstream Internet collection devices are generally incapable of distinguishing transactions containing only a single discrete communication to, from, or about a tasked selector from transactions containing multiple discrete communications, not all of which may be to, from, or about a tasked selector at the time of acquisition; moreover, NSA cannot separate transactions containing multiple discrete communications into logical constituent parts post-acquisition. Thus, in the event that NSA's Section 702 upstream Internet collection resulted in the unintentional acquisition of a transaction containing a wholly domestic communication, consistent with subsection 1806(i), NSA would purge the entire transaction, unless the Attorney General has authorized its retention after first

[9] NSA additionally advised the Court that except in certain limited circumstances, NSA cannot separate transactions into logical constituent parts post-acquisition either without rendering the transaction unusable for analytic or other purposes. *See* June 1 Submission at 27 & n.27. ~~(TS//SI//OC/NF)~~

[10] *See* Government's Analysis of Section 1806(i), DNI/AG 702(g) Certification [redacted] Docket No. 702(i)-08-01, filed Aug. 28, 2008; [redacted] Mem. Op. at 25-27. ~~(TS//SI//OC/NF)~~

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


determining that its contents indicated a threat of death or serious bodily harm to any person.[11] ~~(TS//SI//OC/NF)~~

**11. Please provide a thorough legal analysis supporting your view that the knowing and intentional acquisition of large volumes of Internet transactions containing discrete communications that are neither to, from, nor about a targeted selector (as well as other information not pertaining to the users of targeted selectors) is merely "incidental" to the authorized purpose of the collection as a whole, and therefore reasonable under the Fourth Amendment.**

Fourth Amendment reasonableness is concerned only with the effect on Fourth Amendment protected interests. Thus, in evaluating reasonableness under the Fourth Amendment, the relevant issue for the Court in considering the acquisition of communications incidental to the purpose of this collection is the extent to which such incidental communications involve United States persons or persons located in the United States. ~~*Cf.* [redacted] Mem. Op. at 37-38~~ (recognizing that non-U.S. persons outside the United States "are not protected by the Fourth Amendment" (citing *United States v. Verdugo-Urqidez*, 494 U.S. 259, 274-75 (1990)). For the reasons more particularly explained in the Government's responses to question 1 above and question 14 below, most of the communications incidentally acquired pursuant to this collection have no effect on any Fourth Amendment protected interests. The Government acknowledges that it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain information pertaining to United States persons or persons located in the United States. That, however, does not mean that the acquisition of multiple discrete communications is any more likely to result in the acquisition of United States person information than in the collection of single, discrete communications to, from, or about a non-United States person located outside the United States. This is particularly true because the technology NSA uses to prevent the acquisition of wholly domestic communications also acts to limit the acquisition of communications among and between United States persons.[12] ~~(TS//SI//OC/NF)~~

---

[11] See also the Government's response to question 7 above, which explains that there are other scenarios under which NSA could unknowingly and unintentionally acquire a wholly domestic communication. In the unlikely event that NSA does unintentionally acquire such a communication, NSA will purge the communication upon recognition unless its continued retention is authorized by the Attorney General in accordance with subsection 1806(i). If the communication is itself contained within a transaction that contains other discrete communications, the whole transaction will be purged unless its continued retention is authorized by the Attorney General in accordance with subsection 1806(i), regardless of whether those other discrete communications are foreign. ~~(TS//SI//OC/NF)~~

[12] For example, the Court has expressed particular concern regarding the acquisition of [redacted] ~~(TS//SI//OC/NF)~~

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



Moreover, even with respect to those instances in which U.S. person information is acquired, courts in both the FISA and criminal (Title III) contexts have recognized that the acquisition of communications incidental to the purpose of a collection may be necessary to achieve the goal of a search or surveillance, as well as reasonable under the Fourth Amendment. *See, e.g., In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1015 (Foreign Int. Surv. Ct. Rev. 2008) (hereinafter "*In re Directives*") ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.") (citations omitted)); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000), *aff'd sub nom. In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157 (2d Cir. 2008), *cert. denied sub nom. El-Hage v. United States*, 130 S.Ct. 1050 (2010) ("[I]ncidental interception of a person's conversations during an otherwise lawful [Title III] surveillance is not violative of the Fourth Amendment."). ~~(TS//SI//OC/NF)~~

In cases where NSA acquires Internet transactions that include multiple discrete communications, the Government considers any discrete communications not to, from, or about the tasked selector to be incidentally acquired. Specifically, the Government's purpose in acquiring such a transaction is to acquire the foreign intelligence information likely contained within the discrete communication to, from, or about a tasked selector. However, because it is technologically infeasible for NSA's upstream collection systems to extract only the discrete communication that is to, from, or about a tasked selector, the only way to obtain the foreign intelligence information in that discrete communication is to acquire the entire transaction. Thus, the acquisition of the other discrete communications within the transaction is properly considered "incidental," because it is a necessary but unavoidable consequence of achieving the Government's goal of acquiring the foreign intelligence information contained within the discrete communication to, from, or about a tasked selector. *See* H.R. Rep. No. 95-1283, pt. 1, at 55 (1978) (noting that "in many cases it may not be possible for technical reasons to avoid acquiring all information" when conducting foreign intelligence surveillance); *see also id.* at 56 ("[I]t may not be possible or reasonable to avoid acquiring all conversations."); *cf. United States v. McKinnon*, 721 F.2d 19, 23 (1st Cir. 1983) ("Evidence of crimes other than those authorized in a [Title III] wiretap warrant are intercepted 'incidentally' when they are the by-product of a bona fide investigation of crimes specified in a valid warrant."). ~~(TS//SI//OC/NF)~~

That is not to say, however, that the acquisition of non-pertinent information is reasonable in all cases simply because the collection of that information is "incidental" to the purpose of the search. *United States v. Ulrich*, 228 Fed. Appx. 248, 252 (4th Cir. 2002) (noting that "fishing expeditions" or "a random exploratory search or intrusion" violate the Fourth Amendment) (quotation marks omitted). Here, NSA's acquisition of transactions is conducted in accordance with FISC-approved targeting procedures reasonably designed to ensure that the acquisitions are directed "toward communications that are likely to yield the foreign intelligence information sought, and thereby afford a degree of particularity that is reasonable under the Fourth Amendment." [redacted] Mem. Op. at 39-40 (footnote omitted). The fact that such transactions may contain non-pertinent information -- even in significant amounts -- does not by itself render the acquisition of those transactions unreasonable under the Fourth Amendment. *See Scott v. United States*, 436 U.S. 128, 140 (1978) (recognizing that "there are surely cases,

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


such as the one at bar [involving a Title III wiretap], where the percentage of nonpertinent calls is relatively high and yet their interception was still reasonable"); *Abraham v. County of Greenville*, 237 F.3d 386, 391 (4th Cir. 2001) ("[I]ncidental overhearing is endemic to surveillance."); *United States v. Doolittle*, 507 F.2d 1368, 1372 (5th Cir. 1975) ("There is no question that some irrelevant and personal portions of gambling conversations were intercepted or that certain nonpertinent conversations were intercepted. But this is inherent in the type of interception authorized by Title III, and we do not view the simple inclusion of such conversations, without more, as vitiating an otherwise valid wiretap.")[13]; *see also, e.g., Board of Educ. v. Earls*, 536 U.S. 822, 837 (2002) ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotations marks omitted)). ~~(TS//SI//OC/NF)~~

As such, the incidental collection at issue here is reasonable under the Fourth Amendment because it is a necessary and unavoidable by-product of NSA's effort to obtain the foreign intelligence information contained within a discrete communication that is a part of a larger transaction which could contain non-pertinent communications. *See United States v. Wuagneux*, 683 F.2d 1343, 1352-53 (11th Cir. 1982) (observing that "a search may be as extensive as reasonably required to locate the items described in the warrant," and on that basis concluding that it was "reasonable for the agents [executing the search] to remove intact files, books, and folders when a particular document within the file was identified as falling within the scope of the warrant"); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence sought may be seized"). Moreover, as described in the response below, NSA takes the steps it can to ensure that it conducts its Section 702 upstream collection in a manner that minimizes the intrusion into the personal privacy of United States persons. ~~(TS//SI//OC/NF)~~

**12. The statute requires the targeting procedures to "be reasonably designed to ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States and [to] prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). How can procedures that contemplate the knowing acquisition of huge volumes of transactions that will include quantifiable amounts of information relating to non-targets, including information of or about U.S. persons abroad or persons located in the United States, meet this statutory requirement?**

[13] These cases upholding the Fourth Amendment reasonableness of Title III surveillances that resulted in the acquisition of significant amounts of nonpertinent communications are particularly noteworthy given that Title Iain's requirement to minimize the acquisition of such communications is considerably stricter than FISA's. *See* H.R. Rep. 95-1283, pt. 1, at 56 ("It is recognized that given the nature of intelligence gathering, minimizing acquisition should not be strict as under [Title III] with respect to law enforcement surveillances."). ~~(TS//SI//NF)~~

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


For the reasons more particularly discussed in its response to question 1.b.ii. in the June 1 Submission, which took into account the means by which communications to, from, or about a tasked selector are acquired through NSA's upstream Internet collection techniques, the Government respectfully submits that NSA's targeting procedures are reasonably designed to ensure that an authorized acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located within the United States. *See* June 1 Submission at 3-12, 20-24. As discussed in the Government's June 1 Submission, for acquisition of both to/from communications and abouts communications, the person being "targeted" is the user of the tasked selector, who, by operation of the targeting procedures, is a non-United States person reasonably believed to be located outside the United States. *See* June 1 Submission at 3-4. This remains true for all Section 702 upstream acquisitions, including the acquisition of transactions containing several discrete communications, only one of which may be to, from, or about the user of a tasked selector. ~~(TS//SI//NF)~~

Specifically, the sole reason a transaction is selected for acquisition is that it contains the presence of a tasked selector used by a person who has been targeted in accordance with NSA's targeting procedures.[14] Indeed, at the time a transaction is acquired, NSA cannot always know whether the transaction includes other data or information representing communications that are not to, from, or about the target, let alone always have knowledge of the parties to those communications. *Cf.* [redacted] Mem. Op. at 18-19 (noting that with respect to abouts communications, "the government may have no knowledge of [the parties to a communication] prior to acquisition"). It therefore cannot be said that the acquisition of a transaction containing multiple discrete communications results in the intentional targeting of any of the parties to those communications other than the user of the tasked selector. *Cf. Bin Laden*, 126 F. Supp. 2d at 281 (acknowledging that in light of *United States v. Verdugo-Urquidez*, 494 U.S. 259, 265 (1990), and Title III "incidental interception" case law, overseas surveillance of a United States person terrorism suspect would have posed no Fourth Amendment problem "if the Government had not been aware of [his] identity or of his complicity in the [terrorism] enterprise"). The fact that a transaction acquired pursuant to the targeting procedures may also contain communications to, from, or about persons other than the user of the tasked selector does not mean those persons are likewise being targeted by that acquisition. *Cf.* H.R. Rep. No. 95-1283, pt. 1, at 50 (explaining, with regard to electronic surveillance as defined by 50 U.S.C. § 1801(f)(1), that "[t]he term 'intentionally targeting' includes the deliberate use of surveillance techniques which can monitor numerous channels of communication among numerous parties, where the techniques are designed to select out from among those communications the communications to which a particular U.S. person located in the United States is a party, and where the communications are

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

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


selected either by name or by other information which would identify the particular person and would select out his communications"). Rather, as discussed in the response to question 11 above, the acquisition of such non-pertinent communications is incidental to the purpose of the collection as a whole and therefore reasonable under the Fourth Amendment. ~~(TS//SI//NF)~~

Similarly, to the extent that one of the discrete non-pertinent communications within an acquired transaction is a communication in which the sender and all intended recipients were located in the United States at the time of acquisition, the acquisition of this wholly domestic communication would be incidental and, as discussed in response to question 10 above, unintentional. NSA's targeting procedures require that, in conducting upstream collection of abouts communications, NSA either employ "an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas" or '[redacted]' *E.g.*, Amendment 1 to DNI/AG 702(g) Certification [redacted] Ex. A, filed [redacted] 2010, at 1-2; *see also* [redacted] Mem. Op. at 19. The Court has previously found that these [redacted] means were "reasonably designed to prevent the intentional acquisition of communications as to which all parties are in the United States," while recognizing that it is "theoretically possible that a wholly domestic communication could be acquired as a result of the [redacted] Mem. Op. at 20 & n.17. As discussed in the June 1 Submission, apart from one exception involving [redacted] NSA analysts have yet to identify a wholly domestic communication acquired through NSA's upstream collection systems. *See* June 1 Submission at 8-9. Accordingly, the Government continues to believe that NSA's [redacted] means for preventing the acquisition of wholly domestic communications remain efficacious, and that the theoretical scenarios in which NSA would acquire a wholly domestic communication do not prevent the Court from continuing to find that NSA's targeting procedures are reasonably designed to prevent the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be in the United States. ~~(TS//SI//OC/NF)~~

To the extent that NSA does unintentionally acquire and then recognize such a wholly domestic communication within an acquired transaction, as described in response to question 10 above, NSA would be required to purge the entire transaction, unless the Attorney General determined "that the contents indicate[d] a threat of death or serious bodily harm to any person." ~~(TS//SI//OC/NF)~~

**13. In its discussion of the Fourth Amendment, the government asserts that "upstream collection" in general is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs." June 1 Submission at 16.**

**a. To what extent can the same be said for the acquisition of Internet transactions [redacted] in particular?**

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



**b. Is the acquisition of Internet transactions via upstream collection the only source for certain categories of foreign intelligence information? If so, what categories?**

**c. Please describe with particularity what information NSA would acquire, and what information NSA would not acquire, if NSA were, in comparison to its current collection, to limit its acquisition of Internet communications to: (1) acquisitions conducted with the assistance of [redacted]; and (2) the upstream collection of discrete communications to, from, or about tasked selectors that are [redacted] (id. at 2, n.2).**

The Government's assertion that upstream collection is "an essential and irreplaceable means of acquiring valuable foreign intelligence information that promotes the paramount interest of protecting the Nation and conducting its foreign affairs" is equally applicable to its acquisition of Internet transactions. This is true because the Government's acquisition of Internet transactions is not a subset of its upstream collection of Internet communications. Instead, acquisition of Internet transactions is the technical means by which all upstream collection of Internet communications accounts are acquired. ~~(TS//SI//NF)~~

Section 702 upstream collection of Internet communications provides NSA with certain types of information (further described below) which are extremely valuable to its national security mission. Disseminated end product reports derived from this collection have proven to be of critical value to high-level customers, including the White House, State Department, Joint Chiefs of Staff, the National Counterproliferation Center, Central Intelligence Agency (CIA), Defense Intelligence Agency, Federal Bureau of Investigation (FBI), and others. In addition,

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

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

Section 702 upstream collection offers unique opportunities to detect target information, including but not limited to the following examples:

[redacted]

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


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

[redacted] As such, and as the Court has recognized, NSA's upstream collection is "*uniquely capable* of acquiring certain types of targeted communications containing valuable foreign intelligence information." *In re DNI/AG Certification* [redacted] Mem. Op. at 25-26 (USFISC [redacted] 2009) (emphasis added; internal citations omitted). ~~(TS//SI//NF)~~

Additionally, NSA's Section 702 upstream collection would not acquire many of the above categories of communications, and thus the foreign intelligence contained within these communications, if NSA's upstream collection were limited to acquisition solely of discrete communications to, from, or about tasked selectors that are [redacted] referenced in footnote 2 on page 2 of the June 1 Submission. Currently, [redacted] ~~(TS//SI//NF)~~

15 [redacted]

(TS//SI//NF)

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



[redacted]

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

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

The Court's question asks for "categories of foreign intelligence information" that can be obtained exclusively through NSA's acquisition of Internet transactions via upstream collection. This is a difficult question to answer, as types of foreign intelligence may be conveyed through a variety of communication means. For example, [redacted] as described above, it is entirely possible that this communication may only be acquired through NSA's Section 702 upstream collection of communications other than those [redacted] ~~(TS//SI//NF)~~

In an effort to fully answer the Court's question, however, the Government respectfully submits the following examples of instances where NSA has obtained substantial foreign intelligence information from Section 702 upstream collection. The examples detail only a few

[redacted]

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

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



of the many instances in which Section 702 upstream collection has provided such substantial foreign intelligence. In many of these examples, Section 702 upstream collection provided important leads that led to [redacted]. Although all forms of Section 702 upstream collection have proved to be of critical importance to the NSA's national security mission, the examples below involve the acquisition by Section 702 upstream collection of communications other than [redacted]
~~(TS//SI//NF)~~

[redacted] ~~(S)~~

[redacted]

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

[redacted] (S)

[redacted]

[redacted]

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


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

[redacted] ~~(U//FOUO)~~

[redacted]

**14. The Fourth Amendment also requires the Court to examine the nature and scope of the intrusion upon protected privacy interests. How can the Court conduct such an assessment if the government itself is unable to describe the nature and scope of the information that is acquired or the degree to which the collection includes information pertaining to U.S. persons or persons located in the United States?**

Although, as discussed above, it is difficult for the Government to fully describe to the Court every possible type of information that may be contained within a transaction acquired through NSA's upstream collection, the Government respectfully suggests that the Court can nonetheless assess whether NSA's upstream collection of such transactions is reasonable under the Fourth Amendment. ~~(TS//SI//OC/NF)~~

First, the Supreme Court has recognized that an appreciation of all of the possible ways a search can intrude upon interests protected by the Fourth Amendment is not an indispensable component of assessing the reasonableness of the search. *See Dalia v. United States*, 441 U.S. 238, 257 (1979) ("Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant."); *cf. Payton v. New York*, 445 U.S. 573, 601-02 (1980) (recognizing that "for Fourth Amendment purposes, an arrest warrant founded on probable cause implicitly carries with it the limited authority to enter a dwelling in which the suspect lives when there is reason to believe the suspect is within," even though "an arrest warrant requirement may afford less [privacy] protection than a search warrant requirement"). Thus, the Government respectfully suggests that the Court can assess the Fourth Amendment reasonableness of NSA's upstream collection even if the Government cannot fully describe every possible type of information that collection may acquire. ~~(TS//SI//OC/NF)~~

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



Moreover, while it may be difficult for the Government to describe the full scope of the types of information that may be acquired by NSA's upstream collection, it is nevertheless possible to ascertain the degree to which that information would pertain to United States persons or persons located in the United States. For the reasons discussed below, the Government does not believe that information about United States persons or persons located in the United States would be acquired through NSA's upstream collection of transactions to a greater degree, in relative terms, than other types of communications acquired under Section 702. ~~(TS//SI//OC/NF)~~

First, certain transactions are acquired because they contain a discrete communication to or from a tasked selector used by a person who, by virtue of the application of NSA's FISC-approved targeting procedures, is a non-United States person reasonably believed to be located outside the United States. This Court has recognized that "the vast majority of persons who are located overseas are non-United States persons and that most of their communications are with other, non-United States persons, who are located overseas." *In re Directives to Yahoo!* Mem. Op. at 87 (footnote omitted). Accordingly, it is reasonable to presume that most of the discrete communications that may be within the acquired transaction are between non-United States persons located outside the United States. Second, with respect to transactions that contain a discrete communication about a tasked selector, the technical means by which NSA prevents the intentional acquisition of wholly domestic communications is to ensure that the acquisition of transactions is directed at persons reasonably believed to be located outside the United States. Again, these individuals reasonably can be presumed to be non-United States persons, and most of their communications can be presumed to be with other non-United States persons located outside the United States. *Id.* This combination of targeting non-United States persons located outside the United States and directing acquisitions at persons located outside the United States operates to significantly diminish the likelihood that information pertaining to United States persons or persons in the United States will be acquired. ~~(TS//SI//OC/NF)~~

To be sure, it is possible that a transaction containing multiple discrete communications only one of which is to, from, or about a tasked selector could contain information pertaining to United States persons or persons in the United States. That, however, does not by itself mean that the volume of such information in transactions will be greater than in the collection of other types of communications that have previously been discussed and approved.

