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

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

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

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

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

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

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

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

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

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

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

NYT v DOJ, 16 CIV 7020_000367

NSA-WIKI 00237

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[redacted]

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

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

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

[redacted][4]

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

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

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

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

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

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

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

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

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

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

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

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

[redacted]

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

[redacted]

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

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

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

[redacted]

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

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

[redacted]

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

[redacted]

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

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

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

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

The second test included [redacted]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[13] [redacted]

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

NYT v DOJ, 16 CIV 7020_000377

NSA-WIKI 00247

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

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

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

c. Conclusion (U)

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

The remainder of this page intentionally left blank.

NYT v DOJ, 16 CIV 7020_000378
NSA-WIKI 00248

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

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

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

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

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

The Fourth Amendment protects the right "to be secure . . . against unreasonable searches and seizures" and directs that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. As demonstrated below, the Fourth Amendment requires no warrant here, and the upstream collection conducted by NSA is a reasonable exercise of governmental power that satisfies the Fourth Amendment. ~~(TS//SI//NF)~~

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

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

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

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

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

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

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

NYT v DOJ, 16 CIV 7020_000380
NSA-WIKI 00250

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

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

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

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

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

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

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

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against --
  (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
  (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
  (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to --
  (A) the national defense or the security of the United States; or
  (B) the conduct of the foreign affairs of the United States.

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

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

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

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

50 U.S.C. § 1801(e). (U)

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

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

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

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

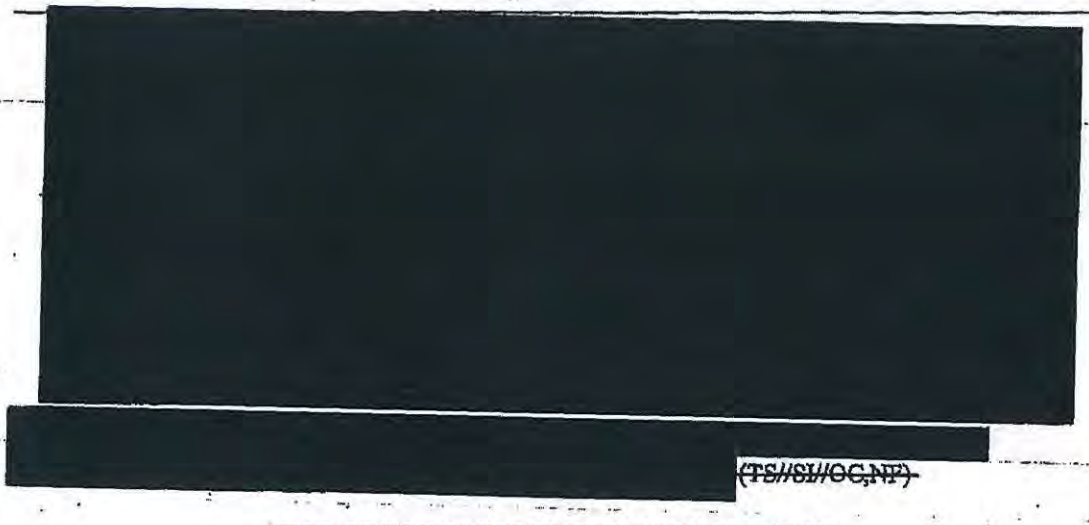
[redacted]

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

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

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

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



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

NYT v DOJ, 16 CIV 7020_000384
NSA-WIKI 00254

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

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

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

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

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

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

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

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

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

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

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

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

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

a. Acquisition (U)

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

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

b. Retention (U)

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

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

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

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

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

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

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

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

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

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

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

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

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

c. Dissemination (U)

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

[redacted]

NYT v DOJ, 16 CIV 7020_000390
NSA-WIKI 00260

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

[redacted]

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

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

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

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

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

[redacted]

[redacted]

[redacted]

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

NYT v DOJ, 16 CIV 7020_000392
NSA-WIKI 00262

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

[redacted]

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

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

[redacted]

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

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

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

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

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

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

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

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

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

NYT v DOJ, 16 CIV 7020_000394
NSA-WIKI 00264

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

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

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

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

NYT v DOJ, 16 CIV 7020_000395

NSA-WIKI 00265

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

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

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

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

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

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

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

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

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

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

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

A. Introduction (U)

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

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

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

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

B. Statutory Framework (U)

i. Section 1809 (U)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DECLARATION OF SCOTT BRADNER

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

Appendix D

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

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

OBJECTIONS AND RESPONSES BY DEFENDANTS NATIONAL SECURITY AGENCY AND ADM. MICHAEL S. ROGERS, DIRECTOR, TO PLAINTIFF'S INTERROGATORIES

Pursuant to Rule 33 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 Interrogatories, dated November 7, 2017.

GENERAL OBJECTIONS AND OBJECTIONS TO DEFINITIONS AND INSTRUCTIONS

1. The NSA Defendants object to Plaintiff's Interrogatories to the extent, as set forth in response to specific interrogatories below, that they seek information regarding the activities of the NSA, which is absolutely protected from disclosure by the statutory privilege under 50 U.S.C. § 3605(a).

2. The NSA Defendants object to Plaintiff's Interrogatories to the extent, as set forth in response to specific interrogatories 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.

3. As set forth in response to each interrogatory below, the NSA Defendants object to the definition the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

4. As set forth in response to specific interrogatories 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 interrogatories 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 interrogatories below, the NSA Defendants object to the definition of the term "Review" as compound, unduly burdensome and oppressive,

and so vague and ambiguous as to render the specific interrogatories in which it is used incapable of reasoned response.

7. As set forth in response to specific interrogatories below, the NSA Defendants object to the definition of the term "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 the specific interrogatories in which it is used incapable of reasoned response.

8. As set forth in response to specific interrogatories below, the NSA Defendants object to Plaintiff's Interrogatories 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. As set forth in response to specific interrogatories below, the NSA Defendants object to Instruction No. 3 in Plaintiff's Interrogatories to the extent that identification or description of each document or oral communication as to which privilege is claimed would itself divulge privileged information.

10. The NSA Defendants object to Plaintiff's Interrogatories to the extent that they seek information not involving the NSA's Upstream Internet acquisition techniques as authorized by Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1881a. In formulating these answers, the NSA Defendants have limited the scope of their inquiry of knowledgeable persons, as well as their searches of appropriate records, to those persons and records reasonably calculated to possess information involving the NSA's Upstream Internet acquisition techniques as authorized by Section 702 of the FISA.

11. 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.

12. Nothing contained in the following objections and responses shall be construed as a waiver of any applicable objection or privilege as to any interrogatory 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 INTERROGATORIES

INTERROGATORY NO. 1: DESCRIBE YOUR understanding of the definition of the term "international Internet link" as used by the government in its submission to the Foreign Intelligence Surveillance Court— titled "Government's Response to the Court's Briefing Order of May 9, 2011," and filed on June 1, 2011, *see* [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011)—and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 1 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants also object to Interrogatory No. 1 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 Interrogatory No. 1 on the grounds that the instruction to "provide all information supporting [their] understanding [of the definition of the

term 'international Internet link']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 1 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 1 on the ground that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 2: DESCRIBE YOUR understanding of the definition of the term "circuit" as used at pages 36 to 37 of the PCLOB Report, and provide all information supporting that understanding, including but not limited to all information furnished by DEFENDANTS to the Privacy and Civil Liberties Oversight Board concerning this term.

OBJECTION: The NSA Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 2 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants also object to Interrogatory No. 2 on the grounds that the instruction to "provide all information supporting [their] understanding [of the definition of the term 'circuit']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

The NSA Defendants further object to this interrogatory on the ground that 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.

Finally, to the extent that Interrogatory No. 2 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 2 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the 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.

As of the time of this response the NSA Defendants are unaware of any information furnished by Defendants to the PCLOB regarding the meaning of the term "circuit" that would differ from the understanding set forth above.

INTERROGATORY NO. 3: DESCRIBE YOUR understanding of the definition of the term "filtering mechanism" as used at pages 10 and 47–48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 3 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 3 on the grounds that the instruction to "provide all information supporting [their] understanding [of the definition of the term 'filtering mechanism']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 3 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 3 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the 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.

INTERROGATORY NO. 4: DESCRIBE YOUR understanding of the definition of the term "scanned" as used at page 10 of the Memorandum in Support of Defendants' Motion to Dismiss the First Amended Complaint, *Wikimedia Foundation v. NSA*, No. 15-cv-662-TSE (D. Md. Aug. 6, 2015), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 4 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 4 on the grounds that the instruction to "provide all information supporting [their] understanding [of the definition of the term 'scanned']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 4 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 4 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term "scanned," as used in the above-referenced brief when filed, meant, in unclassified terms, the use of a screening device in the Upstream Internet collection process to acquire only Internet transactions containing at least one tasked selector. Today the term "scanned" would mean, in unclassified terms, the use of a screening device in the Upstream Internet collection process designed to identify for acquisition Internet transactions to or from persons targeted in accordance with the current NSA targeting procedures.

INTERROGATORY NO. 5: DESCRIBE YOUR understanding of the definition of the term "screen" as used at page 48 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 5 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 5 on the grounds that its instruction to "provide all information supporting [their] understanding [of the definition of the term 'screen']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 5 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 5 on the grounds that it seeks information 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

object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term "screen," as used in the above-referenced brief when filed, meant, in unclassified terms, the use of a screening device in the Upstream Internet collection process to acquire only Internet transactions containing at least one tasked selector. Today, the term "screened" would mean, in unclassified terms, the use of a screening device in the Upstream Internet collection process designed to identify for acquisition Internet transactions to or from persons targeted in accordance with the current NSA targeting procedures.

INTERROGATORY NO. 6: DESCRIBE YOUR understanding of the definition of the term "discrete communication" as used in the 2014 NSA Minimization Procedures, and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to Interrogatory No. 6 on the grounds that 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. The NSA Defendants also object to the definition the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 6 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 6 on the grounds that the instruction to "provide all information supporting [their] understanding [of the definition of the

term 'discrete communication']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 6 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 6 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, in the context of the 2014 NSA Section 702 Minimization Procedures, the term "discrete communication" means a single communication.

INTERROGATORY NO. 7: DESCRIBE YOUR understanding of all features that a series of INTERNET PACKETS comprising an "Internet transaction" has in common, as the term "Internet transaction" is used in at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding. For example, the INTERNET PACKETS comprising an "Internet transaction" might share source and destination IP addresses, source and destination ports, and protocol type (albeit with the source and destination IP addresses and ports reversed for packets flowing in the opposite direction).

OBJECTION: NSA Defendants object to the definition the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 7 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 7 on the grounds that its instruction to "provide all information supporting [their] understanding [of the 'features that a

series of Internet packets comprising an "Internet transaction" has in common']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, the NSA Defendants object to Interrogatory No. 7 on the ground that it seeks classified information about alleged NSA intelligence activities 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 8: DESCRIBE YOUR understanding of the definitions of the terms "single communication transaction" and "multi-communication transaction" as used by the government in its submission to the Foreign Intelligence Surveillance Court, filed on August 16, 2011, and provide all information supporting that understanding. *See* [*Redacted*], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011).

OBJECTION: The NSA Defendants object to Interrogatory No. 8 on the grounds that 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. The NSA Defendants also object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 8 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants also object to Interrogatory No. 8 as vague and ambiguous insofar as it attributes the phrase "single communication transaction" 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 *9 (FISC Oct. 3, 2011).

The NSA Defendants further object to Interrogatory No. 8 on the grounds that its instruction to "provide all information supporting [their] understanding [of the terms 'single communication transaction' and 'multi-communication transaction']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 8 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 8 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the 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-communication transaction" meant, in unclassified terms, an Internet transaction that contained multiple discrete communications.

INTERROGATORY NO. 9: DESCRIBE YOUR understanding of the definitions of the terms "access" and "larger body of international communications" as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 9 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 9 on the grounds that its instruction to "provide all information supporting [their] understanding [of the terms 'access' and 'larger body of international communications']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 9 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 9 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding (i) the term "larger body of international communications," as used in the above-referenced brief when filed, meant, in unclassified terms, the body of at least one-end-foreign Internet transactions transiting the Internet backbone networks of electronic communications service providers that were screened during the

Upstream Internet collection process for the purpose of identifying those containing at least one tasked selector; and (ii) the term "access," as used in the same brief when filed, referred in unclassified terms to the means making it possible to screen this "larger body of international communications" for those that contained at least one tasked selector. As noted above in response to Interrogatory Nos. 3-5, today Internet transactions are screened during the Upstream Internet collection process to identify for acquisition those transactions that are to or from persons targeted in accordance with the current NSA targeting procedures.

INTERROGATORY NO. 10: DESCRIBE YOUR understanding of the definition of the term "acquired" as used at page 10 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 10 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 10 on the grounds that its instruction to "provide all information supporting [their] understanding [of the term 'acquired']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 10 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 10 on the grounds that it seeks information 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 object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify

and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term "acquired," as used in the above-referenced brief in relation to Internet transactions, meant when filed (and still means today), in unclassified terms, ingested into Government databases after the Internet transactions have passed through the filtering and scanning processes conducted during Upstream Internet collection.

INTERROGATORY NO. 11: DESCRIBE YOUR understanding of the definition of the term "collection" as used at page 10 n.3 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 11 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 11 on the grounds that its instruction to "provide all information supporting [their] understanding [of the term 'collection']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 11 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 11 on the grounds that it seeks information 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

object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the NSA Defendants respond that to their understanding the term "collection," as used in the above-referenced brief in relation to communications, meant when filed (and still means today), in unclassified terms, ingestion into Government databases after Internet transactions have passed through the filtering and scanning processes conducted during Upstream Internet collection.

INTERROGATORY NO. 12: DESCRIBE YOUR understanding of the definition of the term "Internet 'backbone'" as used at page 1 of the Brief for Defendants–Appellees, *Wikimedia Foundation v. NSA*, No. 15-2560 (4th Cir. April 11, 2016), and provide all information supporting that understanding.

OBJECTION: The NSA Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 12 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

The NSA Defendants further object to Interrogatory No. 12 on the grounds that its instruction to "provide all information supporting [their] understanding [of the term 'Internet 'backbone']" is unduly burdensome and oppressive, and in the context of this interrogatory so vague and ambiguous as to be incapable of reasoned response.

Finally, to the extent that Interrogatory No. 12 seeks classified information about alleged NSA intelligence activities, the NSA Defendants object to Interrogatory No. 12 on the grounds that it seeks information 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

object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

RESPONSE: Subject to the objections stated above, and without waiving them, the 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.

INTERROGATORY NO. 13: DESCRIBE in detail all steps taken by the NSA to PROCESS communications in the course of Upstream surveillance.

OBJECTION: The NSA Defendants object to Interrogatory No. 13 on the grounds that 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. The NSA Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 13 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous.

Finally, the NSA Defendants object to Interrogatory No. 13 on the ground that it seeks information about alleged NSA intelligence activities that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(!0 and 50 U.S.C. § 3605(a). The NSA Defendants object to any instruction or purported requirement, *see* Fed. R.

Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

INTERROGATORY NO. 14: DESCRIBE the entire process by which, pursuant to Upstream surveillance, the contents of INTERNET COMMUNICATIONS are INTERACTED WITH.

OBJECTION: The NSA Defendants object to the definition of the term "Describe" to the extent it calls for "identification of all persons, communications, acts, transactions, events, agreements, recommendations, and Documents used, necessary, or desirable to support [the NSA Defendants' narrative statement]" in response to Interrogatory No. 14 on the grounds that it is unduly burdensome and oppressive, and vague and ambiguous. The NSA Defendants also 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 this interrogatory incapable of reasoned response.

The NSA Defendants further object to Interrogatory No. 14 to the extent grounds that 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.

Finally, the NSA Defendants object to Interrogatory No. 14 on the ground that it seeks information about alleged NSA intelligence activities that is protected from disclosure by the state secrets privilege and the statutory privileges under 50 U.S.C. § 3024(i)(!0 and 50 U.S.C. § 3605(a). The NSA Defendants object to any instruction or purported requirement, *see* Fed. R. Civ. P. 26(b)(5)(A), to identify and/or describe information withheld on this basis as unduly burdensome and oppressive and itself calling for information protected by these privileges.

Dated: December 22, 2017

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
CAROLINE J. ANDERSON
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

Pursuant to 28 U.S.C. § 1746, I, Jason D. Padgett, declare under penalty of perjury that the foregoing answers to Plaintiff Wikimedia's Interrogatories are true and correct to the best of my knowledge and belief, based on my personal knowledge and information made available to me in the course of my duties and responsibilities as an Attorney in the Office of General Counsel, National Security Agency.