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

Moreover, the fact that within an acquired transaction there may be multiple discrete communications containing information pertaining to United States persons or persons in the United States cannot by itself render the acquisition of that transaction unreasonable under the Fourth Amendment. As discussed above, the acquisition of such information is incidental to the purpose of the transaction's acquisition -- the acquisition of the discrete communication(s) to,

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



from, or about a tasked selector within the transaction. *See In re Directives*, 551 F.3d at 1015 ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.") (citations omitted)). ~~(TS//SI//OC/NF)~~

In any event, any information pertaining to a United States person or person located in the United States present in a transaction containing multiple discrete communications would be handled under the NSA minimization procedures in the exact same manner as if that information appeared in a discrete communication to, from, or about a tasked selector. For example, the use and dissemination of United States person information acquired from a [redacted] would be subject to the same restrictions as United States person information acquired from [redacted] ~~(TS//SI//OC/NF)~~

**15. In light of the government's emphasis on the limited querying of Section 702 acquisitions that is currently permitted (see June 1 Submission at 23), why is it reasonable and appropriate to broaden the targeting procedures to permit querying using U.S.-person identifiers?**

Although NSA's current minimization procedures prohibit the use of United States person names or identifiers to retrieve any Section 702-acquired communications in NSA systems, *see* Current NSA Minimization Procedures, § 3(b)(5), the statute requires no such limitation. Rather, it is reasonable and appropriate for the Court to approve the Government's proposal to enable NSA analysts to use United States person identifiers as selection terms because the request is consistent with the statutorily required minimization procedures. *See* Proposed NSA Minimization Procedures § 3(b)(5) (providing, in pertinent part, that "[c]omputer 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*. Any United States person identifiers used as terms to identify and select communications must be approved in accordance with NSA procedures.") (emphasis added). ~~(TS//SI//OC/NF)~~

Minimization procedures must be designed to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly availably information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. 50 U.S.C. § 1801(h)(1). Where, as here, "it may not be possible for technical reasons to avoid acquiring all information," Congress has recognized that minimization procedures "must emphasize the minimization of retention and dissemination." H.R. Rep. No. 95-1283, pt. 1, at 55. Congress also acknowledged that "a significant degree of latitude be given in counterintelligence and counterterrorism cases" with respect to retention and dissemination of information. *Id.* at 59. In light of such latitude, "rigorous and strict controls" should -- and will -- be placed on the retrieval of United States person information and "its dissemination or use for purposes other than counterintelligence or counterterrorism." *Id.* ~~(TS//SI//OC/NF)~~

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



With respect to acquisition, the Government's proposal to use United States person identifiers as selection terms does not broaden the scope of what the Government can acquire under the certifications. Because, for the reasons detailed above, it is not possible "to avoid acquiring" the incidentally obtained information, the focus will be on the retention and dissemination provisions of the procedures. *Id.* at 55. As a general matter, NSA's minimization procedures contain detailed provisions regarding the retention and dissemination of United States person information that the Court has previously approved. *See, e.g.* [redacted] Mem. Op. at 21-32, 40-41. In addition, the Government's proposal provides that United States person identifiers may only be used "in accordance with NSA procedures" governing the circumstances under which U.S. person information can be queried. Although the Government is still developing such procedures, and NSA analysts will not begin using United States identifiers as selection terms until they are completed, the Government will ensure that the procedures contain "rigorous and strict controls" for the retrieval and dissemination of United States person information to ensure that only selection terms likely to produce foreign intelligence information are retrieved, and dissemination is limited to counterintelligence and counterterrorism purposes. Moreover, the Government's proposed changes to NSA's minimization procedures require that NSA maintain records of all United States person identifiers approved for use as selection terms and that NSD and ODNI conduct oversight of NSA's activities. *See* Proposed NSA Minimization Procedures § 3(b)(5). ~~(TS//SI//OC/NF)~~

**16. The government acknowledges that it previously "did not fully explain all of the means by which . . . communications are acquired through NSA's upstream collection techniques" (June 1 Submission at 2), yet states that the "[Attorney General] and [Director of National Intelligence] have confirmed that their prior authorizations remain valid" (id. at 35). At the time of each previous Certification under Section 702, were the Attorney General and the Director of National Intelligence aware that the acquisitions being approved included Internet "transactions" [redacted]? If so, why was the Court not informed? If not, why are the prior Certifications and collections still valid?**

The Government acknowledges that its prior representations to the Court -- and to the Attorney General and Director of National Intelligence -- regarding the steps NSA must take in order to acquire single, discrete communications to, from, or about a tasked selector did not fully explain all of the means by which such communications are acquired through NSA's upstream Internet collection techniques. *See* June 1 Submission at 2. That said, for the reasons described in the answer to question 5 in the June 1 Submission, both the prior Certifications and collection remain valid. *See* June 1 Submission at 31-38. ~~(TS//SI//OC/NF)~~

The Certifications executed by the AG and DNI and submitted to the Court for approval were based on an understanding that Section 702 collection would, at a minimum, acquire discrete communications that are to, from, or about a tasked selector. As described in detail previously, due to certain technological limitations, in general the only way that NSA can acquire certain Internet communications upstream that are to, from, or about a tasked selector is by acquiring an Internet transaction which may include a single, discrete communication to, from, or about a tasked selector (e.g., an e-mail message) or may include several discrete

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


communications, only one of which may be to, from, or about a tasked selector.[17] *See* June 1 Submission at 27-28. In this respect, the acquisition is comparable to the Government's seizure of a video, book, or intact file that contains a single photo, page, or document that a search warrant authorizes the Government to seize. *See, e.g., United States v. Rogers*, 521 F.3d 5, 10 (1st Cir. 2008) (concluding that a videotape is a "plausible repository of a photo" and that therefore a warrant authorizing seizure of "photos" allowed the seizure and review of two videotapes, even though warrant did not include videotapes); *Wuagneux*, 683 F.2d at 1353 (holding that it was "reasonable for the agents to remove intact files, books and folders when a particular document within the file was identified as falling within the scope of the warrant."); *United States v. Christine*, 687 F. 2d 749, 760 (3d Cir. 1982) (*en banc*) (emphasizing that "no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision. Nor does the Fourth Amendment prohibit seizure of an item, such as a single ledger, merely because it happens to contain other information not covered by the scope of the warrant."); *United States v. Beusch*, 596 F.2d 871, 876-77 (9th Cir. 1979) (rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence may be seized"). None of these cases even hint that the warrant is somehow invalid because the magistrate did not know in advance that the search or seizure of authorized documents or photos would also encompass the search or seizure of additional, intermingled documents or photos, even in cases where such documents could have been physically separated from the larger files or books in which they were contained. Rather, it is well-established that warrants need not state with specificity the precise manner of execution, and, so long as it is reasonable, a search or seizure will be upheld even if conducted in a manner that invades privacy in a manner not considered at the time the warrant was issued. *See United States v. Grubbs*, 547 U.S. 90, 98 (2006) ("Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed.") (citation omitted); *Dalia,* 441 U.S. at 259 ("Often in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant."). ~~(TS//SI//OC/NF)~~

Moreover, having considered the additional information that is being presented to this Court, the AG and DNI have confirmed that the collection fully complies with the statutory requirements of Section 702, as well as the Fourth Amendment, and that therefore the prior Certifications and collection remain valid. *See* June 1 Submission at 35. ~~(TS//SI//OC/NF)~~

As discussed previously, transactions are only acquired if they contain at least one discrete communication to, from, or about a tasked selector. Each tasked selector has undergone review, prior to tasking, to ensure that the user is a non-United States person reasonably believed to be outside the United States. Moreover, with respect to "abouts communications," the targeting procedures are also reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known to be located in the

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

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



United States at the time of acquisition. *See id.* at 3-12, 28-30. Just as the Government's acquisition of an entire book based on the fact that a single page falls within the scope of the warrant does not call into question the warrant's specificity, the incidental acquisition of additional communications that are not to, from, or about the tasked selector does not negate the validity of the targeting procedures that are relied on to acquire a particular transaction. ~~(TS//SI//OC/NF)~~

Moreover, the AG and DNI have confirmed that the additional information regarding incidentally acquired communications does not alter the validity of their prior Certifications. *See id.* at 35. As discussed in detail previously, the minimization and targeting procedures fully comport with all of the statutory requirements, including the requirement that the targeting procedures are reasonably designed to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located within the United States, *see id.* at 3-12, 20-24; and the procedures and guidelines are consistent with the requirements of the Fourth Amendment, *see id.* at 13-24. ~~(TS//SI//OC/NF)~~

DECLARATION OF SCOTT BRADNER

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

# Appendix S

This document was also filed as ECF No. 168-30 and can be found in this Joint Appendix at JA3193.

DECLARATION OF SCOTT BRADNER

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

# Appendix T

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2014 JUL 28 PM 3:56
LEEANN FLYNN HALL
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 (FISA or "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. (S) 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 [redacted]

~~(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 [redacted]; (2) they conduct research [redacted] to determine whether NSA knows the location of the person, or knows information that would provide evidence concerning that location; and (3) they conduct [redacted] 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.

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

~~(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 overseas, or [redacted] 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 [redacted]

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

[redacted]

**~~(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, [redacted], 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, [redacted]

[redacted]

~~(S)~~ **NSA** [redacted]

~~(S)~~ NSA may also [redacted] 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:

[redacted]

~~(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, [redacted] 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 [redacted]

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


[redacted]

~~(S)~~ [redacted]

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

~~(S)~~ In assessing whether the target possesses, is expected to receive, 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:

- [redacted]

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

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


- [redacted]

b. With respect to Internet communications:

- [redacted]

[redacted]

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


- [redacted]

## 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:

a) ~~(S)~~ For telephone numbers:

- [redacted]
- 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.

b) ~~(S)~~ For electronic communications [redacted]

- Routinely checking all electronic communications [redacted] tasked pursuant to these procedures [redacted] to determine if an electronic communications [redacted] was accessed from inside the United States. [redacted]

[redacted]

[redacted]

- [redacted]

- 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.[2]

~~(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. [redacted].

~~(S)~~ NSA analysts will also analyze content for indications that a target is a United States person.[3] Such content analysis will be conducted according to analytic and intelligence requirements and priorities. If NSA determines that a target who at the time of targeting was believed to be a non-United States person is believed to be 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. (S) 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

---

[2] ~~(S)~~ [redacted]

[3] ~~(S)~~ [redacted]

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, [redacted] 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. ~~(S)~~ OVERSIGHT AND COMPLIANCE

~~(S)~~ NSA will implement a compliance program, and will conduct ongoing oversight, with respect to its exercise of the authority under section 702 of the Act, including the associated targeting and minimization procedures adopted in accordance with section 702. NSA 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. NSA 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. NSA 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. NSA will also ensure that necessary corrective actions are taken to address any identified deficiencies. To that end, NSA 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 approximately once every two months.

~~(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 is believed to be 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. ~~(S)~~ 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.

7/24/14
Date

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

DECLARATION OF SCOTT BRADNER

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

# Appendix U

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. ~~TOP SECRET//COMINT//ORCON, NOFORN~~ Approved for Public Release


FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE: DNI/AG 702(g) CERTIFICATION [redacted] (S)

[redacted], 2008

Washington, D.C.

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE MARY A. McLAUGHLIN
UNITED STATES FISC JUDGE

APPEARANCES:

Department of Justice: [redacted]
MATTHEW OLSEN

National Security Agency: [redacted]

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


P R O C E E D I N G S

THE COURT: Good morning again, everyone, and we are on the record. Well, thank you all for coming. I really appreciate it. Before I swear in the nonlawyers who will be speaking, let me just get everybody to introduce themselves, at least those who may be participating in this, and that perhaps I guess could be everybody. Is this [redacted] to my far left and [redacted] And then go ahead, sir.

[redacted]: [redacted], National Security Division.

THE COURT: All right.

[redacted]: [redacted] from the National Security [redacted]

MR. OLSEN: Matt Olsen from National Security [redacted]

THE COURT: Then we're with [redacted]

[redacted] FBI.

[redacted], FBI.

[redacted], FBI Office of General [redacted]

[redacted] from NSA General Counsel's [redacted]

THE COURT: And especially those in the back, please speak up so the court reporter can hear you and the little mic can pick up. So that was [redacted] and this is?

[redacted]: I'm [redacted] the FISA technical lead from Oversight and Compliance at NSA.

THE COURT: Thank you. Yes, ma'am.

(b)(6) [redacted] I'm here on behalf of the Director of National Intelligence, Office of General Counsel.

[redacted]: [redacted] from NSA/OGC.

[redacted]: [redacted] from NSA.

[redacted] (b)(6): I'm (b)(6) [redacted] from the Office of General Counsel for CIA.

THE COURT: Very good. And why don't we have our staff introduce themselves as well.

(b)(6) [redacted]

THE COURT: All right. Thank you.

Now I would like to swear in the nonlawyers who may be speaking today. Whoever that consists of, do you want to rise? I'll do it all at one time. All right.

(The witnesses are sworn.)

THE COURT: Well, let me state for the record why we're here, although I think we all do know why we're here.

The purpose of today's hearing is for the Court to receive additional information and/or clarification with respect to its judicial review under section 702(i) of the FISA Amendments Act of 2008.

The Court, of course, did receive from the government on August 5, 2008, an ex parte submission entitled "Government's Ex Parte Submission of [redacted] and Related Procedures and Requests for an Order Approving Such Certification and Procedures."

At that point, the Court reviewed the submission, as the staff did, and after that the staff met with certain members of the government and relayed my questions and their questions to the government. We then received yesterday, August 26, a document entitled "Government's Preliminary Responses to Certain Questions Posed By the Court."

That was very helpful to get that, and I know you must have had to work hard to put it together on such short notice. So I appreciate it, and it was very helpful.

What I'd like to do today is go over some questions that I still have. I think your written response answered -- the questions that you did deal with I think were answered completely, and I probably won't be doing too much with them. I may just want to confirm a couple of things.

Then I have some additional questions that I think probably you're prepared for because the staff raised them, but I didn't

see them in your responses. Okay?

All right. Let me just start with, again, this first couple things I'm doing relates to what you filed yesterday, and again it's just to sort of pinpoint a couple of things on page 5 of yesterday's submission where you were responding to my question concerning [redacted]

In particular, I raise the issue of some concern about the phrase [redacted]

And you did a lengthy response to that, and I appreciated it, and I just want to sort of confirm and hone in on the fact that it is going to be a situation where you're all going to try -- they're going to try to figure out whether this person is a U.S. person. That was the only issue I had, was what's the due diligence that will go on.

And especially I'm impressed with the second bullet point where you said, [redacted] And then you go on and elaborate.

So I just want to get a confirmation that this is not a situation where, [redacted]

[redacted] I mean, it's after due diligence and analysis [redacted] That is correct, Your Honor. As you know, the statute requires us to have a reasonable belief that a target is located outside the United States. The targeting procedures are designed to ensure that NSA analyzes information that gives rise to that reasonable belief. So it is the targeting procedures that imposes the due diligence requirement on the NSA in that respect.

THE COURT: Okay. That's fine. And I think that answers my question.

My next question with respect to what you had given us is on No. 6, page 7, and it's the discussion of the post targeting analysis done by NSA in the targeting procedures, and my question was the procedure said that that [redacted] and I sort of asked that that be fleshed out a little bit, and you all did, and the first two points I understand.

I wasn't too sure, though, what the meaning of the third bullet point was. I mean, I understand the words, but I'm wondering if someone could flesh that out for me a little. It says, "In all cases, analysts remain responsible for following their target's location and for the validity of continued acquisition of information regarding the target."

[redacted] It's my understanding -- and, [redacted] correct me if I'm wrong -- NSA analysts track particular targets. So it is the analyst who determines the extent to which they need to rely on content analysis to determine a target's location as opposed to something more [redacted]. But it is ultimately the analyst's responsibility for maintaining a reasonable belief that that target is located outside the United States.

And I don't know if you'd like to elaborate on that, [redacted]

[redacted] That's correct, and every selector that goes into an NSA [redacted] database has an analyst's name identified with that so we know who bears the ultimate responsibility, and we have processes set up in place to ensure they're doing their work.

THE COURT: Could you just do a minute or two on the processes?

[redacted]: Yes, ma'am. How far back should I start?

THE COURT: I don't know what that means, "how far back," but just hone in on the fact that they're responsible for following their target's locations; in other words, for following it and the validity of the continued acquisition. So having made the initial foreignness determination, how do you go about making sure they are remaining responsible?

[redacted] The first thing they would do, they would [redacted]

[redacted] And if NSA did intercept information, the first thing they would be responsible for would be to review the content of that information to ensure they got the right target and that it was providing foreign intelligence.

Once they do that, they're going to periodically check that depending on [redacted] the analyst has to ensure that they've reviewed that target and that it is meeting a foreign intelligence purpose.

THE COURT: Okay. Any of the staff have any questions on that topic before I move away from it?

All right. Now, this next one relates to an issue that came up at the December '07 hearing before Judge Kotelly on the Protect America Act, and it relates to oversight reviews.

Obviously, the targeting procedures that we're talking about now, at least with respect to the location of potential targets, are similar to what was reviewed by Judge Kotelly and requires oversight reviews by personnel of Justice and the Office of the Director of National Intelligence.

I read the transcript of the hearing before Judge Kotelly, and she took a lot of testimony concerning the oversight up to that point. Can somebody fill me in on where we are today on

that? Has the methodology that's been used by the reviewers changed at all? Could somebody summarize the results of those reviews?

(b)(6); (b)(7)(C) The methodology has been changed. It's been refined. Back in December, because of the volume of selectors and because we hadn't worked through an exact process in how we would conduct our oversight, we weren't in a position to be able to review every single tasking decision that the NSA had made.

We would do it on a sampling basis. Sometimes we randomly picked certain days and we would look at tasking decisions for those days, or if we had a range of selectors that had been tasked, we would randomly select the sources of information upon which the foreignness determinations for those particular selectors were based.

Since then, we've refined our process such that we're actually able to at the very least receive all of the documentation concerning every single tasking decision that NSA has made. Typically, they're sent to us in electronic format.

So we receive those, we print them off, and we review them to make sure that all of the documentation that the targeting procedures require is present, that being a notation about the foreign intelligence purpose of the collection and the source of the information upon which the foreignness determination for that particular selector was based.

~~As~~ we've gone on and we've refined our methodology and we've had back-and-forth with NSA over how we can improve their performance with respect to filling out particular fields in the sheets, as a result of that back-and-forth, we've actually had to review less and less sources because NSA is relying more and more on [redacted] we don't necessarily need to review per se.

I mean, the most common source of information that NSA relies upon is [redacted] selector is used by a [redacted] So therefore, we don't necessarily need to delve into too much more behind that foreignness determination [redacted]

[redacted]

So I guess in a nutshell, we've been able to do basically

more oversight because our oversight over time has become more efficient.

THE COURT: And how about -- and maybe you've in one sense maybe answered this in part, but what's the result of the reviews been? What are the problems you're seeing at this point?

(b)(6); (b)(7)(C) I would say the most common problem -- and "common" is a relative term here, because the volume of selectors is huge, and the number of problems that we're actually seeing is relatively small. As I've said, as we've engaged in oversight and engaged NSA in discussions on how they can improve the sheets and tasking determinations and things of that nature, the number of problems that we've seen have diminished over time.

I would say the most common problem is to the extent that a tasking determination is based on a wide range of information, there may be a problem with how the source of that information is cited, whether it be somebody just inadvertently mistyped [redacted] or inadvertently left out a [redacted] a key piece of information that was part of the broader range of circumstances upon which NSA made its foreignness determination.

So it's more the little technical things that we've been seeing problems with on a very small scale, and as I've said, it's diminished over time.

THE COURT: I think before Judge Kotelly you identified about [redacted] cases where it appeared that a targeted person was in the U.S., and again, I don't even think I know what time frame that was for, but in any event, can you do anything like that now? I mean, since that hearing in December of '07.

(b)(6); (b)(7)(C) Since that time, that number captured a number of different types of incidents that were reported to us. There are incidents where there's true noncompliance with the targeting procedures that results in basically an improper tasking, whether it be because the person was actually located in the United States or the person was a U.S. person and we did not have 2.5 authority to target that person.

That number also captured instances where NSA had a reasonable belief that the person was located outside the United States at the time of targeting but since that time has roamed into the United States, what we call a "roaming incident."

A third type of incident that that number captured is what we would call a tasking error where NSA would run a particular facility through its targeting procedures but in the act of actually targeting that, by keying in the account or phone number into the tasking tool, there was a typo or something of that nature.

At the time of the hearing, we hadn't fully determined which incidents fell necessarily into which category. Since

that time, we've had an opportunity to do that. And for incidents that were reported to us through May 9 of this year, [redacted] incidents involved instances where a target was targeted improperly under the targeting procedures.

We had [redacted] incidents -- one of the things that NSA is required to do when they identify somebody who has roamed into the States is to notify us of that within 72 hours of making that determination.

We had [redacted] instances where a person had roamed into the States but the NSA did not meet that 72-hour reporting requirement. But in all of those [redacted] cases, the tasking itself was reasonable; it's just that they failed to comply with the reporting requirement.

We're tracking a number of other incidents, but with respect to those incidents, we're pretty much in the same posture that we were back in December: They've been reported to us; we don't have all the facts with respect to those incidents yet in order to be able to categorize them and say, okay, this is a true noncompliance incident, this is just a roaming incident, or this is just a tasking error.