Executed this 22nd day of December, 2017

Jason D. Padgett
Attorney
Office of General Counsel
National Security Agency

DECLARATION OF SCOTT BRADNER

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

Appendix E

Filed
United States Foreign
Intelligence Surveillance Court

APR 26 2017

LeeAnn Flynn Hall, Clerk of Court

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

[redacted]

MEMORANDUM OPINION AND ORDER

These matters are before the Foreign Intelligence Surveillance Court ("FISC" or "Court") on the "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," which was filed on September 26, 2016 ("September 26, 2016 Submission"), and the "Government's Ex Parte Submission of Amendments to DNI/AG 702(g) Certifications and Ex Parte Submission of Amended Targeting and Minimization Procedures," which was filed on March 30, 2017 ("March 30, 2017 Submission"). (Collectively, the September 26, 2016 and March 30, 2017 Submissions will be

referred to herein as the "2016 Certification Submissions.") For the reasons explained below, the government's request for approval of the certifications and procedures accompanying the September 26, 2016 Submission, as amended by the March 30, 2017 Submission, is granted, subject to certain reporting requirements. The Court's approval of the amended certifications and accompanying targeting and minimization procedures is set out in separate orders, which are being entered contemporaneously herewith.

I. BACKGROUND

A. The Initial 2016 Certifications

The September 26, 2016 Submission included [redacted] certifications that were executed by the Attorney General ("AG") and the Director of National Intelligence ("DNI") pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA" or "the Act"), which is codified at 50 U.S.C. § 1881a [redacted] Each of the [redacted] certifications submitted in September (collectively referred to as "the Initial 2016 Certifications") was accompanied by the supporting affidavits of the Director of the National Security Agency ("NSA"), the Director of the Federal Bureau of Investigation ("FBI"), the Director of the Central Intelligence Agency ("CIA"), and the Director of the National Counterterrorism Center ("NCTC"); two sets of targeting procedures, for use by the NSA and FBI respectively;[1] and four sets of minimization procedures, for use by the

[1] The targeting procedures for each of the Initial 2016 Certifications are identical. The (continued...)

NSA, FBI, CIA, and NCTC respectively.[2] The September 26, 2016 Submission also included an explanatory memorandum prepared by the Department of Justice ("DOJ") ("September 26, 2016 Memorandum").

The Court was required to complete its review of the Initial 2016 Certifications within 30 days of their submission, i.e., by October 26, 2016. See 50 U.S.C. § 1881a(i)(1)(B). The Court may extend this period, however, "as necessary for good cause in a manner consistent with national security." See 50 U.S.C. § 1881a(j)(2). The Court has issued two such extensions in these matters.

---

[1](...continued)
targeting procedures for the NSA ("NSA Targeting Procedures") appear as Exhibit A to each of the 2016 Certifications and the March 30, 2017 Submission includes identical amendments to those procedures for each of the certifications. (Unless otherwise specified, references to those targeting procedures shall refer to the procedures as amended, as discussed below, in the March 30, 2017 Submission.) The targeting procedures for the FBI ("FBI Targeting Procedures") appear as Exhibit C to each of the 2016 Certifications and are not amended by the March 30, 2017 Submission.

[2] The minimization procedures for each of the Initial 2016 Certifications are identical. The minimization procedures for the NSA ("NSA Minimization Procedures") appear as Exhibit B to each of the 2016 Certifications and the March 30, 2017 Submission includes identical amendments to those procedures for each of the certifications. (Unless otherwise specified, references to those minimization procedures shall refer to the procedures as amended, as discussed below, in the March 30, 2017 Submission.) The minimization procedures for the FBI ("FBI Minimization Procedures") appear as Exhibit D to each of the 2016 Certifications. The minimization procedures for the CIA ("CIA Minimization Procedures") appear as Exhibit E to each of the 2016 Certifications. The minimization procedures for the NCTC ("NCTC Minimization Procedures") appear as Exhibit G to each of the 2016 Certifications. The minimization procedures for the FBI, CIA, and NCTC are not amended by the March 30, 2017 Submission.

On October 24, 2016, the government orally apprised the Court of significant non-compliance with the NSA's minimization procedures involving queries of data acquired under Section 702 using U.S. person identifiers. The full scope of non-compliant querying practices had not been previously disclosed to the Court. Two days later, on the day the Court otherwise would have had to complete its review of the certifications and procedures, the government made a written submission regarding those compliance problems, see October 26, 2016, Preliminary and Supplemental Notice of Compliance Incidents Regarding the Querying of Section 702-Acquired Data ("October 26, 2016 Notice"), and the Court held a hearing to address them. The government reported that it was working to ascertain the cause(s) of those compliance problems and develop a remedial plan to address them. Without further information about the compliance problems and the government's remedial efforts, the Court was not in a position to assess whether the minimization procedures accompanying the Initial 2016 Certifications, as they would be implemented, would comply with statutory standards and were consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A)-(B). Accordingly, the Court found good cause to extend the time limit for its review of the Initial 2016 Certifications through January 31, 2017, and, based on the government's representations, found that such extension was consistent with national security.[3] See Docket Nos [redacted] Order entered on Oct. 26, 2016 ("October 26, 2016 Order").

[3] By operation of the statute, the predecessors to each of the Initial 2016 Certifications and the procedures accompanying them remained in effect during the extended periods for the Court's consideration of the 2016 Certifications. See 50 U.S.C. § 1881a(i)(3)(A)-(B).

On January 3, 2017, the government made a further submission describing its efforts to ascertain the scope and causes of those compliance problems and discussing potential solutions to them. See January 3, 2017, Supplemental Notice of Compliance Incidents Regarding the Querying of Section 702-Acquired Data ("January 3, 2017 Notice"). The Court was not satisfied that the government had sufficiently ascertained the scope of the compliance problems or developed and implemented adequate solutions for them and communicated a number of questions and concerns to the government. The government submitted another update on January 27, 2017, in which it informed the Court that, due to the complexity of the issues involved, NSA would not be in a position to provide thorough responses to the Court's questions and concerns by January 31, 2017. See January 27, 2017, Letter In re: DNI/AG 702(g) Certifications [redacted] and their Predecessor Certifications ("January 27, 2017 Letter"). The government submitted that a further extension, through May 26, 2017, was necessary for it to address those issues and that such extension would be consistent with national security. The Court granted a shorter extension, through April 28, 2017, for reasons stated in its order approving the extension. See Docket Nos. [redacted] Order entered on Jan. 27, 2017 ("January 27, 2017 Order").

B. The 2017 Amendments

On March 30, 2017, the Attorney General and Director of National Intelligence, acting pursuant to 50 U.S.C. § 1881a(i)(1)(C), executed Amendments to each of the [redacted] Initial 2016 Certifications. See Amendment to [redacted]

[redacted] (collectively, the "2017 Amendments").[4] As discussed below, those amendments substantially change how NSA will conduct certain aspects of Section 702 collection, and largely resolve the compliance problems mentioned above. The March 30, 2017 Submission included the 2017 Amendments, a revised supporting affidavit by the Director of NSA, and revised targeting and minimization procedures for NSA, which replace Exhibits A and B, respectively, to each of the Initial 2016 Certifications. That submission also included an explanatory memorandum prepared by DOJ ("March 30, 2017 Memorandum").

C. Subject Matter of the Certifications

Each of the 2016 Certifications involves "the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information." [redacted]

[4] Unless otherwise stated, subsequent references to the "2016 Certifications" are to the Initial 2016 Certifications and accompanying procedures, as later amended by the 2017 Amendments and the accompanying revised procedures.

[redacted]

Each of the 2016 Certifications generally proposes to continue acquisitions of foreign intelligence information that are now being conducted under the corresponding certification made in 2015 ("the 2015 Certifications"). See September 26, 2016 Memorandum at 2. The 2015 Certifications, which are similarly differentiated by subject matter and [redacted] were approved by the FISC on November 6, 2015.[5] The 2015 Certifications, in turn, generally renewed authorizations to acquire foreign intelligence information under a series of certifications made by the AG and DNI pursuant to Section 702 that dates back to 2008.[6] The government also seeks approval of amendments to the certifications in the Prior 702 Dockets, such that the NSA, CIA, FBI and NCTC henceforward will apply the same minimization

[5] See Docket Nos. [redacted] Memorandum Opinion and Order entered on Nov. 6, 2015 ("November 6, 2015 Opinion"). The Court issued an order on November 9, 2015, approving amendments to prior Section 702 certifications and authorizing the use of revised minimization procedures in connection with those certifications.

[6] See Docket Nos. [redacted] These dockets, together with Docket Numbers [redacted] are collectively referred to as "the Prior 702 Dockets."

procedures to information obtained under prior certifications as they will to information to be obtained under the 2016 Certifications. See September 26, 2016 Memorandum at 2-3; [redacted] This practice, long approved by the FISC, has the advantage of applying a single set of updated procedures to Section 702-acquired information rather than requiring personnel to follow different rules for information acquired on different dates.

D. Review of Compliance Issues

The Court's review of targeting and minimization procedures under Section 702 is not confined to the procedures as written; rather, the Court also examines how the procedures have been and will be implemented. See, e.g., Docket No. [redacted], Memorandum Opinion entered on Apr. 7, 2009, at 22-24 ("April 7, 2009 Opinion"); Docket Nos. [redacted] Memorandum Opinion entered on Aug. 30, 2013, at 6-11 ("August 30, 2013 Opinion"). Accordingly, for purposes of its review of the 2016 Certifications, the Court has examined quarterly compliance reports submitted by the government since the most recent FISC review of Section 702 certifications and procedures was completed on November 6, 2015,[7] as well as individual notices of non-compliance relating to implementation of Section 702. The Court held a hearing on October 4, 2016, to address certain issues raised by the September 26,

[7] See Quarterly Reports to the FISC Concerning Compliance Matters Under Section 702 of FISA, submitted on December 18, 2015, March 18, 2016, June 17, 2016, September 16, 2016, December 16, 2016 and March 17, 2017. These reports are cited herein in the form "[Date] Compliance Report."

2016 Submission, as well as certain compliance issues regarding the government's collection and handling of information under prior certifications ("October 4, 2016 Hearing").[8] The Court held a further hearing on October 26, 2016, to address matters raised in the October 26, 2016 Notice ("October 26, 2016 Hearing").[9]

II. REVIEW OF CERTIFICATIONS [redacted] AND OF THEIR PREDECESSOR CERTIFICATIONS AS AMENDED BY THE SEPTEMBER 26, 2016 AND MARCH 30, 2017 SUBMISSIONS

The Court must review a certification submitted pursuant to Section 702 "to determine whether [it] contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). The Court's examination of Certifications [redacted] as amended by the 2017 Amendments, confirms that:

(1) the certifications have been made under oath by the AG and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), see [redacted]

(2) the certifications contain each of the attestations required by 50 U.S.C. § 1881a(g)(2)(A), see [redacted]

(3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures and minimization procedures;

---

[8] See generally Transcript of Proceedings Held Before the Honorable Rosemary M. Collyer on October 4, 2016 ("October 4, 2016 Transcript").

[9] See generally Transcript of Proceedings Held Before the Honorable Rosemary M. Collyer on October 26, 2016 ("October 26, 2016 Transcript").

(4) each of the certifications is supported by the affidavits of appropriate national security officials, as described in 50 U.S.C. § 1881a(g)(2)(C);[10] and

(5) each of the certifications includes an effective date for the authorization in compliance with 50 U.S.C. § 1881a(g)(2)(D) – specifically, the certifications become effective on April 28, 2017, or on the date upon which this Court issues an order concerning the certifications under Section 1881a(i)(3), whichever is sooner, see [redacted].[11]

The Court therefore finds that [redacted] contain all the required statutory elements. See 50 U.S.C. § 1881a(i)(2)(A).

Similarly, the Court has reviewed the certifications in the Prior 702 Dockets, as amended by the 2016 Certifications, and finds that they also contain all the elements required by the statute. Id.[12]

---

[10] See Affidavits of Admiral Michael S. Rogers, United States Navy, Director, NSA; Affidavits of James B. Comey, Director, FBI; Affidavits of John O. Brennan, Director, CIA; and Affidavits of Nicholas Rasmussen, Director, NCTC, which are appended to each of Certifications [redacted]. Admiral Rogers filed amended affidavits in connection with the March 30, 2017 Submission.

[11] The statement described in 50 U.S.C. § 1881a(g)(2)(E) is not required in this case because there has been no "exigent circumstances" determination under Section 1881a(c)(2).

[12] The effective dates for the amendments to the certifications in the Prior 702 Dockets are the same as the effective dates for the 2016 Certifications. See [redacted]

III. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is also required, pursuant to 50 U.S.C. § 1881a(i)(2)(B) and (C), to review the targeting and minimization procedures to determine whether they are consistent with the requirements of 50 U.S.C. § 1881a(d)(1) and (e)(1). Pursuant to 50 U.S.C. § 1881a(i)(3)(A), the Court further assesses whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

A. Statutory Standards for Targeting Procedures

Section 1881a(d)(1) requires targeting procedures that are "reasonably designed" to "ensure that any acquisition authorized under [the certification] 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." In addition to these statutory requirements, the government uses the targeting procedures as a means of complying with Section 1881a(b)(3), which provides that acquisitions "may not intentionally target a United States person reasonably believed to be located outside the United States." The FISC considers steps taken pursuant to these procedures to avoid targeting United States persons as relevant to its assessment of whether the procedures are consistent with the requirements of the Fourth Amendment. See Docket No. 702(i)-08-01, Memorandum Opinion entered on Sept. 4, 2008, at 14 ("September 4, 2008 Opinion").

Under the procedures adopted by the government, NSA is the lead agency in making targeting decisions under Section 702. Pursuant to its targeting procedures, NSA may target for

acquisition a particular "selector," which is typically a facility such as a telephone number or e-mail address. The FBI Targeting Procedures come into play in cases where [redacted] that has been tasked under the NSA Targeting Procedures. See FBI Targeting Procedures § I.1. "Thus, the FBI Targeting Procedures apply in addition to the NSA Targeting Procedures, whenever [redacted] acquired." September 4, 2008 Opinion at 20 (emphasis in original). Proposed changes to the existing NSA and FBI targeting procedures are discussed below.

B. Statutory Standards for Minimization Procedures

Section 1881a(e)(1), in turn, requires minimization procedures that "meet the definition of minimization procedures under [50 U.S.C. §] 1801(h) or 1821(4)]." Sections 1801(h) and 1821(4) define "minimization procedures" in pertinent part as:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance [or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;[13]

---

[13] Section 1801(e) defines "foreign intelligence information" as

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> >
> > (B) sabotage, international terrorism, or the international proliferation of

(continued...)

> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in [50 U.S.C. § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes[.]

50 U.S.C. § 1801(h); see also id. § 1821(4).[14] Each agency having access to "raw," or unminimized,[15] information obtained under Section 702 is governed by its own set of

---

[13](...continued)

> weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or a foreign territory that relates to, and if concerning a United States person is necessary to –
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

[14] The definitions of "minimization procedures" set forth in these provisions are substantively identical (although Section 1821(4)(A) refers to "the purposes . . . of the particular physical search"). For ease of reference, subsequent citations refer only to the definition set forth at Section 1801(h).

[15] This opinion uses the terms "raw" and "unminimized" interchangeably. The proposed NCTC Minimization Procedures define "raw" information as "section 702-acquired information that (i) is in the same or substantially the same format as when NSA or FBI acquired it, or (ii) has been processed only as necessary to render it into a form in which it can be evaluated to

(continued...)

minimization procedures in its handling of Section 702 information. Under Section 1881a(i)(2)(C), the Court must determine whether the agencies' respective minimization procedures meet the statutory definition of minimization procedures set forth at 50 U.S.C. §§ 1801(h) or 1821(4), as appropriate.

The most significant changes to the procedures proposed by the government in connection with the 2016 Certifications relate to: (i) the changes in the scope of NSA collection under Section 702, as reflected in the March 30, 2017 Amendments; and (ii) the government's proposal in the September 26, 2016 Submission to allow NCTC access to unminimized information acquired by NSA and FBI [redacted] relating to international terrorism [redacted]. Because those changes cut across several sets of procedures, each is discussed individually in a separate section. This opinion then examines several other changes to various sets of procedures proposed by the government in the September 26, 2016 Submission. The opinion then will assess whether, taken as a whole and including the proposed changes, the proposed targeting and minimization procedures satisfy applicable statutory and Fourth Amendment requirements.

C. Significant Changes to NSA Targeting and Minimization Procedures in the March 30, 2017 Submission

The October 26, 2016 Notice disclosed that an NSA Inspector General (IG) review and report and NSA Office of Compliance for Operations (OCO) verification activities indicated that,

---

[15](...continued)
determine whether it reasonably appears to be foreign intelligence information or to be necessary to understand foreign intelligence information or assess its importance." NCTC Minimization Procedures § A.3.d.

with greater frequency than previously disclosed to the Court, NSA analysts had used U.S.-person identifiers to query the results of Internet "upstream" collection, even though NSA's Section 702 minimization procedures prohibited such queries. To understand why such queries were prohibited, and why this disclosure gave the Court substantial concern, some historical background is necessary.