THE COURT: Now, the [redacted] situations where you hadn't been notified within 72 hours, you picked it up in a review much later, or how did it come -- did they report it in 72 hours plus 10, or was it picked up when you went over and --

[redacted] No. They actually reported those to us.

THE COURT: Okay.

[redacted] It was just for a variety of reasons they could not comply with the 72 hours. Sometimes it's just because a final determination can take a little while simply to the extent that the information is somewhat ambiguous. I think NSA errs on the side of caution and probably sets the date of that determination sooner rather than later such that the 72-hour reporting requirement is triggered basically at the first instance or first indication as opposed to when a final determination is made.

Again, we've sort of refined the reporting requirement and have explained to NSA basically when that 72-hour reporting requirement kicks in such that we've, again, seen less and less of these incidents as time has gone on.

THE COURT: So you've taken steps to make sure that NSA, their people understand at least your view of the 72 hours in order to cut down on the situations where things aren't reported.

[redacted] Yes. That's one of the most, I think, valuable aspects of the oversight visits. It's not just to, you know, we sit there and we review and go over things with NSA, but then we sort of have -- at the end, we sort of have a roundup where we all talk about issues that have been identified and ways that we can either fix problems or correct things. And I think we've won the fruits of that, as I said, because the

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


number of incidents we've seen has been diminishing over time.

THE COURT: Okay. Now, what do you foresee under the FISA Amendments Act? Do you foresee the same procedures for your oversight being implemented? Are you planning on different procedures? What are your thoughts?

(b)(6); (b)(7)(C) I can't say for certain. I would anticipate that things would not change, simply because in my view they've been working very well. As I've said, we've seen improvement, I think, just the whole process as we've refined it over the last year. I think where we are right now is probably -- we're in a good spot with respect to oversight, in my view.

THE COURT: All right. Well, what about the non-U.S. person status, which of course is new under the FISA Amendments Act? Are you going to be changing anything in terms of focusing on that?

(b)(6); (b)(7)(C) We already sort of do with respect to -- the U.S. person status is so intertwined with the location of the target [redacted] to the extent that in the past NSA would actually affirmatively identify targeted U.S. persons to us on the sheets, because one of the additional fields that they put in the sheets is basically a blurb, an explanation and a description of the target.

Clearly, we're not allowed to target U.S. persons anymore, so I don't anticipate seeing any such descriptions on the

sheets. But again, since the status of the person, the determination of how that is made is so intertwined with the same information upon which NSA relies to make a foreignness determination, that it would be hard for us not to identify such information as we're conducting the reviews.

THE COURT: Has there been -- and maybe you've said this, but is there thought to be or are you planning to or have you already sat down with people or issued things so that they can now focus on the fact that we've got the non-U.S. person status, which is also something they need to be focusing on?

[redacted] I don't think we've had formal discussions about it. Again, this wasn't an issue that has cropped up out of nowhere where we sort of had to still deal with this issue in the context of the Protect America Act, because under the certifications, we were not allowed to target U.S. persons unless we had 2.5 authority.

THE COURT: Okay.

[redacted] So we always had this affirmative -- although it was not affirmatively stated in the targeting procedures, there was an implicit requirement to ensure that we're not inadvertently or intentionally targeting U.S. persons in the absence of such authority.

So the types of checks that we're doing now build upon checks that we were doing previously in order to satisfy that requirement or limitation.

THE COURT: (b)(6) [redacted] did you want to follow up on that at all? I know you guys were here last time. Anything?

[redacted] (b)(6); (b)(7)(C): I don't think I have anything.

THE COURT: Okay. Thank you on that.

My next issue has to do with departures from procedures, if I can phrase it that way. Let me find out where we're going.

Here we are. I know that -- at least I believe the staff talked with you about this before this hearing, and it's page 10 of the targeting procedures. Let me just get them out.

"If, in order to protect against immediate threat to the national security, the NSA determines that it must take action, on a temporary basis, in apparent departure from these procedures," and I know that -- again, was it at the hearing perhaps? I'm not remembering whether it was at the hearing or not. In any event, I know in the past there has been a representation of the situations that you contemplate coming within this. I don't think you dealt with that in your response from yesterday.

(b)(6); (b)(7)(C) [redacted]: No, we didn't.

THE COURT: Okay. Could you just confirm for us -- I know you've already had discussions with staff, but tell me what you expect to be contemplated by this provision.

(b)(6); (b)(7)(C) [redacted]: First, I think the circumstances under which this provision would be triggered would be very extreme

circumstances: an imminent terrorist attack or a terrorist attack that has occurred or something of equal significance. With respect to the types of departures, I mean, in all cases we will continue to adhere to the limitations set forth in the statute.

We are anticipating that the types of departures would be on a more technical level such as perhaps because NSA personnel are devoted to addressing or countering this terrorist threat, they may not be able to devote the resources necessarily for us to conduct an oversight review within the allotted 60 days.

THE COURT: Has this been used? Has the PAA provision ever been used?

(b)(6); (b)(7)(C) [redacted] We've never invoked it.

THE COURT: Never invoked. Okay. Can you give me a little more meat on the bones on what you would contemplate?

[redacted]. [redacted] I think the other situation we thought of is an emergency, as (b)(6); (b)(7)(C) describes, and our actual system for recording things is down. So technically we can't get to the system where we'd record this. We'd still make a note of what we've done, so we would comply substantially with what's required, we wouldn't want the issue to arise and prevent us from doing what we need to do, are we complying in every detail.

So that's the kind of thing that I think we contemplate

that it could be used in, and again, my own expectation is it will never be used, but we did provide for it in the unlikely event.

THE COURT: Okay. All right. Let's talk for a little bit about these *about* communications.

What I would find very helpful -- can someone just briefly and with not a lot of technical but some technical aspects talk to me about how communications are acquired? Are they acquired in a different way than the *to-or-from* communications? I mean, as I understand it, you're not acquiring them from Internet service providers, like (b)(1); (b)(3); (b)(7)(E) [redacted]

[redacted]: Judge, if I may, I'm going to let [redacted] come to the table because he's one of the people who can explain this.

THE COURT: Oh, wonderful. Come on up, sir. This is [redacted]

[redacted] Yes, typically for *about* communications, right now we do not acquire them from Internet service providers [redacted]

So what happens there is you pick up things like two unknown communicants to us and the *to-from* talking about one of

our targeted selectors. That's a very useful case to us because

(b)(1); (b)(3); (b)(7)(E)

That's one example.

Another example is (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

In other arenas as well, (b)(1); (b)(3); (b)(7)(E)

same kind of thing. We maybe find (b)(1); (b)(3); (b)(7)(E) of a known target that provides a unique insight into that foreign intel need.

And another example, just to flesh these out, a bit more is we would have a target who (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


(b)(1); (b)(3); (b)(7)(E)

THE COURT: (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E) How do you do it?

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

THE COURT: Yeah.

-- that then ensures (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

THE COURT: Okay. Can we talk for a minute -- obviously, the issue for the Court and for the government, as you came up with all these procedures, is the reasonableness

standard, and the Court is looking at that as well as, obviously, compliance with the Fourth Amendment, which in itself is a reasonableness standard, I guess, as well.

Do the *abouts* present a different issue in terms of the reasonableness, do you think? Let me just expand a little bit on that and have some response to it.

What percentage of the acquisitions are *abouts*, as opposed to *to* and *from*? Is an *about* acquisition more or less likely to pick up communications that otherwise you wouldn't be allowed to pick up for whatever reason? Do they present harder issues for reasonableness?

Somebody want to start discussing that with me? Have you thought about that?

[redacted] As far as the percentage number, we don't have a number for that, because as I mentioned earlier, when we [redacted] we find *to's* and *froms* and [redacted] so we don't categorize those separately to be able to count those communication as *abouts*.

So we don't have any numbers. I can tell you as far as usefulness, they're very useful, and we see them routinely, but I don't have a number for you on that.

THE COURT: And in terms of the usefulness, their importance to what you're trying to accomplish, talk to me a little bit about that. As important as a *to* or *from*, less important? What role do they play in what you're doing?

[redacted] They're very useful in [redacted]

[redacted]

So, for example, in the [redacted] (b)(1); (b)(3); (b)(7)(E) [redacted] (b)(1); (b)(3); (b)(7)(E)

(b)(1); (b)(3); (b)(7)(E)

[redacted]

[redacted]

THE COURT: Now, you're saying in your response, still on the *abouts*, "the operation of the Internet protocol address filters or [redacted] prevents the intentional acquisition of communications about the target as to which the senders and all intended recipients are known at the time of acquisition to be located in the U.S."

[redacted] What about the U.S. person status, how that is more difficult to account for or to --

(b)(6); (b)(7)(C) Well, first of all, it's our position that the target of an *abouts* communication is still the user of the targeted selector. It's not the sender or recipient of the e-mail or other communication that contains the targeted selector. I mean, that's where the foreign intelligence interests lie, in the user of the targeted selector.

To the extent that the IP filters and [redacted] ensure that at least one end of the communication is outside the United States, more often than not, I would suspect both ends of the communication are outside the United States. We're collecting *abouts* of purely transient communications such that it's less likely that there's U.S. persons involved or U.S.-person information involved.

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


But even to the extent that one of the communicants was a U.S. person or was located in the United States, to the extent that there's U.S.-person information in the *abouts* communication, that information will be subject to the minimization procedures.

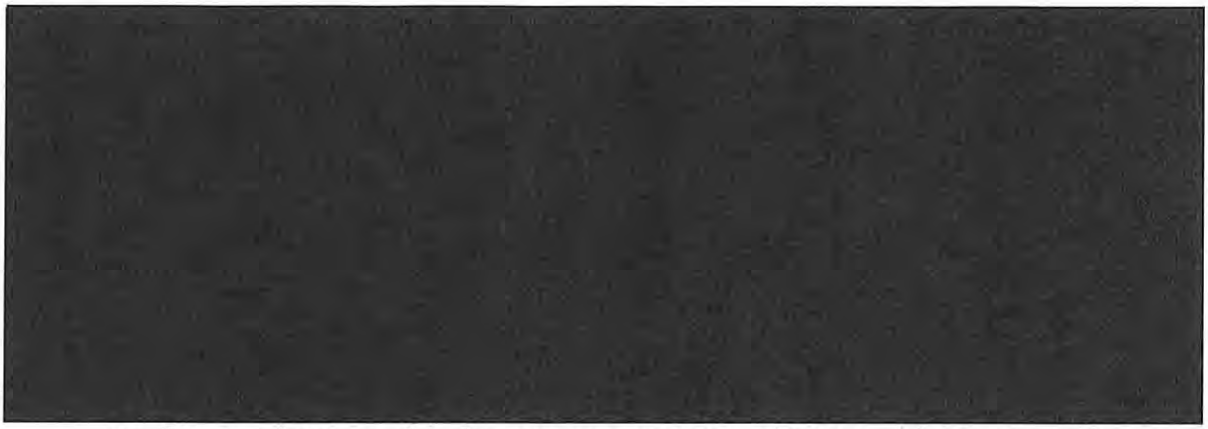
THE COURT: Okay. Anything from staff on the *abouts*? I'm going to talk some more about the filter issue but from a different perspective. Anybody?

[redacted] (b)(6) Judge, I think I do have a question.

THE COURT: Yes. Go ahead, Phil.

[redacted] (b)(6) When you describe how [redacted] these *about* communications, you described it in a way -- well, you said that [redacted] acquiring the *to-or-from* communications [redacted], if you wanted to for whatever reason, would it be technically feasible to -- in the same manner [redacted] would it be technically feasible to acquire only communications that are to or from the selector account and not those communications that otherwise contain a reference or name of a selector account?

[redacted] It is technically feasible. The problem with doing so is if you end up discarding a number of communications that are truly *to-froms* that you should be able to collect but [redacted]



So by trying to limit us to say no *abouts*, then we end up cutting out those kind of communications as well, truly *to-froms*. So it would be -- we're not surgical enough to take that out of the equation without impacting our ability to do *to-froms* effectively.

(b)(6) Okay.

Judge, may I offer --

THE COURT: Sure. This is right?

-- as to the reasonableness. I think you asked the question about reasonableness we haven't addressed. But one of the things the way we have this structured, we think it is akin to -- not exactly the same, but akin to finding a connection between a targeted e-mail address and a person outside the United States.

And for that communication only, we think it's reasonable to make that newly discovered person -- to acquire his communications. There's no automated tasking of that newly discovered person that takes place. Nothing happens as a matter of course. We only collect that single communication, and then

we assess it as to whether we want to make a new target there of the person overseas. But it's important, I think, to understand there's no follow-on automated, *now we found a new person, a new person, a new person*, and those are not automatically added to our task mode.

So it's a limited look with our target, the user of the e-mail address continuing to be our target, [redacted]

[redacted]

THE COURT: Yes. I'm glad you brought that up, [redacted] because what I understand, and I think you've just said it, is that when you're picking up the *about*, you're also getting information on the *to* and *from*. But if the *to* or *from* is now a person of interest, but if it's a U.S. person, for example, or something, you couldn't continue to just pick up that person, directed at the person, but then you'd have to come into court with an application or do whatever else. But you're not automatically then following that person.

[redacted] That's correct.

THE COURT: Now, on the IP -- this is getting to minimization, but because it relates to the filters, let's talk about it. And this is on page 5 of your written response from yesterday. The NSA minimization procedures, you're stating, "contain a provision for allowing retention of information

because of limitations on NSA's ability to filter communications." My question I had was is the filter discussed in targeting the same filtering. I just wanted to understand that, and apparently it is.

But talk to me a little bit, because there seemed to be some tension there. [redacted]

[redacted]

(b)(6); (b)(7)(C) I think the inclusion of that provision in the minimization procedures was intended to be prophylactic in the event that the filters don't necessarily work, and NSA has represented that it's been their experience with the filters and [redacted] that they have not captured purely domestic communications with respect to the *abouts*.

But to the extent that [redacted]

[redacted]

this provision basically captures instances where the filters may not work in every instance.

THE COURT: You did respond to this, but I guess maybe just a little bit more on how limited are they. I mean, what are the limitation of these filters?

[redacted] Limitations really come down to -- the

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted./ Approved for Public Release


filter is basically [redacted]

[redacted]

[redacted]

THE COURT: (b)(6)

(b)(6) Thank you, Judge.

[redacted]

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


[redacted]

THE COURT: Okay.

(b)(6) [redacted] With one other question. For example, with the filters, [redacted]

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


[redacted]

(b)(6) [redacted]

[redacted]

(b)(6) [redacted]:

MR. (b)(6) [redacted]

[redacted] (b)(6) [redacted]:

[redacted]

MR. (b)(6) [redacted]

[redacted]

(b)(6) [redacted]

[redacted]

MR. (b)(6) [redacted]

[redacted]

THE COURT: Okay. Again, going on or continuing with minimization procedures, let me see where I am here. Just a couple of things that I think the staff confirmed with you prior to the hearing when they raised various issues. And it wasn't in your memo from yesterday, so I'll just raise it here. But as I understand it, (b)(1); (b)(3); (b)(7)(E) [redacted]

(b)(6); (b)(7)(C) That's correct.

THE COURT: Okay. And on page 1, I guess it was, of (b)(1); (b)(3); (b)(7)(E) [redacted]

[redacted] (b)(6); (b)(7)(C) Yes.

THE COURT: All right. And then I wanted to go to 3(b)(1) of the minimization procedures, a paragraph I will tell you that I had some struggles with, but now I think I understand it.

(b)(6) [redacted] This will be the NSA minimizations --

THE COURT: I'm sorry, NSA.

All right. Now, first of all, as I understand it, I thought there was a "not" missing, and there was.

(b)(6); (b)(7)(C) [redacted] There is.

THE COURT: Okay, that's fine. I kept reading and thinking I was missing something, and it took me awhile. But let me just say to you what I understand this paragraph to mean, and then tell me if it -- that "NSA shall destroy inadvertently acquired U.S.-persons communications once they are identified as both clearly not relevant to the authorized purpose of the acquisition and not containing evidence of a crime." And also "inadvertently acquired U.S.-person communications includes these electronic communications acquired because of limitations of the ability to filter." That was the filter issue.

That's what will happen, and the time limit is a maximum of five years.

(b)(6); (b)(7) [redacted]: Correct.

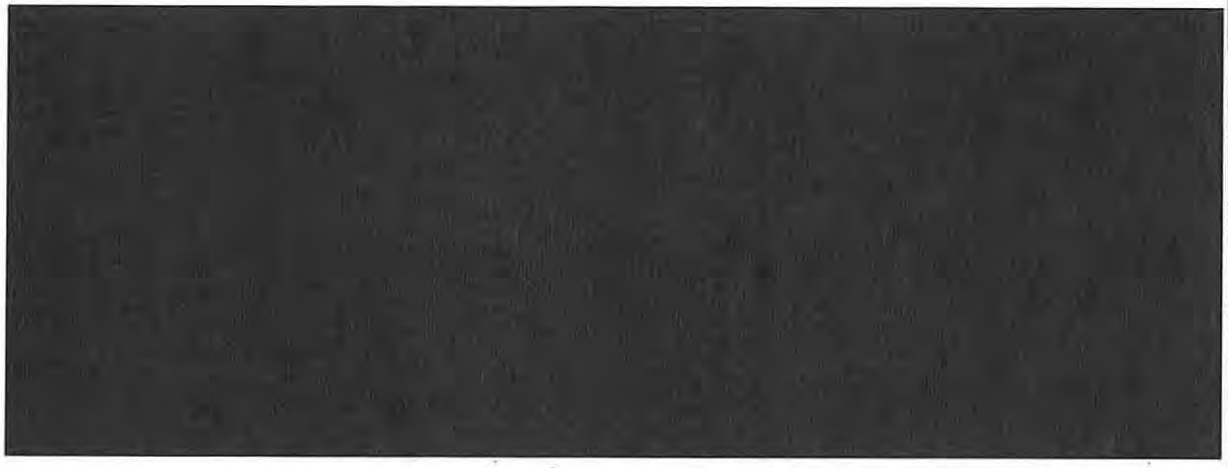
THE COURT: It will be done at least with respect to the first part of 3(b)(1) at the earliest practical point, but at least five years --

(b)(6); (b)(7)(C) [redacted]: No later than five years.

THE COURT: No later than five years. And I understand that five years has been a time frame that has appeared in other procedures, but I think it probably would be helpful to just sort of talk a bit about where that comes from, why is that a number that's been selected.

(b)(6); (b)(7)(C) [redacted]: NSA can correct me if I'm wrong; the five years comes from the fact that [redacted]

[redacted]



That, I think, is the general thinking behind the five-year retention period. That's the potential analytical life cycle of a particular piece of information.

[redacted] Your Honor, this is [redacted] for the NSA.

THE COURT: Sure. Yes, sir.

[redacted] In a couple of other places in our minimization procedures, namely in Section 5 and Section 6, we talk about the five-year rule where in certain cases the intelligence director may extend that in the case of domestic communications or in the case of U.S.-person information if again it has foreign intelligence value or evidence of a crime.

So in 3(b)(1) we talk about five years, but there are a couple of other sections that might be invoked by our SID director where he could extend it.

THE COURT: Yes. Well, I think this makes clear that it's not talking about things that are not relevant -- it's only talking about things that are not relevant to the authorized

purpose of the acquisition and not containing evidence of a crime. So the implication is that if it does do that, the five years may not necessarily be -- fair enough.

All right. Number 13, page 11 of your response from yesterday. Now, I had a couple of questions with respect to the three minimization procedures and what they say about the director being able to do certain things, but (b)(6); (b)(7)(C), I understand that you alerted the staff before the hearing that there's another potential issue that you have thought of that could impact this issue.

(b)(6); (b)(7)(C) Correct. There's a provision in the FISA that was recently changed, 1806(i), which basically says -- the previous iteration of that provision of the statute said if you are unintentionally acquiring radio communications when the sender and all intended recipients are located in the United States, the attorney general has to determine whether or not that piece of information can be retained in very extreme circumstances, otherwise such circumstances have to be destroyed upon recognition.

The recent FISA Amendments Act struck "radio" out of that provision such that the provision appears to on its face apply to all types of acquisitions conducted under the act. Whether or not that particular provision applies to this type of collection such that it would require us to basically destroy domestic communications as they are recognized is an issue that

we're still trying to work through.

THE COURT: Okay. All right. And I'm sure we'll continue to talk on that as you work it through, and thank you for alerting us to that. Let me go forward, though, with the minimization procedures as they are, and let me ask a couple of questions about them, putting aside for the moment this issue with 1806.

We had one question for you, and now I don't know if we asked you this before, but the one question was the NSA and the CIA procedures had the directors doing things in writing. And the FBI provision didn't say "in writing," but as I understand it, the FBI, as you cite here, has represented that any such determination by the director would be made in writing even if not expressly required.