1. Upstream Collection and the Acquisition of MCTs

"Upstream" collection of Internet communications refers to NSA's interception of such communications as they transit the facilities of an Internet backbone carrier [redacted] as distinguished from acquiring communications from systems operated by Internet service providers [redacted].[16] Upstream Internet collection constitutes a small percentage of NSA's overall collection of Internet communications under Section 702, see, e.g., October 3, 2011 Memorandum Opinion at 23 n.21 (noting that, at that time, upstream Internet collection constituted only 9% of NSA's Internet collection), but it has represented more than its share of the challenges in implementing Section 702.

In 2011, the government disclosed that, as part of its upstream collection of Internet transactions, NSA acquired certain "Multiple Communication Transactions" or "MCTs."[17]

---

[16] See In re DNI/AG 702(g) Certifications [redacted] Memorandum Opinion, October 3, 2011 ("October 3, 2011 Memorandum Opinion"), at 5 n.3. For purposes of the discussion that follows, familiarity with that opinion is presumed. As discussed below, NSA does not share raw upstream collection (Internet or telephony) with any other agency.

[17] NSA's procedures define an Internet transaction as consisting of either a discrete communication (e.g., an individual e-mail) or multiple discrete communications obtained within (continued...)

MCTs might take the form of [redacted] containing multiple e-mail messages [redacted]. See March 30, 2017 Memorandum at 8 n.8. The term "active user" refers to the user of a communication service to or from whom the MCT is in transit when it is acquired (e.g., the user of an e-mail account [redacted] Eventually, as discussed below, a complicated set of minimization rules was adopted for handling different types of MCTs, based on whether the active user was the target[18] and, if not, the nationality and location (to the extent known) of the active user.

Moreover, NSA upstream collection acquired Internet communications that were to, from ***or about*** (i.e., containing a reference to) a selector tasked for acquisition under Section 702. As a result, upstream collection could acquire an entire MCT for which the active user was a non-target and that mostly pertained to non-targets, merely because a ***single*** discrete communication within the MCT was to, from ***or contained a reference to*** a tasked selector. Such acquisitions could take place even if the non-target active user was a U.S. person in the United States and the MCT contained a large number of domestic communications[19] that did not pertain to the foreign

---

[17](...continued)
an MCT. See NSA Targeting Procedures § I, at 2 n.1; NSA Minimization Procedures § 2(g).

[18] With a narrow exception for [redacted] all users of a selector tasked for acquisition under Section 702 are considered targets. See March 30, 2017 Memorandum at 6 n.7.

[19] In this opinion, "domestic communications" are communications in which the sender (continued...)

intelligence target who used the tasked selector. Because of those types of acquisitions particularly, upstream Internet collection was "more likely than other forms of Section 702 collection to contain information of or concerning United States persons with no foreign intelligence value." November 6, 2015 Opinion at 25 n.21.

It should be noted, however, that not all MCTs in which the active user is a non-target are equally problematic; for example, some MCTs within that description may involve an active user who is a non-U.S. person outside the United States, and for that reason are less likely to contain a large volume of information about U.S. persons or domestic communications.

2. The 2011 Finding of Deficiency and Measures to Remedy the Deficiency

In its October 3, 2011 Memorandum Opinion, the Court found the NSA's minimization procedures, proffered in connection with Section 702 certifications then under consideration, statutorily and constitutionally deficient with respect to their protection of U.S. person information within certain types of MCTs. See October 3, 2011 Memorandum Opinion at 49-80. In response to the Court's deficiency finding, the government submitted amended minimization procedures that placed significant new restrictions on NSA's retention, use, and dissemination of MCTs. Those procedures included a sequestration regime for more problematic categories of MCTs.[20] A shorter retention period was also put into place, whereby an MCT of any type could not be retained longer than two years after the expiration of the certification pursuant to which it

---

[19](...continued)
and all intended recipients are in the United States.

[20] This sequestration regime is discussed in Section IV below in connection with an instance of NSA's not complying with that regime.

was acquired, unless applicable retention criteria were met. And, of greatest relevance to the present discussion, those procedures categorically prohibited NSA analysts from using known U.S.-person identifiers to query the results of upstream Internet collection. In substantial reliance on these and other changes, the Court approved the modified procedures for acquiring and handling MCTs. See In re DNI/AG 702(g) Certifications [redacted] Memorandum Opinion, November 30, 2011 ("November 30, 2011 Memorandum Opinion").

The Court also observed that one category of MCTs presented far fewer statutory and constitutional difficulties than the others:

> [I]f the target is the active user, then it is reasonable to presume that all of the discrete communications within an MCT will be to or from the target. Although United States persons and persons in the United States may be party to any of those communications, NSA' s acquisition of such communications is of less concern than the communications described in the [other] categories [of MCTs] because the communicants were in direct communication with a tasked facility, and the acquisition presumptively serves the foreign intelligence purpose of the collection.

October 3, 2011 Memorandum Opinion at 38. See also id. at 58 n.54 ("The government has also suggested that NSA may have limited capability, at the time of acquisition, to identify some MCTs as to which the "active user" is a tasked selector. To the extent that NSA is able to do so, such acquisitions ***would be consistent with FISA and the Fourth Amendment*** because all discrete communications within this class of MCTs would consist of communications to or from a tasked selector.") (internal citation omitted, emphasis added); id. at 80 (finding that the

proposed NSA procedures, although deficient as applied to other forms of MCTs, were consistent with the statute and the Fourth Amendment as applied to "MCTs as to which the 'active user' is known to be a tasked selector"). That point is significant to the current matters: as discussed below, the 2016 Certifications only authorize acquisition of MCTs when the active user is the target of acquisition.

3. The October 26, 2016 Notice and Hearing

Since 2011, NSA's minimization procedures have prohibited use of U.S.-person identifiers to query the results of upstream Internet collection under Section 702. The October 26, 2016 Notice informed the Court that NSA analysts had been conducting such queries in violation of that prohibition, with much greater frequency than had previously been disclosed to the Court. The Notice described the results of an NSA IG Report which analyzed queries using a set of known U.S.-person identifiers (those associated with targets under Sections 704 and 705(b) of the Act, 50 U.S.C. §§ 1881c and 1881d(b)), during the first three months of 2015, in a subset of particular NSA systems that contain the results of Internet upstream collection. That relatively narrow inquiry found that [redacted] analysts had made [redacted] separate queries using [redacted] U.S.-person identifiers that improperly ran against upstream Internet data. The government reported that the NSA IG and OCO were conducting other reviews covering different time periods, with preliminary results suggesting that the problem was widespread during all periods under review.

At the October 26, 2016 hearing, the Court ascribed the government's failure to disclose those IG and OCO reviews at the October 4, 2016 hearing to an institutional "lack of candor" on NSA's part and emphasized that "this is a very serious Fourth Amendment issue." October 26,

2016 Transcript at 5-6. The Court found that, in light of the recent revelations, it did not have sufficient information to assess whether the proposed minimization procedures accompanying the Initial 2016 Certifications would comply with statutory and Fourth Amendment requirements, as implemented. Based on the government's representation that an extension of time through January 31, 2017, would provide the government sufficient opportunity to assess and report on the scope of the problem and an appropriate remedial plan, and was consistent with the national security, the Court extended the time period for its consideration of the 2016 Certifications to that date.

4. The January 3, 2017 Supplemental Notice and January 27, 2017 Letter

In anticipation of the January 31 deadline, the government updated the Court on these querying issues in the January 3, 2017 Notice. That Notice indicated that the IG's follow-on study (covering the first quarter of 2016) was still ongoing. A separate OCO review, limited in many of the same ways as the IG studies, and covering the periods of April through December 2015 and April through July of 2016, found that some [redacted] improper queries were conducted by [redacted] analysts during those periods.[21] The January 3, 2017 Notice stated that "human error was the primary factor" in these incidents, but also suggested that system design issues contributed. For

[21] NSA further reported that OCO reviewed queries involving a number of identifiers for known U.S. persons who were not targets under Sections 704 or 705(b) of the Act, and which were associated with "certain terrorism-related events that had occurred in the United States." January 3, 2017 Notice at 6. NSA OCO found [redacted] such queries, [redacted] of which improperly ran against Section 702 upstream Internet data. [redacted] of the improper queries were run in a system called [redacted] which NSA analysts use to [redacted] of a current or prospective target of NSA collection, including under Section 702. Id. at 6-7.

example, some systems that are used to query multiple datasets simultaneously required analysts to "opt-out" of querying Section 702 upstream Internet data rather than requiring an affirmative "opt-in," which, in the Court's view, would have been more conducive to compliance. See January 3, 2017 Notice at 5-6. It also appeared that NSA had not yet fully assessed the scope of the problem: the IG and OCO reviews "did not include systems through which queries are conducted of upstream data but that do not interface with NSA's query audit system." Id. at 3 n.6. Although NSD and ODNI undertook to work with NSA to identify other tools and systems in which NSA analysts were able to query upstream data, id., and the government proposed training and technical measures, it was clear to the Court that the issue was not yet fully scoped out.

On January 27, 2017, the government provided further information on the technical and training measures NSA was taking and proposed to take to address this issue. NSA was implementing its technical measures only on systems with respect to the system thought to be used most frequently to query Section 702 data. The government still had not ascertained the full range of systems that might have been used to conduct improper U.S.-person queries. See, e.g., January 27, 2017 Letter at 5 ("NSA is progressing with its efforts to identify other tools or systems that analysts are using to query upstream data."). The government also reported that the NSA IG study for the first quarter of 2016 had found [redacted] improper queries, a substantial

improvement over the first quarter of 2015.[22] But NSA was still working to determine the scope of its U.S.-person query problem and to identify all relevant storage systems and querying tools.

The January 27, 2017 Letter concluded that, "[b]ased on the complexity of the issues, NSA will not be in a position to provide thorough responses [to the Court's questions] on or before January 31, 2017." January 27, 2017 Letter. The government represented that a further extension of the Court's time to consider the 2016 Certifications through May 26, 2017, would be consistent with the national security and would allow the government time to investigate and remedy the problem.

The Court granted an extension only through April 28, 2017.[23] January 27, 2017 Order at 6. In doing so, the Court noted its concern about the extent of non-compliance with "important safeguards for interests protected by the Fourth Amendment." Id. at 5. The Court also observed that, while recent remedial measures appeared promising, they were being implemented only on certain systems, while other systems remained to be assessed. Id. at 5-6.

On March 17, 2017, the government reported that NSA was still attempting to identify all systems that store upstream data and all tools used to query such data, though that effort was nearly complete. March 17, 2017 Compliance Report at 100. NSA had also redoubled training on querying requirements and made technical upgrades to certain commonly-used querying tools

---

[22] In addition to the findings of the IG and OCO reviews, the government identifies improper queries in the course of regular oversight efforts. The government reports those incidents to the Court through individual notices and quarterly reports.

[23] By operation of Section 1881a(i)(1)(B), the government's submission on March 30, 2017, of amendments to the 2016 Certifications and revised procedures started a new 30-day period for Court review, which ends on April 29, 2017.

that were designed to reduce the likelihood of non-compliant queries. Id. at 100-101. Meanwhile, the government continued to report further compliance issues regarding the handling and querying of upstream Internet collection[24] and to investigate potential root causes of non-compliant querying practices. April 7, 2017 Preliminary Notice (Queries) at 4 n.4.

5. The 2017 Amendments

As embodied in the March 30, 2017 Submission, the government has chosen a new course: [redacted]; sequestering and then destroying raw upstream Internet data previously collected; and substantially narrowing the scope of upstream collection [redacted]. Most significantly, the government will eliminate "abouts" collection altogether, which will have the effect of eliminating acquisition of the more problematic types of MCTs. These changes should substantially reduce the acquisition of non-pertinent information concerning U.S. persons pursuant to Section 702.

As of March 17, 2017, NSA had [redacted]. Revisions to the NSA Minimization Procedures now state that all Internet transactions acquired on or before that date and existing in NSA's institutionally managed

[24] See April 7, 2017, Preliminary Notice of Compliance Incidents Regarding the Labeling and Querying of Section 702-Acquired Data ("April 7, 2017 Preliminary Notice (Mislabeling)") (nearly [redacted] communications acquired through upstream Internet collection were "incorrectly labeled" as acquired from Internet service providers and, as a result, likely subject to prohibited queries using U.S.-person identifiers); April 7, 2017, Preliminary Notice of Potential Compliance Incidents Regarding Improper Queries ("April 7, 2017 Preliminary Notice (Queries)") (identifying another [redacted] potential violations of prohibition on using U.S.-person identifiers to query Internet upstream collection).

repositories[25] will be sequestered pending destruction such that "NSA personnel will not be able to access the[m] for analytical purposes." March 30, 2017 Memorandum at 4; see NSA Minimization Procedures §3(b)(4)a.

NSA will destroy such sequestered Internet transactions as soon as practicable through an accelerated age-off process. See NSA Minimization Procedures §3(b)(4)a. The government represents that the age-off may take up to one year to complete and verify (with quarterly reports to the Court), and that:

- Pending destruction, sequestered transactions (a) will not be subject to separate age-off or purge processes that otherwise would apply to them, see March 30, 2017 Memorandum at 15-16 & nn. 16-17; and (b) will be available only to NSA technical and compliance personnel for the limited purposes of ensuring the integrity of the systems used to store them and the controls that limit other employees' access to them, see id. at 14 n.13; NSA Minimization Procedures §3(b)(4)a.

- Copies of sequestered transactions will remain in backup and archive systems, not available for use by intelligence analysts, until they age off of those systems in the ordinary course. See March 30, 2017 Memorandum at 14 n.13;

- Sequestered transactions may be retained for litigation purposes as contemplated by Section 3(c)(3) of the NSA Minimization Procedures, subject to prompt notification to the Court. See id. at 16-17 & n.18.

- Certain records derived from upstream Internet communications (many of which have been evaluated and found to meet retention standards) will be retained by NSA, even though the underlying raw Internet transactions from which they are

---

[25] The March 30, 2017 Submission does not define what an "institutionally managed repository" is. If the government intends not to apply the above-described sequester-and-destroy process to any information acquired on or before March 17, 2017, by Internet upstream collection because the information is not contained in an "institutionally managed repository," it shall describe the relevant circumstances in a written submission to be made no later than June 2, 2017; however, the government need not submit such a description for circumstances referenced in this Opinion and Order as ones in which NSA may retain such information.

derived might be subject to destruction. These records include serialized intelligence reports and evaluated and minimized traffic disseminations; completed transcripts and transcriptions of Internet transactions; [redacted];[26] information used to support Section 702 taskings and FISA applications to this Court; and [redacted]."[27] See March 30, 2017 Memorandum at 20-24.

Finally, upstream collection of Internet transactions [redacted] for communications to or from a targeted person, but "abouts" communications may no longer be acquired. The NSA Targeting Procedures are amended to state that "[a]cquisitions conducted under these procedures will be limited to communications ***to or from*** persons targeted in accordance with these procedures," NSA Targeting Procedures § I, at 2 (emphasis added), and NSA's Minimization Procedures now state that Internet transactions acquired after March 17, 2017, "that are not to or from a person targeted in accordance with NSA's section 702 targeting procedures are unauthorized acquisitions and therefore will be destroyed upon recognition." NSA Minimization Procedures § 3(b)(4)b.[28] Because they are regarded as unauthorized, the government will report any acquisition of such communications to the Court as an incident of non-compliance. See March 30, 2017 Memorandum at 17-18.

---

[26] [redacted]. See NSA Targeting Procedures § I at 6.

[27] [redacted] March 30, 2017 Memorandum at 23.

[28] The targeting procedures still require NSA either to use Internet Protocol (IP) filtering of upstream Internet collection to "limit such acquisitions to Internet transactions that originate and/or terminate outside the United States" or [redacted] Id.

Conforming changes are made throughout the NSA Minimization Procedures to remove references to "abouts" collection. Section 3(b)(4) of those procedures, in particular, is significantly revised and streamlined to reflect the narrower scope of authorized collection. For example, detailed procedures previously appearing in Section 3(b)(4) requiring sequestration and special handling of MCTs in especially problematic categories (e.g., those in which the "active user" is a non-target who is in the United States or whose location is unknown) are removed. Because NSA is no longer authorized to acquire those forms of MCTs, if it somehow acquires one, NSA must now destroy it upon recognition.[29]

NSA may continue to acquire MCTs under the amended procedures, but only when it can ensure that the target is a party to the entire MCT or, in other words, when the target is the active user. [redacted]

[29] Internet transactions properly acquired through NSA upstream collection after March 17, 2017, will continue to remain subject to a two-year retention limit, "unless the NSA specifically determines that at least one discrete communication within the Internet transaction meets the retention standards" in the NSA Minimization Procedures. See NSA Minimization Procedures § 3(c)(2). This reflects no change from the current procedures.