(b)(6); (b)(7)(C): Correct.

THE COURT: Okay. That answers that. Another similar kind of question. There may be no significance to the difference in language, but the NSA procedures at page 5 say, and I'm paraphrasing because I don't have the exact quote, that unless the director "specifically determines" something.

And then the FBI provisions simply say "unless the director determines," and I think the CIA also says "unless the director determines." Is there any meaning I'm supposed to take from "specifically?"

(b)(6); (b)(7)(C): No. I think "specifically" was just

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


intended to capture the notion that this would be on a case-by-case basis as opposed to just a broad-base, I'm going to exempt this particular gigantic class of communications.

THE COURT: But I take it the FBI and a CIA would also be on a case-by-case basis.

[redacted] Yes.

THE COURT: Yeah, I didn't think it had a lot of significance, but you never know, so I thought I'd ask.

You know, I may be at the end of my list. What I'd like to do is take a break. But since there's fewer of us than of you, we will step out, and then you can stay here and if -- because there's a lot of people here.

Obviously, use the time. If something was said here that you have an issue with because, you know, at least from your experience it doesn't work that way, please talk among yourselves and we can straighten that out. Or, if I had asked a question and you say, *Gee, I think the best answer is X and nobody said X*, please feel free to tell [redacted] and we can get that better answered on the record.

Okay. Thanks, everybody. Just give us a few minutes.

(Recess taken.)

THE COURT: Just a couple things. Going back to the *abouts*, if we can go back to them for a moment, you know the Court will have to do, obviously, a Fourth Amendment analysis in terms of the reasonableness -- of all the procedures, not just

of the *abouts*.

But I guess my question is, is there a different analysis for the *abouts* than for the *to* or *from*? Or to put it another way, could somebody articulate for me what you believe why the *abouts* don't present a different Fourth Amendment issue from the *to's* and the *froms*, that it's the same issue?

Again, to amplify even a little more, is the possibility of acquiring information that otherwise it would not be permissible to acquire in the *about* scenario different from the *to* or *from*?

In other words, is it incidental? Would you describe it in that way? If not, how would you describe it? Is it any less or more likely to happen with the *abouts* than with the *to* or *from*? Or any other aspect of the Fourth Amendment analysis that you think is relevant.

(b)(6); (b)(7)(C) I don't think that the Fourth Amendment analysis is any different with respect to an *abouts* communication or *to* or *from*. I mean, it's just as likely that one end of a *to* or *from* could be a U.S. person in communication with a target as an *about*.

In either case, the U.S.-person information contained in that communication would be subject to the minimization procedures, and it's not that U.S. person that is the target of the acquisition of that particular communication; it is the user of the targeted selector that appears in the body of that communication. So I think for Fourth Amendment purposes, with

respect to U.S. persons, I don't think the analysis is any different.

MR. OLSEN: We have given some thought to this, because *abouts* collections has been an issue in this collection as well as prior court orders. But I just would reiterate what [redacted] said in terms of our view of it in that it's essentially for the Fourth Amendment purposes an incidental collection where the target is the targeted account, and to the extent that a U.S. person's communication -- to or from a U.S. person, that would be deemed to be incidental to the collection.

And therefore under the analysis we put forward in, for example, the Yahoo litigation, that would be permissible and reasonable under the Fourth Amendment as long as minimization procedures are appropriately applied.

THE COURT: Is it more or less likely to pick up U.S.-person information in an *about* than a *to* or a *from*?

MR. OLSEN: I don't know the answer in practice. At least from my perspective in theory, I wouldn't see why it would be more likely than a targeted *to* or *from* collection where the target's outside the United States where there's similarly the possibility that that target would be in communication with someone in the United States, with a U.S. person in the United States.

So, just analytically, I think the same incidental collection subject to minimization procedures framework would

apply. And so under the Fourth Amendment applying, that we would submit would be reasonable under the Fourth Amendment.

(b)(6); (b)(7)(C) And I would note that in his opinion on the Yahoo litigation, Judge Walton recognized the reasonableness of a presumption that non-U.S. persons located overseas are more likely to communicate with other non-U.S. persons located overseas which may bear on the volume of potentially -- or *abouts* communications that potentially implicate U.S. persons versus non-U.S. persons. I think if you apply that presumption, it's more likely that an *about* will not implicate U.S.-person information.

THE COURT: Okay. Fair enough.

Well, that's really all that I --

(b)(6) Judge, I'm sorry.

THE COURT: Yes. Go ahead, (b)(6)

(b)(6) With regard to the *abouts*, it's occurred to me, just to be clear on the record, there were [redacted] sort of subcategories of such communications that were laid out in a footnote to Judge Kotelly's opinion in the PAA that in turn I think referred to an opinion issued or an order issued by Judge Vinson last year.

Do those [redacted] categories, as previously set out in those places, continue to be accurate and up to date and complete in terms of the communications that are obtained?

[redacted] I think so. If I recall correctly, and I

may not have all [redacted] categories off the top of my head, we have the instance where the selector is mentioned in the body of an e-mail sent between two communicants.

You have an instance where [redacted]

THE COURT: Well, there was [redacted]

[redacted] (b)(6); (b)(7)(C): Oh, [redacted] yes.

(b)(6) [redacted] And [redacted]

(b)(6); (b)(7)(C) [redacted]

(b)(6) [redacted]

[redacted] Yes.

THE COURT: Okay. Thank you, (b)(6), for that. Appreciate it. So I guess the only other outstanding issue at the moment is the 1806, I'll call it, issue, and what is your thinking in terms of timing? Obviously, at this point at least we have the September 4 deadline that we're looking at, but what are your thoughts on timing?

MR. OLSEN: We're going to turn to this immediately

following the hearing. This has been, as I think (b)(6); (b)(7)(C) mentioned, been an issue we identified yesterday or the day before in the evening.

So we have the right folks here to talk about it, and my expectation first would be that we would be able to communicate directly with the Court staff. I don't know how quickly we will have a definitive answer, but I would expect that we will have a definitive answer, understanding the timing of this overall, by tomorrow at some point and that what I expect to do is to have something in writing, perhaps not very formal, something along the lines of what we recently gave to the Court to address this issue.

It may be that that will be, in terms of our view, that we think we have a resolution to the issue and that no further action is necessary. It may be that we have other steps to propose to the Court, but we certainly understand the importance of moving quickly and turn to this right away.

THE COURT: Okay. Fair enough.

(b)(6); (b)(7)(C) And there were three other issues that we'd just like to clarify, statements that were made previously that we just want to provide maybe a fuller context to.

THE COURT: Sure.

(b)(6); (b)(7)(C) With respect to oversight and the number of compliance incidents that we've identified, just to give you some perspective on the relative nature of that number, since

the acquisition of the Protect America Act began, NSA has tasked over [redacted] selectors. So the fact that we've identified [redacted] or so actual compliance incidents is, relatively speaking, a very, very small number.

Another point that we'd just like to provide a little more clarification on is the point that [redacted] made with respect to extending the five-year retention period for particular communications, and maybe [redacted] can expand on this a little bit more.

We just want to make it clear that with respect to the determination by the SID director to extend that, that's not on a communication-by-communication or selector-by-selector basis. It can be a broader range of communications that the SID director may make that determination for and extend the retention period.

THE COURT: Are you focusing on a particular part of the procedures? Can we look at them? That will help me, I think. These are the NSA minimization procedures?

(b)(6) [redacted] It's section 6(b).

(b)(6); (b)(7)(C) [redacted] There's one in 6(b), and there's one in 5(3)(b).

(b)(6) [redacted]: May I ask a question?

THE COURT: Absolutely. Go ahead, (b)(6) [redacted]

(b)(6) [redacted] Has the SID director invoked this provision? Is there an extension currently in place?

[redacted]: There's not under PAA. [redacted]

[redacted]

[redacted]

(b)(6) [redacted]

[redacted]

[redacted]: [redacted].

(b)(6) [redacted]: Oh, I see.

[redacted]: [redacted]

[redacted] Our concern, we don't want to leave a misimpression, when you read this together, if we discover -- if we find that there are U.S.-person communications here, we will take this action.

If, however, we haven't discovered that and the SID director extends the period, it's possible it will be undiscovered U.S.-person communication during that seven-year period. So we don't want to give a misimpression by saying retained no longer than five years in any event.

I guess it should be read to say in any event -- I don't know where it is, but it allows the SID director to extend the retention period as invoked. In that case, undiscovered. We haven't realized it, but we have these kinds of communications. They would continue to be retained as well.

THE COURT: That's because they're undiscovered. If it's discovered, it's five years.

MR. [redacted]: That's correct. If it's discovered --

All withheld information exempt under (b)(1) and/or (b)(3) unless otherwise noted. Approved for Public Release


THE COURT: Yeah. If they're discovered.

[redacted] They would be destroyed at that time.

THE COURT: Obviously, if they're not -- okay.

(b)(6); (b)(7)(C), now that I've read them again, can you just repeat what you said you wanted to make clear, that this wasn't on a case-by-case basis?

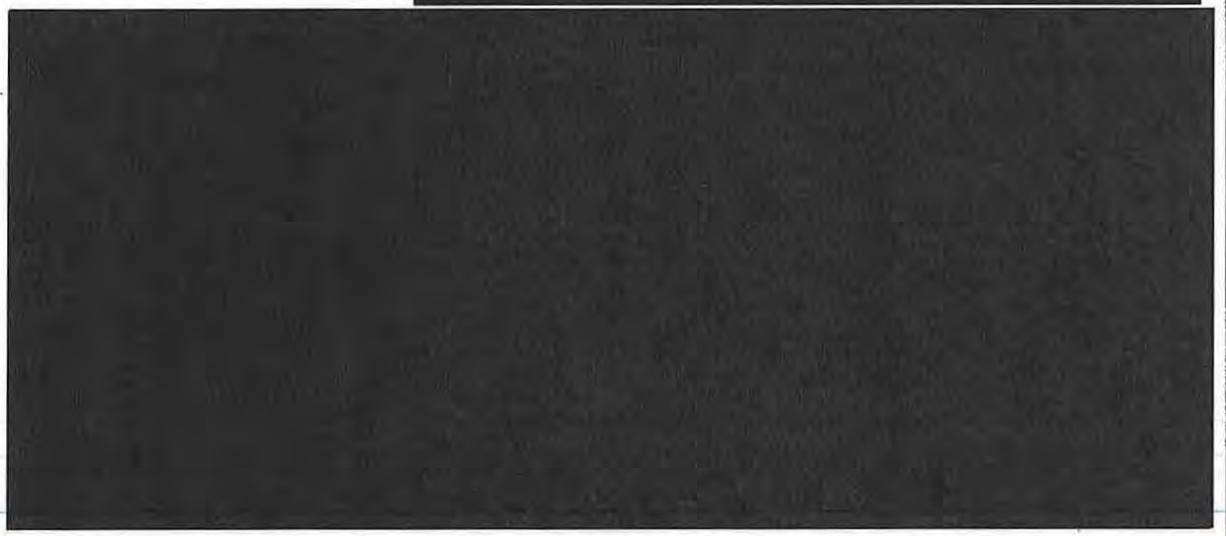
(b)(6); (b)(7)(C) It can apply to a broader range of communications. It's not, okay, the SID director determines that this --

THE COURT: Particular little thing right there.

(b)(6); (b)(7)(C) -- meets this standard, therefore I can extend the retention duration beyond the five years. It can be a range of communications.

THE COURT: Just give me an example. I think we just had one. Can somebody give me an example?

[redacted]



THE COURT: I see. Okay. Thank you.

(b)(6); (b)(7)(C) And one last clarification. With respect to the ongoing requirement that an analyst keep track of its targets and basically is responsible for ensuring the continuing foreign intelligence purpose of the collection, [redacted] said NSA imposes a [redacted] that the analyst has to make that determination.

We just want it to be clear that that is the outer limit of the requirement that that determination be made and that in practice that determination is made on a much more ongoing basis than just [redacted]

THE COURT: And I don't think I understood it to mean [redacted] but I appreciate that clarification.

All right. Anything else?

(b)(6); (b)(7)(C) That's all, Your Honor.

THE COURT: Okay. Thank you so much, everybody. I appreciate it. All right. We are adjourned.

(Proceedings adjourned at 11:02 a.m.)

(b)(6) Deputy Clerk
FISC, certify that this document is a true and correct copy of the original. (b)(6)

DECLARATION OF SCOTT BRADNER

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

# Appendix V

2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum

# A Stream Reassembly mechanism based on DPI

Shuhui Chen
College of Computer Science
National University of Defense Technology
Changsha, China
Email: shchen@nudt.edu.cn

Yong Tang
College of Computer Science
National University of Defense Technology
Changsha, China
Email: ytang@nudt.edu.cn

***Abstract*—Stream Reassembly is an indispensable function of Deep Packet Inspection, which is an critical element of Network Intrusion System. However, since it need to heavily move packet payload from one block of memory to another block of memory, Stream Reassembly has a serious memory performance issue. In this paper, in order to improve the Stream Reassembly performance, a Stream Reassembly Card (SRC) is designed, which enables to manage and assemble streams through adding a level of buffer to adjust the sequence of packets by using the Multi-core NPU. Specifically, three optimistic techniques, namely Stream Table Dispatching, No-Locking Timeout, and Multi-channel Virtual Queue are introduced in SRC design. The experiments show that the reassembly can achieve more than 3 Gbps in terms of processing speed, triply outperforming over the traditional server based architecture.**

***Index Terms*—Network Security; Network Intrusion System; Network Forensics System; Multi-core NPU; Stream Reassembly;**

## I. Introduction

DPI (Deep Packet Inspection) is a critical technique for Network Forensic System (NFS), where packet payloads need to be matched against pre-defined patterns to obtain the evidences with a 4-step process, namely preprocessing, header-matching, content-matching and outputting in NIDS and NFS. In general, in the event of a network with a low speed, server based approach (in which the stream reassembly, rule matching and warning are all conducted by one server) can satisfy the performance requirement. However, with the exponential increasing of bandwidth, the traditional server based approach (even for a server with high performance) no longer meets the performance requirement. To break up this bottleneck, many researches have been carried on to improve the overall performance by achieving efficient content-matching [1]–[6].

Many previously reported methods mainly focus on improving the rule matching algorithms, and/or using FPGA [1], [2] or GPU [3]–[6] for efficient content-matching, and the results show that the ratio of running time used for matching is decreasing with the enhancement of matching performance. Experiments from some other researchers [7] further indicated that when the ratio of the matching time to the overall decrease to 1%, Stream4 (which reassembles streams in previous Snort version) will take on the load of 80% when it is used to assemble the packets.

Currently, advanced progresses have been made in the network electron component area. For example, Raza Micro-electronics has developed XLR, XLS and XLP NPUs, while Cavium has launched OCTEON Series NPU. The emergence of these multi-core NPUs can largely improve the performance of the network devices and network security devices. In this paper, we present a new Stream Reassembly Card (SRC) design, which enables to manage and assemble streams through adding a level of buffer to adjust the sequence of packets by using the Multi-core NPU.

## II. Related Work

There are two open source programs: Libnids [8] and Tcpflow [9] that fulfill TCP stream reassembly, but both of them cannot meet the performance requirements of the current network links. Researchs having relationship with stream are often focus on the measurements.

For example, [10] has used two data recorded from two different operational networks, and studied the flows in size, duration, rate and burst, and examined how they are correlated. [11] concerned on the problem of counting the distinct flows on a high speed network link. They proposed a new timestamp-vector algorithm that retains the fast estimation and small memory requirement of the bitmap-based algorithms while reducing the possibility of underestimating the number of active flows.

[12] has introduced a TCP reassembly model and a stream verification methodology that can be used to derive and compute reassembly errors. [13] has introduced an algorithm that solves the problem of TCP stream reassembling and matching performance problem for network forensics system and IDS. Instead of caching the total fragments, their methods stores each fragment with a two-tuple that is constant size data structure, thus the memory requirement involved in caching fragments is largely reduced.

[14] has introduced a hardware based reassembly system to solve both the efficiency and robust performance problems in the face of the adversaries to subvert it. They characterized the behavior of out-of-sequence packets seen in benign TCP traffic, and designed a system that addresses the most commonly observed packet-reordering case in which connections have at most a single sequence hole in only one direction of the stream.

## III. Why Multi-core NPU is Selected

NIDS obtains copies of packets directly from the network media, regardless of their destination. Raw packets captured

978-0-7695-4676-6/12 $26.00 © 2012 IEEE
DOI 10.1109/IPDPSW.2012.152



IEEE computer society

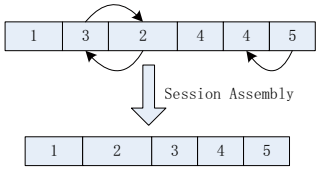



Fig. 1. An example of stream reassembly.

by the NIDS are confused and disordered messes, but DPI in NIDS needs these packets to be fabricated as integrated blocks according to their TCP stream belongings before they are sent to the matching engine.

Figure. 1 gives an instance, and the stream in the example is composed of 6 packets. But packet 2 and packet 3 are out of order, and packet 4 is repeated. The stream reassembly process needs to exchange the sequence of packet 2 and packet 3, and the unwanted second packet 4 should also be deleted. The process incurs 3 times packets movement: packet 2 moving ahead, packet 3 moving backwards, and packet 5 moving ahead. This is just an example of a single stream, and in the real network environment, one backbone link may contain a large number of streams. In other words, there may be too many packet movements in the reassembling process. Modern servers use DRAM (DDR2 or DDR3) as their main memory, one memory access may take a number of cycles to obtain a result because DRAM has a relatively long startup time.

However, multi-core NPU can improve the performance of this kind of operation, which is because:

(1) There are many hardware threads in one core and many cores in one NPU, which makes the total threads in a NPU, will be more than a dozen. The threads of this kind are hardware threads instead of software threads so the switching cost is very low. The large number of hardware contexts enables software to more effectively leverage the inherent parallelism exhibited by packet assembling applications. When one thread is waiting for the result of the memory accessing, the other thread could switch in and makes another memory accessing request, and if many threads use such a pipeline, the latency of the DRAM will be hidden and the effective bandwidths of the DRAM access would increase.

(2) A multi-core NPU is often with low electric power consumption, so it is easy to be manufactured as a card. When a NPU based card is used, an extra buffer is introduced to the processing flow, so the packets can be sorted as they are being transferred from the memory of the card to the memory of the host (server), which is a form of trading space for performance. In this way, when the packets have been received into the memory of the card, they are stored in the memory as their reaching order, but their sequence are maintained by the software running on the NPU.

(3) The architecture of NPU often has a favorable I/O features, and the packets could be imported from the interface to the memory with high throughput. As the dispatching component generally dispatch packet according to the selected bits from the packet head, stream reserved would not be a problem. Since many researches [15], [16] focus on how to accelerate the packets capturing performance, an approach combination packets capture and stream reassembly is cost-effective.

(4) NPU often has a well designed message-passing mechanism between different threads, which uses cross-bar structure or fast shared SRAM as its transferring medium, and makes the cooperation and synchronization between threads facile.

## IV. System Architecture

### A. Stream in TCP Transferring Level

We focus on three different critical actions, which are TCB creation (the point at which an IDS decides to instantiate a new TCB for a detected connection), Packet Reorder(the process an NIDS uses to reconstruct a stream associated with an open TCB), and TCB Termination (the point at which the IDS decides to close a TCB). Every TCP connection can be expressed as a four-element tuple (which includes source IP, source port, destination IP, and destination port). Once a packet is captured, its corresponding stream needs to be found and the TCB data structure needs to be updated. Basically, TCB is attached to a Hash Table indexed by hash algorithm using some bits from the four-element tuple as parameters. Collisions lead to several TCBs attached to one table entry.

### B. Frameworks of SRC

The framework of SRC is depicted in Figure. 2. In SRC, packets are captured from the interfaces to the memory; for maintaining the TCP connection data, a hash table known as Stream Table is used. When the packets enter the memory, their locations are stored in the packet descriptions. Besides the points which point to the packets, packet descriptions also contain the packet length and the fields used to dispatch the packets to the threads.

Threads running on the NPU wait circularly, processing a received packet and then waiting for another packet. Once the data needs to be submitted, every thread is responsible for the task of submitting the packets from the memory of the NPU to the memory of the host. Both the softwares running on the NPU and CPU share a little memory space in the DDR of the NPU for message communication, and the memory space is used by the NPU to get the address of the DMA, the timeout of the host setting, the BlockSize, and the consuming states; CPU can also use the memory space to gain the running states of the NPU. As the packets are DMAed to the host memory, the transferring is conducted one packet after another, which is due to the packets are not stored consecutively in the memory of the NPU while we need them to be consecutive when they reach the memory of the CPU.