[redacted].[30] See March 30, 2017 Memorandum at 10.

It will still be possible, however, for NSA to acquire an MCT that contains a domestic communication. For example, [redacted] If NSA determines that the sender and all intended recipients of a discrete communication within an MCT were located in the United States at the time of that discrete communication, then the entire MCT must be promptly destroyed, see NSA Minimization Procedures § 5, unless the Director makes the required waiver determination for each and every domestic communication contained in the MCT. March 30, 2017 Memorandum at 9 n.9.[31]

U.S.-Person Queries. In light of the elimination of "abouts" communications from Section 702 upstream collection, the government proposes a change to Section 3(b)(5) of the NSA Minimization Procedures that would remove the prohibition on NSA analysts conducting

---

[30] This enumeration is without prejudice to NSA's ability to acquire other types of communications if it can limit acquisition to communications to or from a target as required by the new procedures.

[31] The NSA Minimization Procedures generally take an "all-or-nothing" approach to retention or destruction of MCTs. Thus, an MCT in which ***any*** discrete communication is not to or from a target is also subject to destruction in its entirety. See NSA Minimization Procedures § 3(b)(4)b; March 30, 2017 Memorandum at 13 n.12 ("[I]f for some reason NSA acquires an Internet transaction in which any discrete communication contained therein is not to or from a section 702 target, NSA must destroy such transactions upon recognition.").

queries of Internet upstream data using identifiers of known U.S. persons. Under this proposal, NSA analysts could query upstream data using known U.S. person identifiers, subject to the same requirements that apply to their queries of other Section 702-acquired data. Specifically, any query involving a U.S.-person identifier is subject to NSA internal approval requirements and "require[s] a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information." NSA is required to maintain records of all such determinations and those records are subject to review by NSD and ODNI. See NSA Minimization Procedures § 3(b)(5).[32]

The Court agrees that the removal of "abouts" communications eliminates the types of communications presenting the Court the greatest level of constitutional and statutory concern. As discussed above, the October 3, 2011 Memorandum Opinion (finding the then-proposed NSA Minimization Procedures deficient in their handling of some types of MCTs) noted that MCTs in which the target was the active user, and therefore a party to all of the discrete communications within the MCT, did not present the same statutory and constitutional concerns as other MCTs. The Court is therefore satisfied that queries using U.S.-person identifiers may now be permitted to run against information obtained by the above-described, more limited form of upstream Internet collection, subject to the same restrictions as apply to querying other forms of Section

[32] The Court understands that DOJ and ODNI review all U.S.-person identifiers approved for use in querying contents of Section 702-acquired communications as well as the written documentation of the foreign intelligence justifications for each such query during bi-monthly compliance reviews. See November 6, 2015 Opinion at 25 n.22.

702-acquired data.[33] See generally October 3, 2011 Memorandum Opinion at 22-24 (finding that addition of a provision allowing NSA to query non-upstream Internet transactions using U.S. person identifiers was consistent with the statute and the Fourth Amendment); November 6, 2015 Opinion at 24-26 (after inviting views of amicus curiae on this issue, finding that the CIA and NSA minimization procedures permitting such queries comported with the statute and the Fourth Amendment).

The Court concludes that, taken as a whole, these changes strengthen the basis for finding that the NSA Targeting Procedures meet the requirements of Section 1881a(d)(1) and that the NSA Minimization Procedures meet the definition of such procedures in Section 1801(h). The elimination of "abouts" collection and, consequently, the more problematic forms of MCTs, focuses Section 702 acquisitions more sharply on communications to or from Section 702 targets, who are reasonably believed to be non-U.S. persons outside the United States and expected to receive or communicate foreign intelligence information. That sharper focus should have the effect that U.S. person information acquired under Section 702 will come more

[33] Of course, NSA still needs to take all reasonable and necessary steps to investigate and close out the compliance incidents described in the October 26, 2016 Notice and subsequent submissions relating to the improper use of U.S.-person identifiers to query terms in NSA upstream data. The Court is approving on a going-forward basis, subject to the above-mentioned requirements, use of U.S.-person identifiers to query the results of a narrower form of Internet upstream collection. That approval, and the reasoning that supports it, by no means suggest that the Court approves or excuses violations that occurred under the prior procedures.

predominantly from non-domestic communications that are relevant to the foreign intelligence needs on which the pertinent targeting decisions were based.[34]

D. NCTC Raw Take Sharing

1. Sharing of Unminimized Information Acquired Under [redacted] with NCTC

The September 26, 2016 Submission proposes for the first time to allow NCTC access to unminimized information acquired by NSA and FBI pursuant to [redacted] Previously, NCTC only had access to minimized Section 702-acquired information residing in FBI's general indices and relating to certain categories of investigations concerning international terrorism. NCTC has not, and will not under the government's proposal, engage in FISA collection of its own. It does, however, have significant experience with handling FISA-acquired information, including unminimized information obtained pursuant to Titles I and III and Sections 704 and 705(b) of the Act, pursuant to AG- and FISC-approved minimization procedures.

Beginning in 2008, NCTC was authorized to receive certain FISA-derived information from terrorism cases that FBI had uploaded into its Automated Case Support ("ACS") system. FISA information residing in ACS has been minimized by FBI and appears in investigative

---

[34] When the Court approved the prior, broader form of upstream collection in 2011, it did so partly in reliance on the government's assertion that, due to [redacted] some communications of foreign intelligence interest could only be acquired by such means. See October 3, 2011 Memorandum Opinion at 31 & n. 27, 43, 57-58. This Opinion and Order does not question the propriety of acquiring "abouts" communications and MCTs as approved by the Court since 2011, subject to the rigorous safeguards imposed on such acquisitions. The concerns raised in the current matters stem from NSA's failure to adhere fully to those safeguards.

reports and other work product. The FISC in 2008 found that NCTC's access to such information in ACS was "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information" under 50 U.S.C. § 1801(h)(1). Docket No. [redacted], Memorandum Opinion and Order entered on Oct. 8, 2008, at 3-6. Later, in 2012, NCTC was granted access to raw information from terrorism cases obtained under Titles I and III and Sections 704 and 705(b) of the Act, subject to expanded minimization procedures. See Docket Nos. [redacted], Memorandum Opinion and Order entered on May 18, 2012 ("May 18, 2012 Opinion").

NCTC also has experience handling information obtained under Section 702 of the Act. Since 2012, NCTC has had access to minimized information obtained under Section 702 through its access to certain case categories in FBI's general indices (including ACS and another system known as Sentinel). See Docket Nos. [redacted], Memorandum Opinion entered on Sept. 20, 2012, at 22-25 ("September 20, 2012 Opinion").

In each instance in which the FISC has authorized expanded sharing of FISA-acquired information with NCTC, the FISC has recognized NCTC's role as the government's primary organization for analyzing and integrating all intelligence pertaining to international terrorism and counterterrorism. For example, in approving NCTC's access to minimized Section 702-acquired information in FBI general indices in 2012, the FISC observed that NCTC was statutorily charged with ensuring that intelligence agencies receive all-source intelligence support and that executive and legislative branch officials have access to international terrorism-related intelligence information and analysis to meet their constitutional responsibilities. See id. at 23

(citing then-applicable statutory provisions); see also Affidavits of Nicholas Rasmussen, Director, NCTC, appended at Tab 5 to each of the 2016 Certifications, at 1. The government further avers in support of the current proposal that: (1) NCTC is statutorily charged with providing "strategic operational plans for the civilian and military counterterrorism intelligence and operations across agency boundaries, both inside and outside the United States;" and (2) the NCTC Director "is assigned 'primary responsibility within the United States Government for conducting net assessments of terrorist threats.'" September 26, 2016 Memorandum at 12-13 (citing 50 U.S.C. § 3056(f)(1)(B) and (G)).

The Court is satisfied that NCTC's receipt of information acquired under [redacted] is consistent with its mission. As for the NCTC's need to have access to this information in raw form, the government asserts that NCTC's ability to obtain Section 702-acquired information more quickly and in a form closer to its original, and to examine that information in NCTC systems, using its own analytical tools in the context of potentially related information available in NCTC systems, will enhance NCTC's ability to produce counterterrorism foreign intelligence information. See September 26, 2016 Memorandum at 13-14. The government provides an example in which NCTC was able to use its access to raw FISA-acquired information from collection under other provisions of FISA to provide a timely and unique assessment that was shared with other elements of the Intelligence Community in support of their intelligence collection and analysis functions. See id. at 15. One would hope that this is one of many such examples.