Software running on the NPU mainly executes three actions mentioned in Section. IV-A: TCB Creation, Packet Reordering, and TCB Termination. When a packet reaches one core, the related thread looks up the Stream Tables to determine whether there is a corresponding TCB exists. If not, the corresponding TCB is created, and the packet is appended to the TCB. Or else, the packet is appended to the corresponding TCB and its link position is determined; meanwhile, a judgment is made

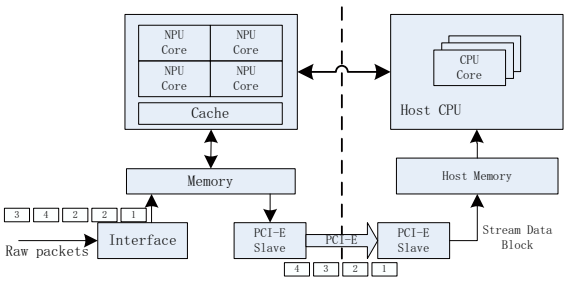



Fig. 2. Frameworks of SRC.

on whether the total packet size of the stream is equal or larger than BlockSize (Submitting Block Size). If the answer is positive, all the packets are submitted in the light of their sequence to the Host.

The total connection records are maintained in a hash table called Stream Table for efficient access. Note that the hash needs to be independent of the permutation of source and destination pairs, which could be achieved by comparison the source IP together with source port and destination IP together with the destination port, and always make the less one to be the first parameter or using some hash algorithms that are not sensitive to the sequence of parameters. Using such hash values as the indexes to the stream table, the corresponding connection can be located. Hash collisions can be resolved by chaining the colliding TCBs in a linked list.

Data submission procedure running by the packet processing threads needs to work cooperatively with the program running on the host CPU. A consecutive memory chunk needs to be allocated to storage the packets uploaded, and for the convenience of the packet organization, the chunk needs to be divided into fix-sized buffers which are organized as a ring. Software (IDS and NFS) running on host continually process the data block received.

### C. The Procedures of Stream Reassembly

The two significant data structures in stream reassembly are stream table and TCB. Stream table is made up of many entries, each of which points to a list of TCBs that have the same hash value. In SRC, two types of threads are used to fulfill the stream reassembly: the packet processing thread and the timeout thread. The packet processing threads are responsible for packet receiving, stream reconstruction and data submission; moreover, stream reconstruction is divided into TCB Creation, Packet Reordering and TCB Termination. The timeout thread is a simple circular procedure; it accesses TCBs one by one ceaselessly, comparing the current time with the time of the last coming packet in every stream. If the gap between the two times is large than the appointed value, timeout thread deems that the corresponding stream may be asleep or dead, so it submits the remaining data and delete the TCB to give space to other streams.

The main purpose of *ReorderPacket* is to sort the one-stream-affiliated packets according to their TCP sequence number, and drop the repeated packets that have the same sequence number. Instead of being processed after a batch of packets belonging to a stream have been received, the packets are maintained their order upon being received. The reasons why it does in this way are as follows: (1) The batch processing could cause the computing burst, which is detrimental to the smooth process; (2) Disordered packets are rare actually, most of the arrived packets are ordinal and consecutive. As a result, processing packets one by one will save more computational resource.

As the data is submitted to the host, all the packets must be insured to be ordinal and consecutive. We use **ordering** to express the sequence of the packet and **continuity** to denote if there is any packet should reach but have not reached. When the packets reache, their ordering can be insured by sorting the sequence number and modifying the points of the list that attached packets, but the continuity cannot be ensured, it is due to the disordered arrival is available. To determine if the data can be submitted, a counter DisContinuity Number (DCN) is used to identify if the received packets is continuous or not. DCN is the counter of gaps between adjoining packets for a stream.

The larger the DCN is, the more the degree of discontinuity is. An example is given as follows: for one direction of a stream, if packets 1, 2, 3, 4, 5, and 7 have been received (the numbers are the order numbers of the packet been sent out, not the sequence numbers of the TCP level), the DCN of the stream is 1, because there is a gap between packet 5 and packet 7. If packets 1, 2, 3, 4, and 7 have been received, the DCN of the stream is still 1, because even through there are two packets between packet 4 and packet 7 as they look like, we do not know there is one packet or two packets can fill in this gap when we receive the packet 7, the only fact we know is that there is a gap between the sequence number of packet 4 and packet 7 from TCP level.

All the packets are linked up while the packets with smaller sequence number are in the front of the link and the packets with bigger sequence number are at the back of the link. Bidirectional links for the packets are needed, because packets needed to submitted from NPU to CPU according to the sequence number of the packets. But when a packet arrivals, locating the inserting point from the verse direction may gain better performance. That is because the gap exists scarcely; and even when it emerges, it will be filled up quickly.

When a stream ends, timeouts or its size exceeds the BlockSize, the packets belong the stream must be uploaded to the CPU. Under the circumstances of stream end or timeout, DCN will be zero if all is OK. If it is not zero for some packets have not been received, there is nothing can be done by the reassembly component. But if we are under the third circumstance, which shows that the size of the stream achieves the BlockSize, and the DCN is not zero, reassembly component needs to find the gap that causing the DCN to be not zero. We can look for the link of the stream, if the lost packets are far from the last packet (for example, 8 packets is an experiential value), the finding process is stopped and the packets are submitted, considering that packets will not arrive.

On the other hand, if the gap is among the last 8 packets, we will submit the integrated packets and maintain the remanent inconsecutive packets of the stream. To sum up, we try to upload the packets that are consecutive to the host.

## V. Improvement

### A. Stream Table Dispatching Technique

There are two techniques can be implemented to organize the TCB in the stream table: shared stream table and separated stream table. For the shared stream table, all the threads share a whole stream table, so all the threads need to access the stream table in the global memory. As a result, a lock must be added to the corresponding item of the stream table when one thread is processing the packet. The contest accessing by all means decrease the performance. And for the separated stream table, every thread uses its own stream table, and we must use more memory than the shared stream table to hold several tables to make the TCB list not too long.

So, if both high utilization and high performance are required, a new technique must be adopted. To solve this problem perfectly, a unified hash method for packet dispatching to the threads and obtaining the stream table index is applied, making all the TCBs have the same stream table index are dispatched to the same thread. Therefore, the items of the stream table need not to append locks because all the packets hashed to the special item will be processed by one special thread. In addition, if the stream table items assigned to every thread are consecutive and their size is aligned to the Cache blocks, then the Cache hit ratio will be high to improve the overall performance.

### B. No-Locking Timeout

A large numbers of concurrent TCP streams are present in the network, so the states of a large number of TCBs attached to the stream table must be maintained. To release the memory space of the streams that are not active in the SRC, three submission schemas have been used: stream timeout, stream termination, and the size of packet buffered achieve a specified size.

Because the packets timed out have to be uploaded, a separated timeout thread is used to confirm whether there is any stream is time out. The timeout thread circularly obtains every item in the stream table and then gains every TCB in the link to determinate if there is a timeout. If a timeout occurs, submission the packets and deletion the TCB are conducted. The stream table and the TCBs become the critical resources and locks are required because that the packet processing threads need to process on the TCBs and their corresponding packets as same as the timeout thread does.

The lock operation should be removed as our experiences on the network device and network security devices because we have not so much time to process a packet. For example, we only have 300 ms to process a packet for a Gbps link [17]. For the multi-cored NPUs of RMI and OCTEON, they both have a fast messaging mechanism to implement the synchronization and information transformation among different threads. The messaging mechanism can be used to remove the locks by the timeout thread sending a message to the packet processing thread, and then the packet processing thread submitting the packets and deleting the TCBs.

### C. Multi-channel Virtual Queue

The performance of the Packet capture is critical to the overall traffic analysis system [18], [19]; similarly, data block submission is critical to the overall system of stream reassembly. It is obvious that multi-core computers are the current dominant trend in computers; thus, how to avoid data coping and make the data block distributed to the several cores in the host evenly can bring distinct improvement to the overall performance.

Luca [16] exploits the feature of the Intel NIC, but he has overtaken that packets on different directions for one stream will be dispatched to different core (Matching Engineer), many attacking warnings will not be reported for this reason. We have ever amended this problem by allowing the driver to re-compute the hash value if the source address is bigger than destination address, and if the source address is less than destination address, hardware distributing mechanism is kept. But it impacts the performance, although it is stream based, the performance of the method is only 60% of the method [16] introduced. Furthermore, Intel NIC only has 4 fixed queues, but the latest CPU can support 8 cores, the packets in 4 queues cannot be dispatched to 8 cores.

The host creates several ringed buffers, and tells the program running on the embedded multi-core NPU the number of ringed buffers, ring descriptors, length, head and tail pointers of the ring through shared memory. NPU then calculate the corresponded queue that each stream data block will be dispatched according to the information given by the CPU.

## VI. Implementation and Performance Evaluation

### A. Implementation

A Stream Reassembly Card is developed using XLS416 produced by Raza Microelectronics, Inc (RMI). The RMI XLS416 is a multi-core, multi-thread MIPS64 processor with a rich set of integrated I/O. XLS 416 has 4 cores and every core has 4 threads, so the total thread number is 16. One thread (referred as timeout thread) is used to take charge of the timeout management, and the other threads (referred as packet processing threads) all execute the same routine, whose job is receiving packets, assembly, and submission, when the timeout thread find that any stream has been timed out, it will send a message to the corresponding thread to notify which stream has been timed out, then every packet processing thread circularly check if there is any timeout message after processing one packet.

XLS 416 has three frequency models: 800M, 1.0G and 1.2G; for the best of the performance, we used the XLS with 1.2G Hz. XLS 416 integrates eight Gigabit Ethernet or two Ten Gigabit Ethernet. To further save the PCB size and consider that the Ten Gigabit Ethernet may be the mainstream link of the campus network, 2 ten-Gigabit interfaces are adopted to

SRC. Our SRC has 4G DRAM with 533 MHz and 1 PCIe1.1 × 4 Bus used to connect to the host. The interface chip is VSC8486-11 that connect the fiber module and the XLS through XAUI. DIMM chips are used instead of DIMM strips, for it occupies less PCB space and the stability is better. The total chip's power consumption is under 26 watts.

In the software level, there are a stream reassembly program running on the SRC and a Driver running on the host. Program running on the SRC is bound to one Image with the RMI OS and is burned into the Flash, which is also used to boot the system. We provide an SRC_API extending from Libnids. In addition to the feature of the Libnids, our SRC_API can be used to obtain the statistics and set the number of the analyses threads running on the host, timeout of the stream, and the BlockSize. 2M space is used to share information by the CPU and NPU, and 64M byte space per capturing thread running on the CPU.

### B. Evaluation

The test topology is depicted in Figure. 3. Dell PowerEdge R710 Server with an Xeon 2.13Ghz E5606 CPU, and total 16GB ECC DDR3 (4x4GB) is used to host the SRC. R710 Server has a PCIe × 8 Bus which can be used to hold the joint of the SRC. Red Hat Enterprise Server 64Bit with a 2.6.18-92.el5 kernel is used as the Operation System. An IXIA XM2 with an Xcellon-Ultra NP 10GbE Load Module is used to construct the evaluation environment. The application level test is carried out by IXIA XM2 [20].

The HTTP is used as the traffic load. Two XM2 ports are used to emulate the traffic between one server and multi-clients. To make use of the transferring bandwidth fully, 8 capture threads in the host are used. To gain the relationship between the NPU core number and stream reassembly performance, we test the performance under different core number circumstance. Since every core has 4 threads, when one core is tested, one thread is used as timeout thread and the other 3 threads are used to reorder the packets; and when two cores are tested, one thread is used as timeout thread and the other 7 threads are used to reorder the packets, and so forth. Because the traditional NIDS used Libnids [8] to conduct its stream reassembly, we tested its performance and the results are depicted in the last column of Table. I.

More cores lead to higher performance, and longer packets produce higher performance. It is also revealed that if all the cores are used, the performance is close to that of the packet capture. It means that when all the threads in the NPU are turned on to reassemble the packets, the performance is near to the PCI transferring ability, so it can be inferred that if the PCI multiplying factor is 8, the performance will be higher than the current implementation. As we know, the average packet length is between 300 and 400 bytes, so the performance of the real environment will be higher than 3Gbps. That is to say, while we formerly used three high performance server to conduct the stream reassembly, now one SRC can accomplish the same task.

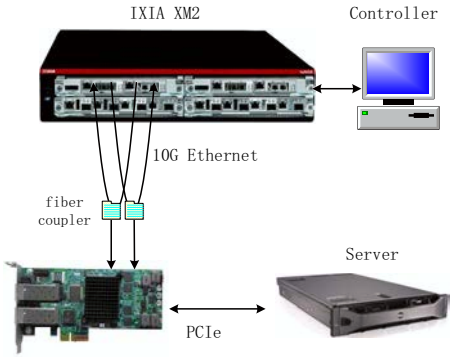



Fig. 3. Stream Reassembly Performance Test Environment.

TABLE I
THROUGHPUT OF SRC AND LIBNIDS.

| Packet Length[1] | 1 core | 2 cores | 3 cores | 4 cores | Libnids |
|---|---|---|---|---|---|
| 64 | 0.22 | 0.33 | 0.61 | 0.64 | 0.45 |
| 128 | 0.25 | 0.47 | 0.98 | 1.18 | 0.48 |
| 256 | 0.59 | 1.02 | 2.50 | 3.11 | 0.82 |
| 512 | 0.75 | 1.51 | 2.66 | 3.48 | 0.93 |
| 1024 | 1.30 | 2.73 | 3.12 | 3.70 | 0.99 |
| 1500 | 1.45 | 2.98 | 3.11 | 3.85 | 1.21 |

[1] Unit: Byte.

## VII. CONCLUSION

The performance of TCP packet reassembly becomes the bottleneck as the matching performance is increasing. In this paper, a co-processing stream reassembly framework based on multi-core NPU has then been introduced as a card, so the packet capture and stream reassembly can be both solved by a card. And to heighten the performance, we brought forward Stream Table Dispatching, No-Locking Timeout, and Multi-channel Virtual Queue to improve the performance of the proposed SRC scheme. The solution adopted cannot hold much memory because the size and electricity limit, whereas the memory size is critical to the performance, we analyzed how much memory is need for a specified timeout, block size and throughput. Last, RMI XLS416 was used to implement a co-processing Stream Reassembly Card, The result showed that our scheme is about 3 times of Libnids used in the current predominant server.

## VIII. ACKNOWLEDGMENT

This work has been supported by the National High-Tech Research and Development Plan of China under Grant No.2011AA01A103 .

## REFERENCES

[1] N. Weaver, V. Paxson, and J. M. Gonzalez, "The shunt: an fpga-based accelerator for network intrusion prevention," in *Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays*, ser. FPGA '07. New York, USA: ACM, 2007, pp. 199–206.

[2] M. Labrecque and J. G. Steffan, "The case for hardware transactional memory in software packet processing," in *Proceedings of the 6th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, ser. ANCS '10, 2010, pp. 37–48.

[3] V. Giorgos, A. Spiros, P. Michalis, E. P. Markatos, and S. Ioannidis, "Gnort: High performance network intrusion detection using graphics processors." in *Proceedings of the 11th international symposium on Recent Advances in Intrusion Detection.* USA: SpringerLink, 2008, pp. 116–134.

[4] G. Vasiliadis, M. Polychronakis, S. Antonatos, E. P. Markatos, and S. Ioannidis, "Regular expression matching on graphics hardware for intrusion detection," in *Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection*, ser. RAID '09, Berlin, Heidelberg, 2009, pp. 265–283.

[5] G. Vasiliadis, M. Polychronakis, and S. Ioannidis, "Midea: a multi-parallel intrusion detection architecture," in *Proceedings of the 18th ACM conference on Computer and communications security*, ser. CCS '11. New York, USA: ACM, 2011, pp. 297–308.

[6] C.-H. Lin, C.-H. Liu, and S.-C. Chang., "Accelerating regular expression matching using hierarchical parallel machines on gpu," in *IEEE Globecom 2011 proceedings*, HOUSTON, TEXAS, USA, pp. 1–5.

[7] S. Egorov and G. Savchuk, "Snortran: An optimizing compiler for snort rules," *Fidelis Security Systems*, 2002.

[8] Libnids, http://libnids.sourceforge.net/.

[9] Tcpflow, http://afflib.org/software/tcpflow.

[10] K. chan Lan and J. Heidemann., "A measurement study of correlation of Internet flow characteristics," *Computer Networks*, vol. 50, no. 1, pp. 46–62, 2006.

[11] H.-A. Kim and D. O'Hallaron, "Counting network flows in real time," in *Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE*, vol. 7. IEEE, dec. 2003, pp. 3888–3893.

[12] G. Wagener, A. Dulaunoy, and T. Engel, "Towards an estimation of the accuracy of tcp reassembly in network forensics," in *Future Generation Communication and Networking, 2008. FGCN '08. Second International Conference on*, vol. 2. IEEE, dec. 2008, pp. 273–278.

[13] M. Zhang and J. Ju, "Space-economical reassembly for intrusion detection system." *Information and Communications Security*, pp. 393–404, 2003.

[14] S. Dharmapurikar and V. Paxson, "Robust tcp stream reassembly in the presence of adversaries," in *Proceedings of the 14th conference on USENIX Security Symposium - Volume 14*, Berkeley, CA, USA, 2005.

[15] E. M. L. Gorka Aguirre Cascallana, "Collecting packet traces at high speed," 2006.

[16] L. Deri, N. S. P. A, V. D. B. Km, and L. L. Figuretta, "Improving passive packet capture: Beyond device polling," in *Proceedings of SANE*, vol. 2004, pp. 85–93.

[17] J. V. Lunteren, T. Engbersen, and S. Member, "Fast and scalable packet classification," *IEEE Journal on Selected Areas in Communications*, vol. 21, pp. 560–571, 2003.

[18] L. Deri, "ncap: Wire-speed packet capture and transmission," in *End-to-End Monitoring Techniques and Services, 2005. Workshop on*. IEEE, 2005, pp. 47–55.

[19] M. Smith and D. Loguinov, "Enabling high-performance internet-wide measurements on windows," in *PAM*, 2010, pp. 121–130.

[20] IXIA, http://www.ixiacom.com/.

DECLARATION OF SCOTT BRADNER

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

# Appendix W

US008813221B1

(12) **United States Patent**
**Dubrovsky et al.**

(10) **Patent No.: US 8,813,221 B1**
(45) **Date of Patent: *Aug. 19, 2014**

(54) **REASSEMBLY-FREE DEEP PACKET INSPECTION ON MULTI-CORE HARDWARE**

(75) Inventors: **Aleksandr Dubrovsky**, San Mateo, CA (US); **John E. Gmuender**, Sunnyvale, CA (US); **Huy Minh Nguyen**, Fountain Valley, CA (US); **Ilya Minkin**, Los Altos, CA (US); **Justin M. Brady**, San Jose, CA (US); **Boris Yanovsky**, Saratoga, CA (US)

(73) Assignee: **SonicWALL, Inc.**, San Jose, CA (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1015 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/238,205**

(22) Filed: **Sep. 25, 2008**

(51) **Int. Cl.**
***G06F 11/00*** (2006.01)

(52) **U.S. Cl.**
USPC ..... **726/22**; 726/23

(58) **Field of Classification Search**
CPC ..... H04L 47/34; H04L 63/14; H04L 63/1416; H04L 63/145; H04L 45/00; H04I 63/1408; G06F 21/00
USPC ..... 726/22, 23
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 5,796,942 | A | 8/1998 | Esbensen | |
| 5,945,933 | A | 8/1999 | Kalkstein | |
| 6,088,803 | A | 7/2000 | Tso et al. | |
| 6,108,782 | A | 8/2000 | Fletcher et al. | |
| 6,119,236 | A | 9/2000 | Shipley | |
| 6,178,448 | B1 | 1/2001 | Gray et al. | |
| 6,219,706 | B1 | 4/2001 | Fan et al. | |
| 6,449,723 | B1 | 9/2002 | Elgressy et al. | |
| 6,851,061 | B1 | 2/2005 | Holland et al. | |
| 7,134,143 | B2 | 11/2006 | Stellenberg et al. | |
| 7,185,368 | B2 | 2/2007 | Copeland, III | |
| 7,304,996 | B1 | 12/2007 | Swenson et al. | |
| 2002/0083331 | A1 | 6/2002 | Krumel | |
| 2003/0084328 | A1 | 5/2003 | Tarquini et al. | |
| 2003/0110208 | A1 * | 6/2003 | Wyschogrod et al. | 709/202 |
| 2003/0145228 | A1 | 7/2003 | Suuronen et al. | |

(Continued)

FOREIGN PATENT DOCUMENTS

| | | |
|---|---|---|
| EP | 1 122 932 | 8/2001 |
| EP | 1 528 743 | 5/2005 |
| WO | WO 97/39399 | 10/1997 |

OTHER PUBLICATIONS

Villa (Feb. 2008). IBM Research Report: Too many words, too little time: Accelerating real-time keyword scanning with multi-core processors. Retrieved from http://domino.research.ibm.com/library/cyberdig.nsf/papers/9EB4740B4B0739CF852573F5005A6311/$File/rc24488.pdf. Retrieval data Mar. 5, 2012.*

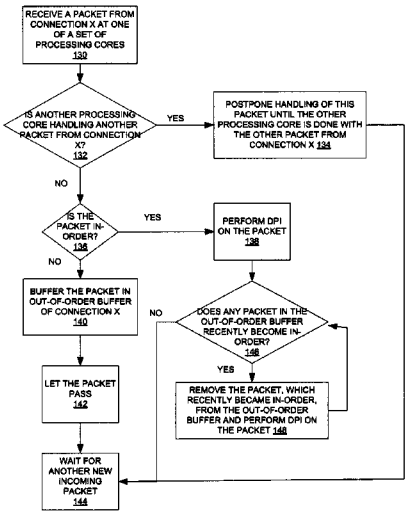
(Continued)

*Primary Examiner* — Brian Shaw
(74) *Attorney, Agent, or Firm* — Lewis Roca Rothgerber LLP

(57) **ABSTRACT**

Some embodiments of reassembly-free deep packet inspection (DPI) on multi-core hardware have been presented. In one embodiment, a set of packets of one or more files is received at a networked device from one or more connections. Each packet is scanned using one of a set of processing cores in the networked device without buffering the one or more files in the networked device. Furthermore, the set of processing cores may scan the packets substantially concurrently.

**16 Claims, 7 Drawing Sheets**



(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 2004/0093513 | A1 | 5/2004 | Cantrell et al. | |
| 2004/0123155 | A1 | 6/2004 | Etoh et al. | |
| 2004/0255163 | A1 | 12/2004 | Swimmer et al. | |
| 2005/0120243 | A1 | 6/2005 | Palmer et al. | |
| 2005/0216770 | A1 | 9/2005 | Rowett et al. | |
| 2005/0262556 | A1 | 11/2005 | Waisman et al. | |
| 2006/0020595 | A1 | 1/2006 | Norton et al. | |
| 2006/0069787 | A1 | 3/2006 | Sinclair | |
| 2006/0077979 | A1 * | 4/2006 | Dubrovsky et al. | 370/394 |
| 2007/0058551 | A1 | 3/2007 | Brusotti et al. | |

OTHER PUBLICATIONS

"The Ultimate Internet Sharing Solution, WinProxy, User Manual," Copyright 1996-2002 Osistis Software, Inc., dated Feb. 2002 (290 pgs).

Roesch, Martin and Green, Chris, "Snort Users Manual," Snort Release 2.0.0, M. Roesch, C. Green, Copyright 1998-2003 M. Roesch, Copyright 2001-2003 C. Green, Copyright 2003 Sourcefire, Inc. dated Dec. 8, 2003 (53 pgs).

Bellovin, S., "Firewall-Friendly FTP," Network Working Group, RFC No. 1579, AT&T Bell Laboratories, Feb. 1994 , http://www.ietf.org/rfc1579.txt?number=1579, downloaded Jul. 15, 2002, 4 pages.

European Search Report, Application No. EP 04 02 5579, May 23, 2005, 3 pages.

Office Action for U.S. Appl. No. 10/697,846 mailed Jan. 5, 2007, 16 pages.

Kruegal, Christopher, et al. "Using Decision Trees to Improve Signature-Based Intrusion Detection", Sep. 8, 2003, RAID 2003: recent Advance in Intrusion Detection, 20 pages.

Branch, Joel, et al., "Denial of Service Intrusion Detection Using Time Dependent Deterministic Finite Automata", RPI Graduate Research Conference 2002, Oct. 17, 2002, 7 pages.

Juniper Networks, "Attack Prevention," www.juniper.net/products/intrusion/prevention.html, downloaded Jun. 11, 2004, 2 pages.

Juniper Networks, "Attack Detection," www.juniper.net/products/intrusion/detection.html, downloaded Jun. 11, 2004, 7 pages.

Juniper Networks, "Intrusion Detection and Prevention," www.juniper.net/products/intrusion/downloaded Jun. 11, 2004, 2 pages.

Juniper Networks, "Architecture," www.juniper.net/products/intrusion/architecture.html, downloaded Jun. 11, 2004, 3 pages.

Juniper Networks, "Juniper Networks NetScreen-IDP 10/100/500/1000," Intrusion Detection and Prevention, Spec Sheet, Apr. 2004, 2 pages.

Roberts, Paul, "NetScreen Announces Deep Inspection Firewall," IDG News Service, Oct. 20, 2003, http://www.nwfusion.com/news/2003/1020netscannou.html, downloaded Jun. 11, 2004, 5 pages.

Snort.org, "The Open Source Network Intrusion Detection System", www.snort.org/about.html, 2 pages.

Blyth, Andrew, "Detecting Intrusion", School of Computing, University of Glamorgan, 14 pages.

Office Action mailed Mar. 1, 2010 for U.S. Appl. No. 11/112,252, filed Apr. 21, 2005., 40 pages.

Final Office Action mailed Oct. 19, 2009 for U.S. Appl. No. 11/112,252, filed Apr. 21, 2005., 32 pages.

Office Action mailed Mar. 31, 2009 for U.S. Appl. No. 11/112,252, filed Apr. 21, 2005., 35 pages.

Office Action mailed Apr. 29, 2008 of U.S. Appl. No. 11/112,252, filed Apr. 21, 2005. 25 pages.

Office Action mailed Nov. 14, 2008 of U.S. Appl. No. 11/112,252, filed Apr. 21, 2005. 26 pages.

Office Action mailed Oct. 2, 2007 of U.S. Appl. No. 10/964,871, filed Oct. 13, 2004. 19 pages.

Final Office Action mailed Mar. 20, 2008 of U.S. Appl. No. 10/964,871, Oct. 13, 2004. 19 pages.

Office Action mailed Jul. 16, 2008 of U.S. Appl. No. 10/964,871, Oct. 13, 2004. 21 pages.

Office Action mailed Jan. 9, 2009 of U.S. Appl. No. 10/964,871, Oct. 13, 2004. 21 pages.

"SonicWALL Content Filtering Service," Comprehensive Internet Security™, © 2005, 2pp.

SonicW ALL Internet Security Appliances, "Content Security Manager Integrated Solutions Guide", Version 3.0, © 2007, 160 pp.

SonicW ALL Internet Security Appliances, "SonicOS 3.8 Standard Administrator's Guide", © 2007, 362 pp.

"SonicOS Standard 3.8.0.2 Release Notes, SonicWALL Secure Anti-Virus Router 80 Series," SonicW ALL, Inc., Software Release: Apr. II, 2007, 13 pp.

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Unified Threat Management, Intelligent Real-time Protection, © 2005 , 2 pp.

"SonicWALL Endpoint Security: Anti-Virus, Automated and Enforced Anti-Virus and Anti-Spyware Protection," © 2007, Mar. 2007, 2 pp.

"SonicWaLL Content Security Manager Series, Easy-to-use, Affordable, Content Security and Internet Threat Protection," © 2006, Dec. 2006, 4 pp.

"SonicWALL Complete Anti-Virus, Automated and Enforced Anti-Virus Protection," © 2005, 2 pp.

Aggarwal, N., "Improving the Efficiency of Network Intrusion Detection Systems", Indian Institue of Technology, May 3, 2006, pp. 1-40.

Van Engelen, R., "Constucting Finite State Automata for High-Performance XML Web Services," International Symposium on Web Services and Applications, 2004, pp. 1-7.

Lucas, Simon M., et al., "Learning Deterministic Finite Automata with a Smart State Labeling Evolutionary Algorithm," IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 27, No. 7, Jul. 2005, pp. 1063-1074.

Office Action mailed Jul. 7, 2010 of U.S. Appl. No. 11/778,546, Jul. 16, 2007. 15 pages.

Office Action mailed May 14, 2009 of U.S. Appl. No. 11/772,723, Jul. 2, 2007. 7 pages.

Office Action mailed Oct. 23, 2009 of U.S. Appl. No. 11/772,723, Jul. 2, 2007. 8 pages.

* cited by examiner

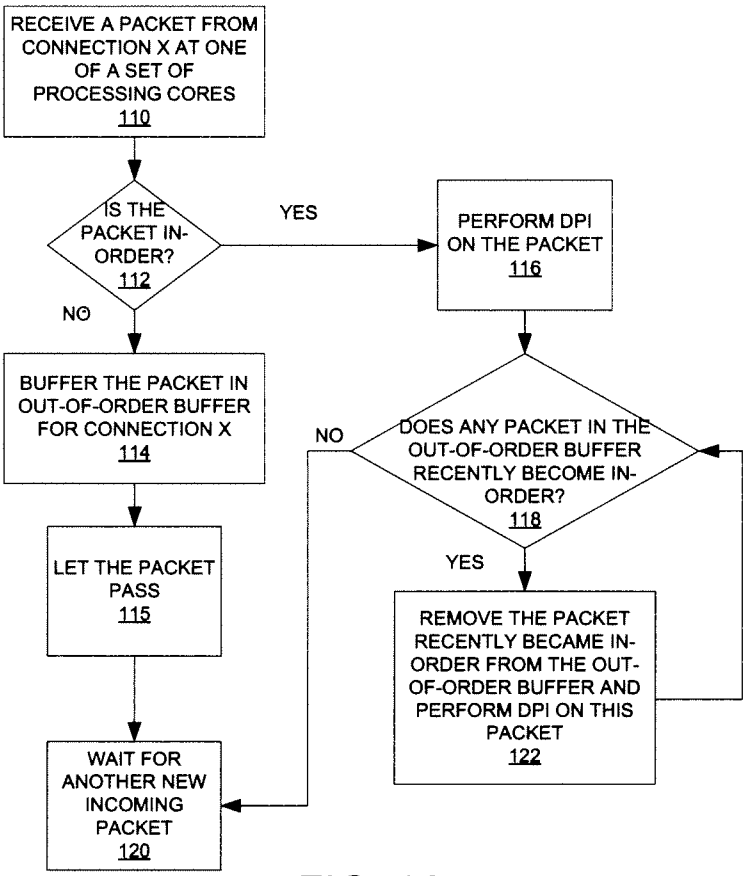

RECEIVE A PACKET FROM CONNECTION X AT ONE OF A SET OF PROCESSING CORES
110
IS THE PACKET IN-ORDER?
112
YES
NO
PERFORM DPI ON THE PACKET
116
BUFFER THE PACKET IN OUT-OF-ORDER BUFFER FOR CONNECTION X
114
DOES ANY PACKET IN THE OUT-OF-ORDER BUFFER RECENTLY BECOME IN-ORDER?
118
NO
YES
LET THE PACKET PASS
115
REMOVE THE PACKET RECENTLY BECAME IN-ORDER FROM THE OUT-OF-ORDER BUFFER AND PERFORM DPI ON THIS PACKET
122
WAIT FOR ANOTHER NEW INCOMING PACKET
120

FIG. 1A

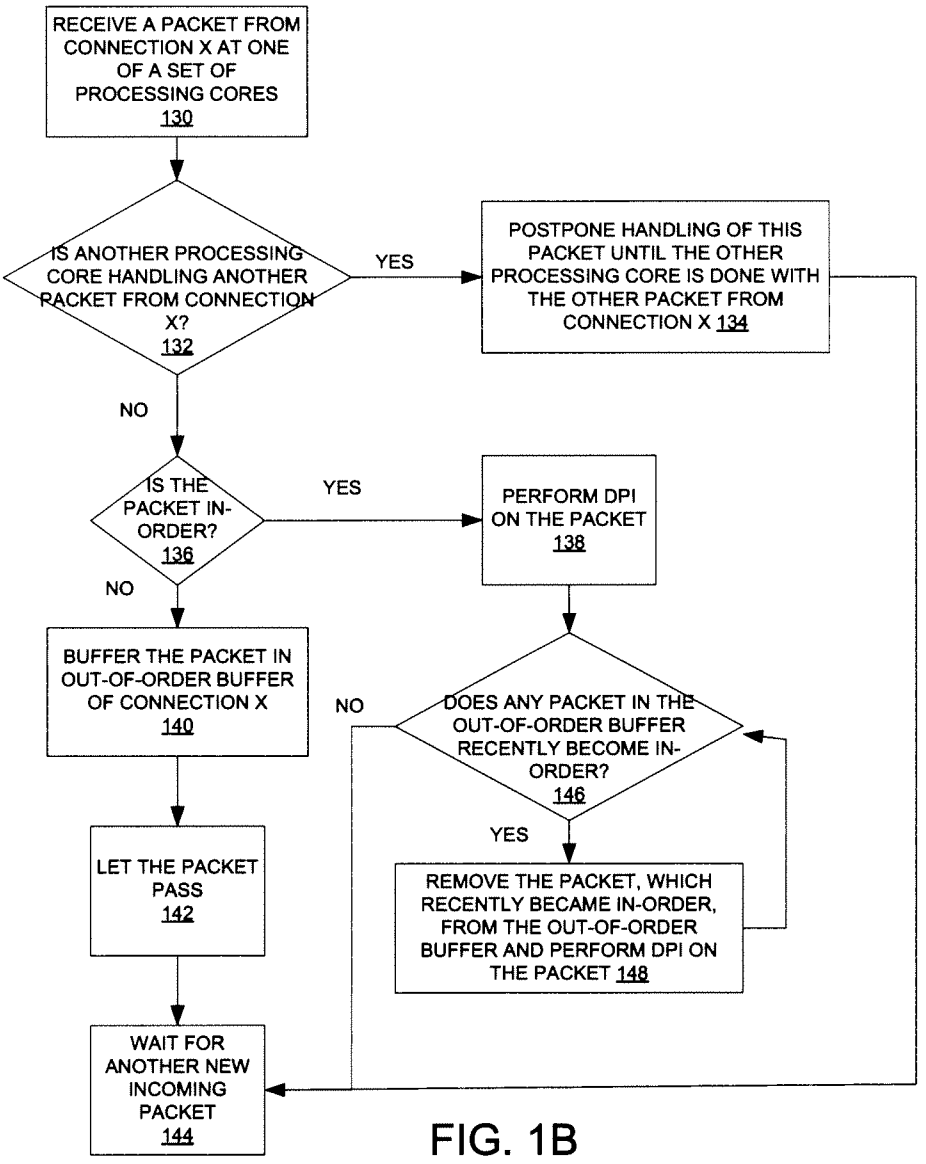

RECEIVE A PACKET FROM CONNECTION X AT ONE OF A SET OF PROCESSING CORES 130
IS ANOTHER PROCESSING CORE HANDLING ANOTHER PACKET FROM CONNECTION X? 132
YES
POSTPONE HANDLING OF THIS PACKET UNTIL THE OTHER PROCESSING CORE IS DONE WITH THE OTHER PACKET FROM CONNECTION X 134
NO
IS THE PACKET IN-ORDER? 136
YES
PERFORM DPI ON THE PACKET 138
NO
BUFFER THE PACKET IN OUT-OF-ORDER BUFFER OF CONNECTION X 140
DOES ANY PACKET IN THE OUT-OF-ORDER BUFFER RECENTLY BECOME IN-ORDER? 146
NO
YES
LET THE PACKET PASS 142
REMOVE THE PACKET, WHICH RECENTLY BECAME IN-ORDER, FROM THE OUT-OF-ORDER BUFFER AND PERFORM DPI ON THE PACKET 148
WAIT FOR ANOTHER NEW INCOMING PACKET 144

FIG. 1B

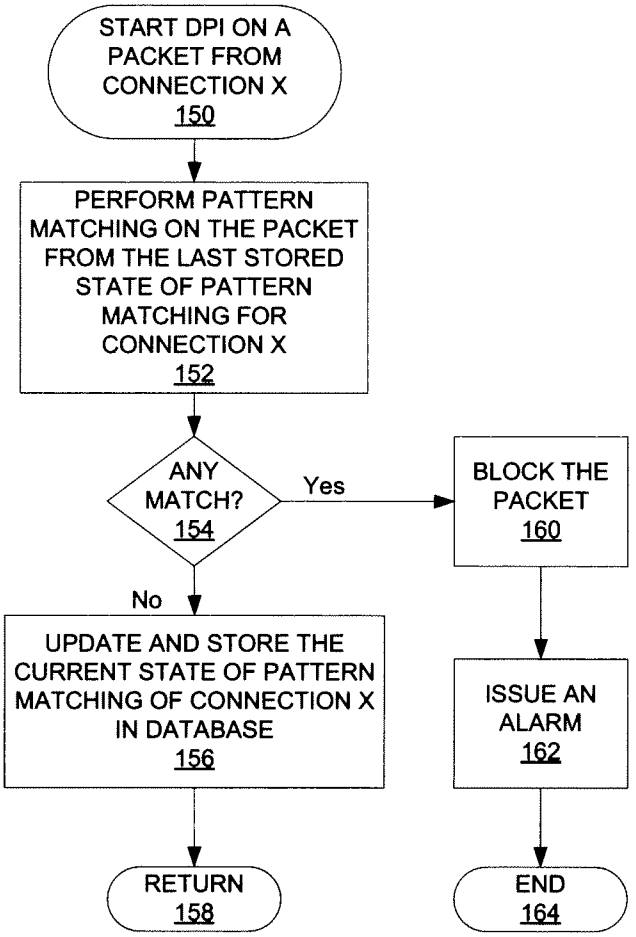

START DPI ON A PACKET FROM CONNECTION X
150
PERFORM PATTERN MATCHING ON THE PACKET FROM THE LAST STORED STATE OF PATTERN MATCHING FOR CONNECTION X
152
ANY MATCH?
154
Yes
BLOCK THE PACKET
160
No
UPDATE AND STORE THE CURRENT STATE OF PATTERN MATCHING OF CONNECTION X IN DATABASE
156
ISSUE AN ALARM
162
RETURN
158
END
164

Figure 1C

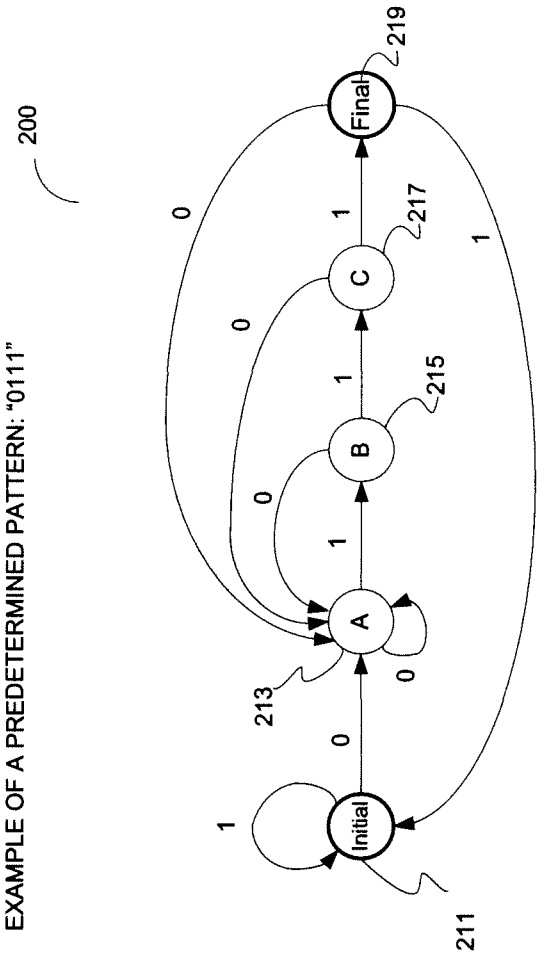

EXAMPLE OF A PREDETERMINED PATTERN: "0111"
200
Initial
A
B
C
Final
211
213
215
217
219
0
1

Figure 2

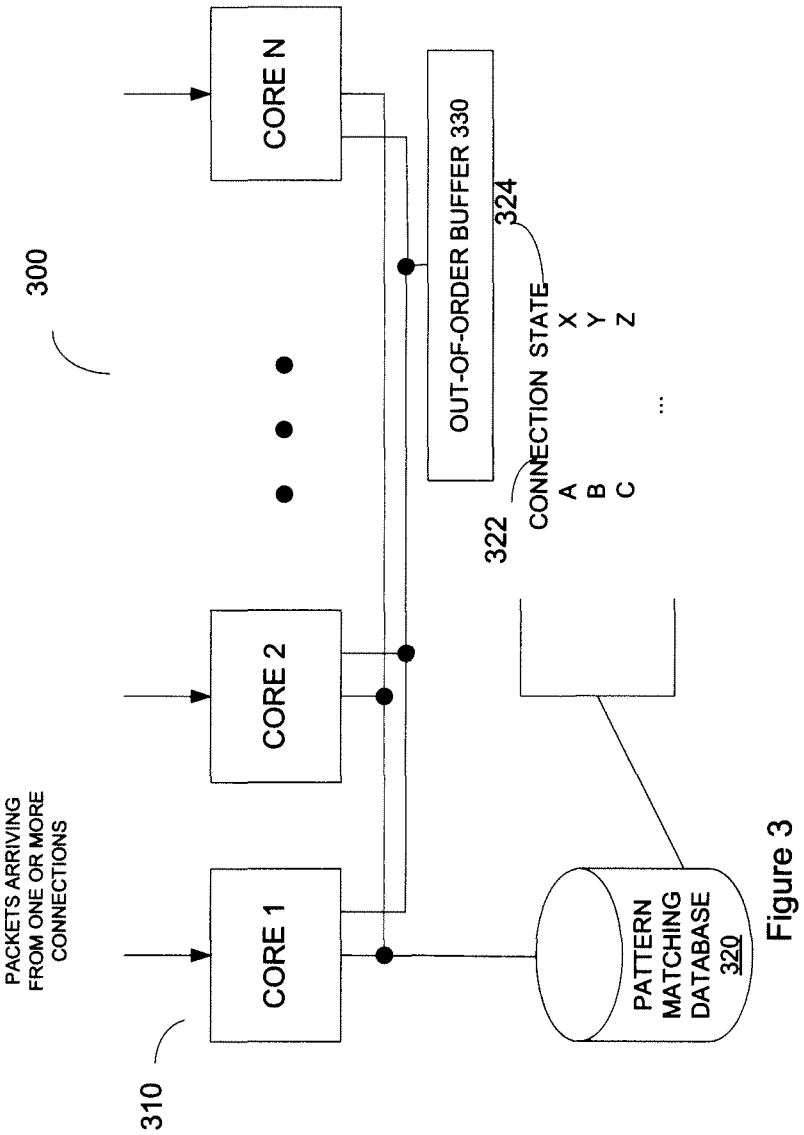

CORE N
CORE 2
CORE 1
300
310
PACKETS ARRIVING FROM ONE OR MORE CONNECTIONS
OUT-OF-ORDER BUFFER 330
324
CONNECTION STATE
322
A
B
C
X
Y
Z
...
PATTERN MATCHING DATABASE 320

Figure 3

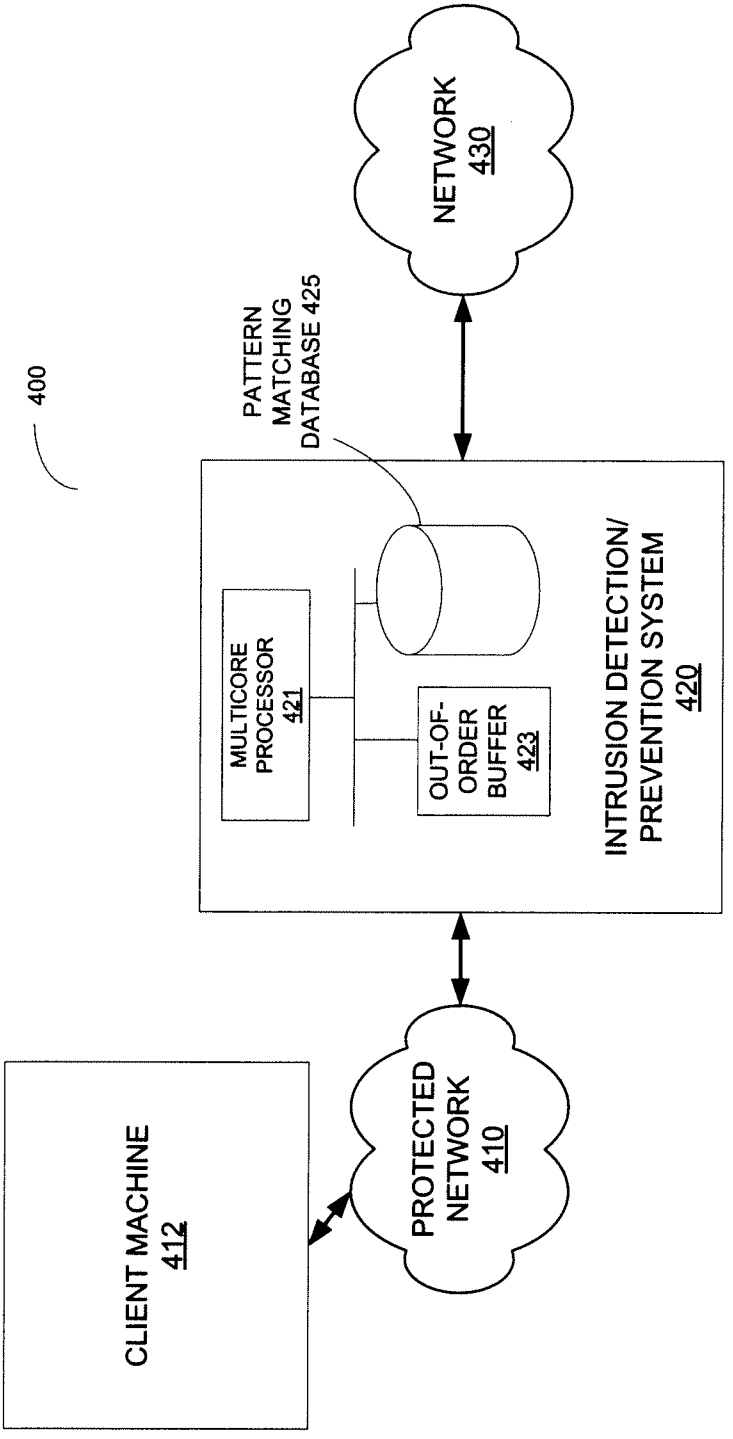

400
NETWORK
430
PATTERN
MATCHING
DATABASE 425
MULTICORE
PROCESSOR
421
OUT-OF-
ORDER
BUFFER
423
INTRUSION DETECTION/
PREVENTION SYSTEM
420
PROTECTED
NETWORK
410
CLIENT MACHINE
412

Figure 4

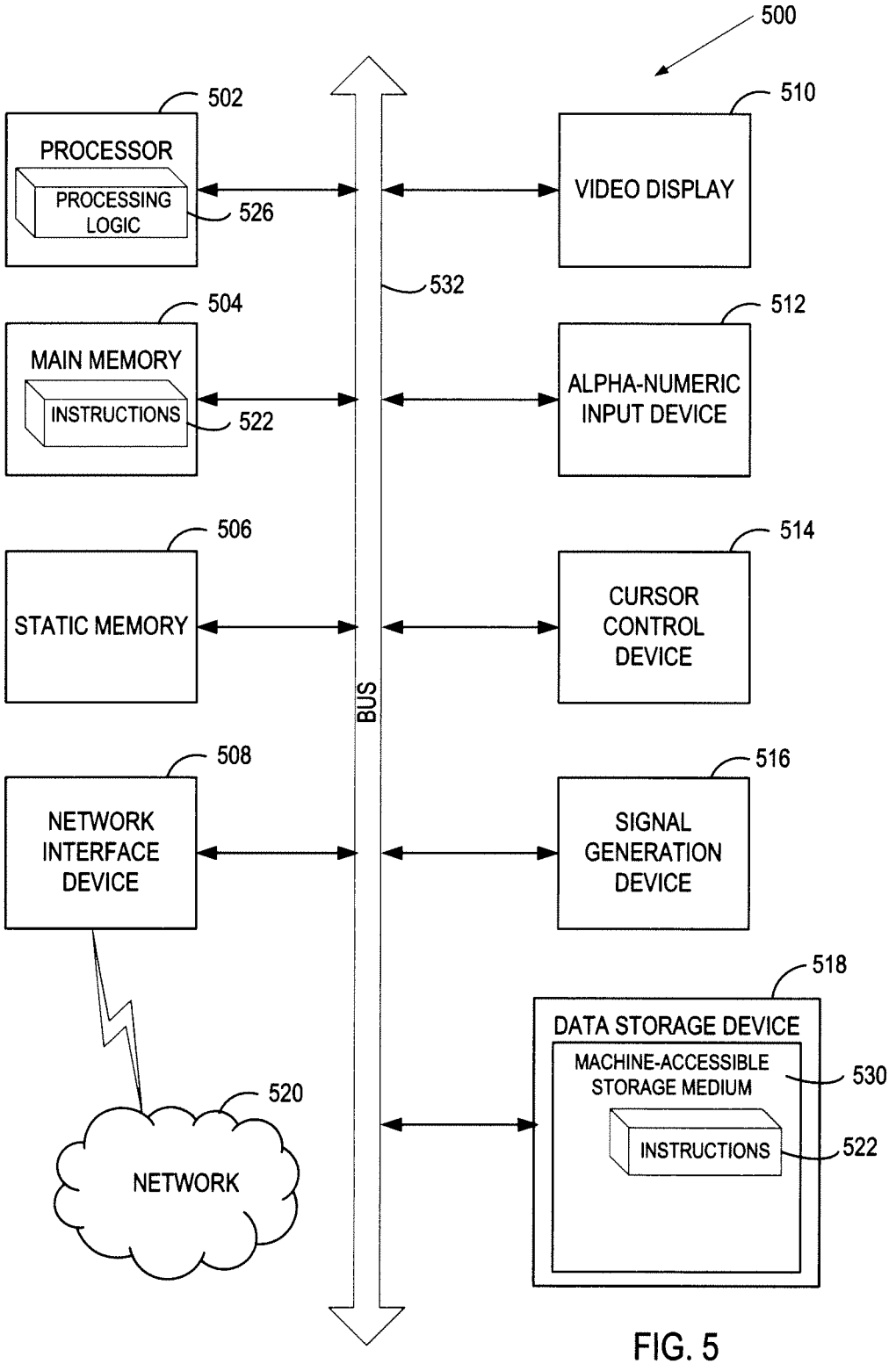

500
502
PROCESSOR
PROCESSING LOGIC
526
504
MAIN MEMORY
INSTRUCTIONS
522
506
STATIC MEMORY
508
NETWORK INTERFACE DEVICE
520
NETWORK
BUS
532
510
VIDEO DISPLAY
512
ALPHA-NUMERIC INPUT DEVICE
514
CURSOR CONTROL DEVICE
516
SIGNAL GENERATION DEVICE
518
DATA STORAGE DEVICE
MACHINE-ACCESSIBLE STORAGE MEDIUM
530
INSTRUCTIONS
522

FIG. 5

# REASSEMBLY-FREE DEEP PACKET INSPECTION ON MULTI-CORE HARDWARE

## TECHNICAL FIELD

The present invention relates to intrusion detection and prevention in a networked system, and more particularly, to performing multiple packet payloads analysis on multi-core hardware.

## BACKGROUND

Today, in many security products, scanning by pattern matching is used to prevent many types of security attacks. For example, some existing desktop virus scanning may include scanning files against certain recognizable patterns. These files may come from mail attachments or website downloads. These desktop applications are simpler in that by the time the pattern matching is performed, the input has been all accumulated in the correct order. The situation is more complicated for gateway products, such as firewalls, attempting to match patterns for other purposes. Some of these products scan for patterns over Transport Control Protocol (TCP) packets. Since TCP usually breaks down application data into chunks called TCP segments, the full pattern may reside in several TCP segments. One conventional approach is to reassemble all TCP packets together into one large chunk and perform pattern matching on this chunk, similar to scanning files. The disadvantage of this approach is that this approach requires processing to reassemble, and it further requires memory to buffer the intermediate result before pattern matching can take place.

To further complicate the problem, many security attacks exhibit more than one pattern, and thus, multiple pattern matching has to be performed in order to successfully screen out these attacks. Such a collection of patterns is called a signature. For example, an attack signature may contain a recognizable header and a particular phrase in the body. To detect such an attack, the detection mechanism has to match all the patterns in the signature. If only part of the signature is matched, false positives may occur. As such, the term "attack pattern" is used to refer to a single pattern or a signature.

When such attacks are transported over TCP, the contents, and therefore the recognizable patterns, may exist in different TCP segments. In fact, even a single pattern is often split over several segments. Therefore, two problems have to be solved at the same time. On one hand, the detection mechanism has to scan each pattern across multiple segments, and on the other hand, the detection mechanism also has to scan across patterns. One existing approach is to reassemble all packets and scan for each pattern in sequence. This approach is inefficient in terms of processing time and memory usage because scanning cannot start until all packets are received and reassembled and extra memory is needed to store the packets received.

Another problem in pattern matching is that the packets may arrive out of order. Again, using TCP as an example, the application data is broken into what TCP considers the best sized chunks to send, called a TCP segment or a TCP packet. When TCP sends a segment, it maintains a timer and waits for the other end to acknowledge the receipt of the segment. The acknowledgement is commonly called an ACK. If an ACK is not received for a particular segment within a predetermined period of time, the segment is retransmitted. Since the IP layer transmits the TCP segments as IP datagrams and the IP datagrams can arrive out of order, the TCP segments can arrive out of order as well. Currently, one receiver of the TCP segments reassembles the data so that the application layer receives data in the correct order.



An existing Intrusion Detection/Prevention System (IPS) typically resides between the two ends of TCP communication, inspecting the packets as the packets arrive at the IPS. The IPS looks for predetermined patterns in the payloads of the packets. These patterns are typically application layer patterns. For example, the pattern might be to look for the word "windows." However, the word may be broken into two TCP segments, e.g., "win" in one segment and "dows" in another segment. If these two segments arrive in the correct order, then IPS can detect the word. However, if the segments arrive out of order, which happens relatively often, then the IPS may first receive the segment containing "dows", and have to hold this segment and wait for the other segment. A typical approach is for the IPS to force the sender to retransmit all the segments from the last missing one, hoping that the segments may arrive in order the second time. One disadvantage of this approach is the additional traffic in between and the additional processing on both ends of the TCP communication.

To take advantage of the introduction of multi-core processors (e.g., Intel® Core™2 Quad Processors from Intel Corporation of Santa Clara, Calif.), some conventional ISPs use multi-core processors to scan incoming segments to speed up the process. In general, each multi-core processor has two or more processing cores. According to one conventional approach, one of the processing cores is used to completely reassemble the file while the remaining processing cores perform scanning or pattern matching in the background after the file has been completely reassembled. However, this approach does not scale in terms of having enough memory to store all files. Also, background scanning by multiple processing cores is less efficient due to extra memory copying overhead and extra scheduling processing overhead.

## BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which:

FIG. **1**A illustrates one embodiment of a method to perform multiple packet analysis on multi-core hardware.

FIG. **1**B illustrates an alternate embodiment of a method to perform multiple packet analysis on multi-core hardware.

FIG. **1**C illustrates one embodiment of a method to perform deep packet inspection.

FIG. **2** illustrates an exemplary Deterministic Finite Automaton (DFA) according to one embodiment of the invention.

FIG. **3** illustrates a functional block diagram of one embodiment of multi-core hardware usable to perform multiple packet analysis.

FIG. **4** illustrates one embodiment of a system in which embodiments of the present invention may be implemented.

FIG. **5** illustrates a block diagram of an exemplary computer system, in accordance with one embodiment of the present invention.

## DETAILED DESCRIPTION

Described herein are some embodiments of reassembly-free deep packet inspection on multi-core hardware. In one embodiment, a set of packets of one or more files is received at a networked device from one or more connections. Each packet is scanned using one of a set of processing cores in the

networked device without buffering the one or more files in the networked device. Furthermore, the set of processing cores may scan the packets substantially concurrently.

In the following description, numerous details are set forth. It will be apparent, however, to one skilled in the art, that the present invention may be practiced without these specific details. In some instances, well-known structures and devices are shown in block diagram form, rather than in detail, in order to avoid obscuring the present invention.

Some portions of the detailed descriptions below are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

The present invention also relates to apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer-readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, flash memory, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general-purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein.

FIG. **1**A illustrates one embodiment of a method to perform multiple packet analysis on multi-core hardware, where multiple processing cores of a set of processing cores are allowed to handle packets from the same connection (hereinafter, "connection X"). In some embodiments, the set of processing cores includes processing cores of a multi-core processor. The method may be performed by processing logic that may comprise hardware (e.g., circuitry, dedicated logic, programmable logic, processing cores, etc.), software (such as instructions run on a processing core), firmware, or a combination thereof.

Initially, one of a set of processing cores receives a packet from connection X (processing block **110**). The packet is part of a file, which may be re-constructed by re-assembling the packet with other packets of the file. Then the processing core determines if the packet is in-order (processing block **112**). For example, the processing core may check a sequence number in a header of the packet against a next packet sequence number of connection X, which may be stored in a database commonly accessible by the processing cores.

If the packet is not in-order, i.e., out-of-order, then the processing core may buffer the packet in an out-of-order buffer associated with connection X (processing block **114**). The processing core may allow the packet to pass (processing block **115**). Then the processing core waits for another new incoming packet (processing block **120**).

If the packet is in-order, then the processing core performs deep packet inspection (DPI) on the packet (processing block **116**). Details of some embodiments of DPI are discussed below. Then the processing core checks if there is any packet in the out-of-order buffer associated with connection X that recently became in-order (processing block **118**). If there is no packet in the out-of-order buffer associated with connection X that is next in sequence (in-order), the processing core transitions to processing block **120** to wait for another new incoming packet. Otherwise, if there is a packet in the out-of-order buffer associated with connection X that is now in-order, then the processing core removes this packet and performs DPI on this packet (processing block **122**). When the processing core completes DPI on this packet, the processing core returns to processing block **118** to check if there is another packet in the out-of-order buffer associated with connection X that is in-order.

Note that the incoming packets are scanned without buffering the file for reassembly because the packets can be inspected for the predetermined pattern without being reassembled into the file. Thus, the above technique is well suited for IPSs that have limited capacity for buffering or storage. Furthermore, the above technique allows the set of processing cores to scan incoming packets substantially concurrently. Therefore, the speed of the scanning may be improved over conventional approaches.

FIG. **1**B illustrates one embodiment of a method to perform multiple payload analysis on multi-core hardware, where only a single core in a set of processing cores is allowed to handle packets from a particular connection (hereinafter, "connection X") at a time. In some embodiments, the set of processing cores includes processing cores of a multi-core processor. The method may be performed by processing logic that may comprise hardware (e.g., circuitry, dedicated logic, programmable logic, processing cores, etc.), software (such as instructions run on a processing core), firmware, or a combination thereof.

Initially, one processing core of the set of processing cores receives a packet from connection X (processing block **130**). Then the processing core checks if there is another processing core in the set of processing cores handling another packet from connection X (processing block **132**). If there is another processing core handling another packet from connection X

currently, then the processing core postpones handling of this packet until the other processing core is done with the other packet from connection X (processing block **134**). The processing core may transition to processing block **144** to wait for another new incoming packet.

If the processing core determines that there is no other processing core in the set of processing cores handling another packet from connection X, then the processing core checks if this packet is in-order (processing block **136**). If this packet is not in-order, i.e., out-of-order, then the processing core buffers this packet in an out-of-order buffer associated with connection X (processing block **140**). The processing core may allow this packet to pass (processing block **142**). Then the processing core waits for another new incoming packet (processing block **144**).

If the processing core determines that this packet is in-order, then the processing core performs DPI on this packet (processing block **138**). Details of some embodiments of DPI are discussed below. After performing DPI on the packet, the processing core checks if there is any packet in the out-of-order buffer associated with connection X, which is now in-order (processing block **146**). If there is a packet in the out-of-order buffer that is now in-order, then the processing core removes the packet that recently became in-order from the out-of-order buffer and performs DPI on this packet (processing block **148**). Then the processing core returns to processing block **146** to repeat the above process. If there is no packet in the out-of-order buffer that is in-order, then the processing core transitions to processing block **144** to wait for another new incoming packet.

Like the technique illustrated in FIG. **1**A, the technique illustrated in FIG. **1**B also allows scanning of the incoming packets without buffering the file for reassembly because the packets can be scanned for the predetermined pattern, without reassembling the packets into the file, by DPI.

FIG. **1**C illustrates one embodiment of a method to perform deep packet inspection (DPI) using one of a set of processing cores. In some embodiments, the set of processing cores includes processing cores of a multi-core processor. The method may be performed by processing logic that may comprise hardware (e.g., circuitry, dedicated logic, programmable logic, processing cores, etc.), software (such as instructions run on a processing core), firmware, or a combination thereof.

Initially, the processing core starts DPI on a packet from connection X at block **150**. This packet is hereinafter referred to as the current packet. The processing core performs pattern matching on the current packet from the last stored state of pattern matching for connection X (processing block **152**). Specifically, the processing core is trying to look for a predetermined pattern or signature in the incoming packets, which may be associated with a computer virus or malicious code. By identifying such pattern or signature in the incoming packets and blocking at least one of the packets containing part of the predetermined pattern or signature, the set of processing cores can protect a system from computer viral attack. In some embodiments, the last stored state of pattern matching for connection X is stored in a database commonly accessible by the set of processing cores. As such, each of the set of processing cores can handle packets from connection X, even though some of the packets may be inspected by different processing cores.

In some embodiments, if there is a match between a predetermined pattern and the data pattern in the incoming packets inspected so far (which includes the current packet), then the processing core blocks the current packet (processing block **160**). Then the processing core may issue an alarm to warn a system administrator of detection of potentially malicious code or virus in the incoming packets (processing block **162**), and the process ends at block **164**.

If there is no match between the predetermined pattern and the data pattern in the incoming packets inspected so far, then the processing core may update and store the current state of pattern matching of connection X in the database (processing block **156**). The method then ends at block **158**.

In some embodiments, pattern matching performed in DPI is accomplished using Deterministic Finite Automaton (DFA). An exemplary DFA is shown in FIG. **2** to illustrate the concept.

FIG. **2** illustrates an exemplary DFA according to one embodiment of the invention. In this example, an IPS is programmed to detect and to prevent a pattern of "0111" to pass through. The DFA **200** shown in FIG. **2** corresponds to this pattern. A set of processing cores may use the DFA **200** to perform pattern matching on a number of packets to determine whether the packets contain the pattern "0111". Furthermore, to simplify the illustration, it is assumed in this example that each packet contains only one digit. However, it should be appreciated that the concept is applicable to scenarios where a packet contains more than one digits and/or alphabetic letters.

Referring to FIG. **2**, the DFA **200** includes 5 states **211**-**219**. The states **211**-**219** in the DFA **200** may be referred to as nodes. A processing core in the set of processing cores begins pattern matching at the initial state **211**. If a packet received contains a "1", the processing core remains in the initial state **211**. If the packet contains a "0", which corresponds to the first digit in the predetermined pattern, the processing core transitions to the A state **213**.

If the processing core receives a "0" subsequently, the processing core remains in the A state **213**. If the processing core receives a "1", which corresponds to the second digit in the predetermined pattern, then the processing core transitions into the B state **215**. From the B state **215**, the processing core may transition back to the A state **213** if the next packet received contains a "0". If the next packet received contains a "1", which corresponds to the third digit in the predetermined pattern, then the processing core transitions to the C state **217**. However, note that another processing core in the set of processing cores may receive and process the next packet in some embodiments.

From the C state **217**, the processing core may transition back to the A state **213** if the next packet received contains a "0". If the next packet received contains a "1", which corresponds to the last digit in the predetermined pattern, then the processing core transitions to the final state **219**. When the processing core reaches the final state **219**, the processing core knows that the packets received so far contain the predetermined pattern. Hence, the processing core may perform the appropriate operations in response to receiving the predetermined pattern, such as blocking the packet of the predetermined pattern last received and issuing an alarm to alert system administrators. To keep track of which state of the DFA is in currently, the processing core stores the current state of the DFA in a database commonly accessible by the set of processing cores. As such, another processing core may continue pattern matching on the next packet from the current state if the other processing core receives the next packet. Furthermore, the current state of the DFA may be associated with a connection from which the packet is received so that the set of processing cores may inspect packets from multiple connections using the information from the database.

One advantage of using the DFA to perform pattern matching on packets is to eliminate the need to reassemble the

packets because the processing cores can walk through the DFA as each packet is received and examined. Because a pattern is typically broken up into a number of segments and each segment is transmitted using a packet, it is necessary to inspect multiple packets in order to identify the pattern. Using the DFA, the processing cores may not have to reassemble the packets in order to find out what the pattern contained in the packets is in order to match the pattern against a predetermined pattern. The processing cores may perform pattern matching on a packet-by-packet basis as each of the packets is received without reassembling the packets by walking through the DFA. If a processing core reaches a final state, there is a match between the pattern contained in the packets received so far and the predetermined pattern. There is no need to store the packets for reassembling the packets. Instead, the processing cores may simply store the current state of the DFA in a database commonly accessible by the processing cores.

The concept described above may be expanded to signature detection. A signature is a collection of multiple patterns. To keep track of which pattern within a signature is being matched, processing logic may use a tree structure, where each node within the tree structure corresponds to a pattern and each pattern is represented using a DFA. Alternatively, a single DFA may represent multiple patterns.

FIG. **3** illustrates a functional block diagram of one embodiment of multi-core hardware usable to perform multiple payload analysis in an IPS. The IPS may be implemented within a set-top box coupled to a protected network. The multi-core hardware **300** includes a set of processing cores **310**, a pattern matching database **320**, and an out-of-order buffer **330**. In some embodiments, the set of processing cores **310** includes processing cores in a multi-core processor. The processing cores **310** are communicably coupled to the database **320** so that each of the processing cores **310** may retrieve and update information in the database **320**. Likewise, the processing cores **310** are also communicably coupled to the out-of-order buffer **330** so that each of the processing cores **310** may access the out-of-order buffer **330**.

In some embodiments, the processing cores **310** receive packets from one or more connections. To prevent harmful virus or malicious code from reaching the protected network, the processing cores **310** performs reassembly-free DPI on the packets. When one of the processing cores **310** receives a packet, the processing core may determine if the packet is in-order or out-of-order. An out-of-order packet may be temporarily stored in the out-of-order buffer **330** and be associated with the connection from which the out-of-order packet is received. In-order packets are examined by the processing cores **310** and are allowed to pass to the protected network if no pattern of harmful virus or malicious code is detected. The processing cores **310** update and store the current pattern matching state of each connection in the database **320**. As such, any one of the processing cores **310** can continue with the on-going pattern matching from the current state of a connection that sends the current packet. In some embodiments, the database **320** includes a relational database that stores the current pattern matching states **324** with their corresponding connections **322** as shown in FIG. **2**. Details of some embodiments of the method to perform reassembly-free DPI have been discussed above.

FIG. **4** illustrates one embodiment of a system in which embodiments of the present invention may be implemented. The system **400** includes a client machine **412** within a protected network **410**, an IPS **420**, and a network **430**. The protected network **410** is communicably coupled to the network **430** via the IPS **420**. Thus, packets transmitting between the protected network **410** and the network **430** have to pass through the IPS **420**. In some embodiments, there may be more than one client machines coupled to the protected network **410**. The network **430** may include a variety of networks, such as local area network (LAN), wide area network (WAN), etc. Furthermore, the network **430** may be publicly accessible, and therefore, computer virus and malicious code targeting the protected network **410** may be sent from the network **430**. As such, the IPS **420** scans the incoming packets to prevent computer virus and malicious code from entering the protected network **410**.

In some embodiments, the IPS **420** includes a multi-core processor **421**, an out-of-order buffer **423**, and a pattern matching database **425**. The multi-core processor **421** includes a set of processing cores, such as the processing cores **310** shown in FIG. **3**.

In some embodiments, each of the processing cores receives packets from the network **430** through different connections. Furthermore, the packets may arrive out-of-order, and if so, the out-of-order packets may be temporarily stored in the out-of-order buffer **423** to be inspected later. The processing cores of the multi-core processor **421** perform DPI on the in-order packets and store the current pattern matching states of the connections in the pattern matching database **425**. If a pattern associated with computer virus or malicious code is identified in the incoming packets inspected so far, the multi-core processor **421** blocks the packet currently being inspected and may further issue a warning to a system administrator. If no pattern associated with computer virus or malicious code is identified in the incoming packets inspected so far, then the multi-core processor **421** allows the packet currently being inspected to pass to the protected network **410**, which may be further transmitted to the client machine **412**. By blocking the packet currently being inspected if the pattern is identified in the packets received so far, the computer virus or malicious code cannot be completely passed into the protected network **410**, and hence, the computer virus or malicious code cannot be completely reassembled on the client machine **412**. The incomplete computer virus or malicious code typically cannot harm the client machine **412** coupled thereto. Details of some embodiments of a method to perform reassembly-free DPI have been discussed above.

FIG. **5** illustrates a diagrammatic representation of a machine in the exemplary form of a computer system **500** within which a set of instructions, for causing the machine to perform any one or more of the methodologies discussed herein, may be executed. In alternative embodiments, the machine may be connected (e.g., networked) to other machines in a LAN, an intranet, an extranet, and/or the Internet. The machine may operate in the capacity of a server or a client machine in client-server network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The machine may be a personal computer (PC), a tablet PC, a set-top box (STB), a Personal Digital Assistant (PDA), a cellular telephone, a web appliance, a server, a network router, a switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term "machine" shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

The exemplary computer system **500** includes a processing device **502**, a main memory **504** (e.g., read-only memory (ROM), flash memory, dynamic random access memory (DRAM) such as synchronous DRAM (SDRAM) or Rambus

DRAM (RDRAM), etc.), a static memory **506** (e.g., flash memory, static random access memory (SRAM), etc.), and a data storage device **518**, which communicate with each other via a bus **532**.

Processing device **502** represents one or more general-purpose processing devices such as a microprocessor, a central processing unit, or the like. More particularly, the processing device may be complex instruction set computing (CISC) microprocessor, reduced instruction set computing (RISC) microprocessor, very long instruction word (VLIW) microprocessor, or processor implementing other instruction sets, or processors implementing a combination of instruction sets. Processing device **502** may also be one or more special-purpose processing devices such as an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), a digital signal processor (DSP), network processor, or the like. The processing device **502** is configured to execute the processing logic **526** for performing the operations and steps discussed herein.

The computer system **500** may further include a network interface device **508**. The computer system **500** also may include a video display unit **510** (e.g., a liquid crystal display (LCD) or a cathode ray tube (CRT)), an alphanumeric input device **512** (e.g., a keyboard), a cursor control device **514** (e.g., a mouse), and a signal generation device **516** (e.g., a speaker).

The data storage device **518** may include a machine-accessible storage medium **530** (also known as a machine-readable storage medium or a computer-readable medium) on which is stored one or more sets of instructions (e.g., software **522**) embodying any one or more of the methodologies or functions described herein. The software **522** may also reside, completely or at least partially, within the main memory **404** and/or within the processing device **502** during execution thereof by the computer system **500**, the main memory **504** and the processing device **502** also constituting machine-accessible storage media. The software **522** may further be transmitted or received over a network **520** via the network interface device **508**.

While the machine-accessible storage medium **530** is shown in an exemplary embodiment to be a single medium, the term "machine-accessible storage medium" should be taken to include a single medium or multiple media (e.g., a centralized or distributed database, and/or associated caches and servers) that store the one or more sets of instructions. The term "machine-accessible storage medium" shall also be taken to include any medium that is capable of storing, encoding or carrying a set of instructions for execution by the machine and that cause the machine to perform any one or more of the methodologies of the present invention. The term "machine-accessible storage medium" shall accordingly be taken to include, but not be limited to, solid-state memories, optical and magnetic media, etc. In some embodiments, machine-accessible storage medium may also be referred to as computer-readable storage medium.

Thus, some embodiments of reassembly-free DPI on multi-core hardware have been described. It is to be understood that the above description is intended to be illustrative, and not restrictive. Many other embodiments will be apparent to those of skill in the art upon reading and understanding the above description. The scope of the invention should, therefore, be determined with reference to the appended claims, along with the full scope of equivalents to which such claims are entitled.

What is claimed is:

**1**. A method comprising:

receiving a plurality of packets of one or more files at a networked device comprising a plurality of processing cores, the packets from a plurality of connections;

processing each of the received packets, wherein processing each received packet comprises:

determining from which of the plurality of connections the packet came, and

postponing processing one of the received packets based on a determination that another processing core is currently processing a packet from a same connection, and

continuing to process the one of the received packets based on a determination that no other processing core is currently processing a packet from the same connection;

storing a current state of pattern matching in a database in memory accessible to each of the plurality of processing cores, wherein the current state of pattern matching corresponds to packets received from the determined corresponding connection, and wherein a plurality of other current states of pattern matching are stored for other connections from the plurality of connections;

scanning each of the plurality of packets using one of the plurality of processing cores in the networked device without buffering the one or more files in the networked device, such that the plurality of processing cores scan the plurality of packets substantially concurrently, wherein when the plurality of packets are from one of the plurality of connections, a first processing core of the plurality of processing core receives an in-order packet and scans the in-order packet, a second processing core of the plurality of processing core receives an out-of-order packet and temporarily buffers the out-of-order packet in an out-of-order buffer without scanning the out-of-order packet, wherein the first processing core retrieves a next in order packet from the out-of-order buffer to scan after scanning the in-order packet; and

updating the current state of pattern matching based on a plurality of scan results from the plurality of processing cores, the updated current state of pattern matching stored with the determined corresponding connection.

**2**. The method of claim **1**, further comprising: resolving conflicts between out-of-order packets among the plurality of packets.

**3**. The method of claim **2**, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order or out-of order;

the first processing core scanning the packet if the first packet is in-order; and

the first processing core temporarily buffering the first packet in an out-of order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

**4**. The method of claim **3**, wherein resolving conflicts between out-of-order packets further comprises:

the second processing core of the plurality of processing cores receiving a second packet from the first connection while the first processing core is still processing the first packet; and

the second processing core re-scheduling scanning of the second packet to a later time.

5. The method of claim 1, wherein storing the current state of pattern matching further comprises storing a plurality of current states in the database, each current state associated with one of the plurality of connections.

6. An apparatus comprising:

a network interface to receive a plurality of packets of one or more files from a plurality of connections;

a plurality of processing cores to perform reassembly-free deep packet inspection on the plurality of packets without buffering the one or more files such that the plurality of processing cores scan the plurality of packets substantially concurrently, wherein each processing core processes each received packet by:

determining from which of the plurality of connections the packet came,

postponing processing one of the received packets based on a determination that another processing core is currently processing a packet from a same connection, and

continuing to process the one of the received packets based on a determination that no other processing core is currently processing a packet from the same connection, wherein when the plurality of packets are from one of the plurality of connections, a first processing core of the plurality of processing core receives an in-order packet and scans the in-order packet, a second processing core of the plurality of processing core receives an out-of-order packet and temporarily buffers the out-of-order packet in an out-of-order buffer without scanning the out-of-order packet, wherein the first processing core retrieves a next in order packet from the out-of-order buffer to scan after scanning the in-order packet; and

memory accessible to each of the plurality of processing cores, the memory associated with a database for storing a current state of pattern matching, the current state of pattern matching corresponding to packets from the determined corresponding connection, wherein a plurality of other current states of pattern matching are stored for other connections from the plurality of connections, wherein the current state of pattern matching is updated based on a plurality of scan results from the plurality of processing cores, the updated current state of pattern matching stored with the determined corresponding connection.

7. The apparatus of claim 6, wherein the plurality of processing cores resolve conflicts between out-of-order packets among the plurality of packets.

8. The apparatus of claim 6, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection and scans the packet if the first packet is in-order, and temporarily buffers the first packet in an out-of-order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

9. The apparatus of claim 6, wherein the second processing core to receive a second packet from a first connection while the first processing core is still processing the first packet, and to re-schedule scanning of the second packet to a later time.

10. The apparatus of claim 6, wherein the database further stores a plurality of current states, each current state associated with one of the plurality of connections.

11. A system comprising the apparatus of claim 6, further comprising: one or more client devices coupled to receive the plurality of packets after the plurality of packets have been scanned without identifying any prohibited content.

12. A non-transitory computer-readable medium embodying instructions that, when executed by a processor, will cause the processor to perform operations comprising:

receiving a plurality of packets of one or more files at a networked device comprising a plurality of processing cores, the packets from plurality of connections;

processing each of the received packets, wherein processing each received packet comprises:

determining from which of the plurality of connections the packet came,

postponing processing one of the received packets based on a determination that another processing core is currently processing a packet from a same connection, and

continuing to process the one of the received packets based on a determination that no other processing core is currently processing a packet from the same connection;

storing a current state of pattern matching in a database accessible to each of the plurality of processing cores, wherein the current state of pattern matching corresponds to packets from the determined corresponding connection, and wherein a plurality of other current states of pattern matching are stored for other connections from the plurality of connections;

scanning each of the plurality of packets using one of the plurality of processing cores in the networked device without buffering the one or more files in the networked device, such that the plurality of processing cores scan the plurality of packets substantially concurrently, wherein when the plurality of packets are from one of the plurality of connections, a first processing core of the plurality of processing core receives an in-order packet and scans the in-order packet, a second processing core of the plurality of processing core receives an out-of-order packet and temporarily buffers the out-of-order packet in an out-of-order buffer without scanning the out-of-order packet, wherein the first processing core retrieves a next in order packet from the out-of-order buffer to scan after scanning the in-order packet; and

updating the current state of pattern matching based on a plurality of scan results from the plurality of processing cores, the updated current state of pattern matching stored with the determined corresponding connection.

13. The non-transitory computer-readable medium of claim 12, wherein the operations further comprise: resolving conflicts between out-of-order packets among the plurality of packets.

14. The non-transitory computer-readable medium of claim 12, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order or out-of order;

the first processing core scanning the packet if the first packet is in-order; and

the first processing core temporarily buffering the first packet in an out-of order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

15. The non-transitory computer-readable medium of claim 14, wherein resolving conflicts between out-of-order packets further comprises:

the second processing core of the plurality of processing cores receiving a second packet from the first connection while the first processing core is still processing the first packet; and

the second processing core re-scheduling scanning of the second packet to a later time.

**16**. The non-transitory computer-readable medium of claim **12**, wherein storing the current state of pattern matching further comprises: storing a plurality of current states in the database, each current state associated with one of the plurality of connections.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

# CERTIFICATE OF CORRECTION



PATENT NO. : 8,813,221 B1
APPLICATION NO. : 12/238205
DATED : August 19, 2014
INVENTOR(S) : Dubrovsky et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Column 10, Lines 44-46 should read:

2. The method of claim 1, further comprising[[:]] resolving conflicts between out-of-order packets among the plurality of packets.

Column 10, Lines 47-59 should read:

3. The method of claim 2, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order; and

the first processing core scanning the packet if the first packet is in-order.

Column 11, Lines 49-56 should read:

8. The apparatus of claim 6, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection and scans the packet if the first packet is in-order.

Column 11, Lines 64-67 should read:

11. A system comprising the apparatus of claim 6, further comprising [[:]] one or more client devices coupled to receive the plurality of packets after the plurality of packets have been scanned without identifying any prohibited content.

Column 12, Lines 47-50 should read:

Signed and Sealed this
Eighteenth Day of August, 2015

Michelle K. Lee

Michelle K. Lee
*Director of the United States Patent and Trademark Office*

**CERTIFICATE OF CORRECTION (continued)** 
**U.S. Pat. No. 8,813,221 B1**

13. The non-transitory computer-readable medium of claim 12, wherein the operations further comprise [[:]] resolving conflicts between out-of-order packets among the plurality of packets.

Column 12, Lines 51-64 should read:

14. The non-transitory computer-readable medium of claim [[12]] 13, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is in-order; and

the first processing core scanning the packet if the first packet is in-order.

Column 13, Lines 7-11 should read:

16. The non-transitory computer-readable medium of claim 12, wherein storing the current state of pattern matching further comprises [[:]] storing a plurality of current states in the database, each current state associated with one of the plurality of connections.

Column 13, Lines 12-19 should read:

17. The method of claim 2, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is out-of-order; and

the first processing core temporarily buffering the first packet in an out-of-order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

Column 13, Lines 20-24 should read:

18. The apparatus of claim 6, wherein when the plurality of packets are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection and temporarily buffers the first packet in an out-of-order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

Column 13, Lines 25-32 should read:

19. The non-transitory computer-readable medium of claim 13, wherein when the plurality of packets

are from distinct ones of the plurality of connections, the first processing core of the plurality of processing cores receives a first packet from a first connection, and resolving conflicts between out-of-order packets further comprises:

the first processing core determining if the first packet is out-of order; and

the first processing core temporarily buffering the first packet in an out-of order buffer associated with the first connection without scanning the first packet if the first packet is out-of-order.

DECLARATION OF SCOTT BRADNER

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

# Appendix X

This document was also filed as ECF No. 168-49 and can be found in this Joint Appendix at JA3404.

DECLARATION OF SCOTT BRADNER

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

# Appendix Y

This document was also filed as ECF No. 168-24 and can be found in this Joint Appendix at JA2748.

DECLARATION OF SCOTT BRADNER

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

# Appendix Z

This document was also filed as ECF No. 178-5 and can be found in this Joint Appendix at JA3728.