In any event, as noted above, the government's proffered rationale for sharing raw information with NCTC was accepted by the FISC in the context of information obtained under other provisions of the Act, and the Court is persuaded that it applies with equal force in the context of collection under Section 702. Among other things, the volume of collection under Section 702 militates in favor of bringing all available analytical resources to bear on the careful analysis and exploitation of foreign intelligence information from such collection. The Court also credits the assertion that time can be of the essence in many rapidly-unfolding counterterrorism investigations. The Court is persuaded that timely access to raw Section 702-acquired information will enhance NCTC's ability to perform its distinct mission, to support the activities of other elements of the Intelligence Community, and to provide valuable input to senior decisionmakers in the Executive Branch and Congress.

Moreover, the information acquired under [redacted] though voluminous – is the result of targeting persons reasonably believed to be non-United States persons located outside the United States. For that reason, it is unlikely to contain as high a proportion of information concerning United States persons as information acquired by FISA electronic surveillance and physical search, which often involve targets who are United States persons and typically are directed at persons in the United States.

To be sure, information concerning unconsenting United States persons has been and will continue to be acquired under Section 702 and [redacted] particularly. The minimization procedures must carefully regulate the government's use and dissemination of such U.S. person information in order to satisfy the definition of "minimization

procedures" at Section 1801(h). The procedures NCTC will be required to follow with respect to its handling of such information are examined in detail below.

The Court also finds that the scope of the proposed sharing with NCTC is appropriate. Consistent with NCTC's mission, the proposed sharing of unminimized Section 702-acquired information is limited to [redacted] The government notes that the sharing will not include telephony data or the results of upstream Internet collection; in other words, it will be limited to Internet communications obtained with the assistance of the direct providers of the communication services involved. See September 26, 2016 Memorandum at 10-11. NCTC will receive raw information [redacted] and subject to the same limitations as CIA (no upstream Internet collection and no telephony). Id.

The government undertakes to notify the Court before altering these arrangements and providing raw telephony or upstream Internet data to NCTC, FBI or CIA. See id. at 11 n.7; accord March 30, 2017 Memorandum at 9-10 n.10. With regard to upstream Internet collection, the Court has determined that mere notification to the FISC would be insufficient, especially as NSA is in the process of transitioning to a narrower form of collection and segregating and destroying the results of the prior, broader collection. Accordingly, the Court is ordering that raw information obtained by NSA's upstream Internet collection under Section 702 shall not be provided to FBI, CIA or NCTC unless it is done pursuant to revised minimization procedures that are adopted by the AG and DNI and submitted to the FISC for review in conformance with Section 702.

With that limitation, the Court finds that NCTC's receipt of raw information acquired under [redacted] subject to appropriate minimization procedures as described below, will "minimize the . . . retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1).[35] The NCTC has followed AG- and FISC-approved minimization procedures in connection with its prior receipt of FISA-acquired information, including Section 702-acquired information, with relatively few documented instances of noncompliance. See generally Docket Nos. [redacted], Memorandum Opinion and Order entered on Aug. 26, 2014 Opinion ("August 26, 2014 Opinion") at 37 (noting that "no significant compliance issues have arisen under [NCTC's Section 702 minimization] procedures").

a. Changes to FBI and NSA Procedures Relating to Raw Information Sharing with NCTC

As noted above, the extension of raw information sharing to NCTC requires changes to several sets of procedures.[36] First, FBI's targeting procedures, and FBI and NSA's minimization procedures, are each amended to reflect the fact that those agencies may now provide to NCTC

---

[35] With regard to § 1801(h)(2)'s limitation on the dissemination of United States person identities, the Court adopts the analysis set out at pages 7-8 of the May 18, 2012 Opinion.

[36] Some technical, conforming edits to the certifications and procedures occasioned by the extension of raw information sharing to NCTC are not discussed herein because they raise no issues material to the Court's review. Certain other changes to the proposed certifications and procedures are not discussed for the same reason.

unminimized communications obtained under [redacted] See FBI Targeting Procedures § I.6; NSA Minimization Procedures § 6(c)(3); FBI Minimization Procedures § V.E. NCTC is required to identify to NSA those individual Section 702 selectors for which it wishes to receive unminimized information, and is required to apply its own approved minimization procedures to such information. See NSA Minimization Procedures § 6(c)(3); FBI Minimization Procedures § V.E.

b. Changes to NCTC Minimization Procedures Relating to Raw Information Sharing with NCTC

The NCTC Minimization Procedures have been enhanced significantly to account for its receiving raw information under Section 702. But they are not crafted out of whole cloth. They are modeled on the previously-approved minimization procedures that apply to NCTC's receipt of information under Titles I and III and Sections 704 and 705(b) of the Act.[37] Modifications are proposed to address issues that are unique to Section 702 collection and in some instances to harmonize the proposed NCTC procedures with those used by the FBI, NSA, and CIA in their handling of Section 702-acquired information. Several key elements of the NCTC Minimization Procedures are discussed below, focusing on instances in which they depart from the previously approved NCTC Title I Procedures.[38]

---

[37] For ease of reference, this opinion refers to these procedures (the "National Counterterrorism Center Standard Minimization Procedures for Information Acquired by the Federal Bureau of Investigation Pursuant to Title I, Title III, or Section 704 or 705(b) of the Foreign Intelligence Surveillance Act") as the "NCTC Title I Procedures."

[38] The government does not propose targeting procedures for NCTC, so NCTC will not be authorized to engage in any Section 702 collection.

The NCTC Minimization Procedures do not have a provision restricting NCTC's processing, retention, and dissemination of third-party information. In NCTC's Title I Procedures, third-party information is defined to include "communications of individuals who are not the targets of the collection," and to exclude "any information contained in a communication to which the target is a party." NCTC Title I Procedures § A.3.h. Third-party information thus defined is subject to stricter retention, processing, and dissemination limitations under NCTC's Title I Procedures than information directly involving the target. See id. § C.4. In 2012, the FBI removed similar third-party information provisions from its Section 702 minimization procedures. In approving that change, the Court explained that in the context of Section 702 collection such rules

> have no practical effect because the term "target" is defined as "the user(s) of a targeted selector." In light of that definition . . . there are no "third party" communications [in Section 702 collection] for the FBI to minimize. Because the deletion of the provisions regarding third party communications does not alter the manner in which the FBI acquires, retains, or disseminates Section 702 information, this change is not problematic under Section 1801(h).

September 20, 2012 Opinion at 17-18 (internal citations omitted). For the same reason, the omission of provisions present in NCTC's Title I Procedures governing the NCTC's retention, processing, and dissemination of third-party information from its Section 702 minimization procedures presents no impediment to their approval.

Exclusion and Departure Provisions. The NCTC Minimization Procedures contain certain exclusions and departure provisions that are consistent with the NCTC Title I Procedures with two notable exceptions:

(1) An exclusion is added for the performance of lawful oversight functions of NSD, ODNI, relevant Inspectors General, and NCTC itself, which is consistent with parallel provisions in other agencies' procedures. See NCTC Minimization Procedures § A.6.e; NSA Minimization Procedures § 1; FBI Minimization Procedures § I.G; CIA Minimization Procedures § 6(f); and

(2) A separate exclusion addresses compliance with congressional and judicial mandates. NCTC Minimization Procedures § A.6.d.

The latter provision was amended across all the agencies' minimization procedures in the September 26, 2016 Submission and is the subject of separate discussion below.

U.S. Person Presumptions. In general, the procedures provide a rebuttable presumption that persons known to be in the United States are United States persons, and those known or reasonably believed to be outside the United States are non-United States persons. Id. § A.4.a and b. The NCTC Minimization Procedures diverge slightly from their Title I counterpart with respect to individuals whose locations are not known. [redacted] NCTC Title I Procedures § A.4.a. That approach makes sense in those procedures, which apply to information predominantly obtained by electronic surveillance and physical search – [redacted] – directed at persons in the United States. [redacted] Id. §

A.4.c. [redacted] NCTC Minimization Procedures §A.4.e.

The Court assesses that Section 702 collection is more analogous to [redacted] than it is to other forms of collection that are regulated by the NCTC Title I Procedures and that the application of the [redacted] is appropriate in this context. Section 702 collection focuses exclusively on electronic data and communications collected with the assistance of electronic communication service providers, and its targets are reasonably believed to be non-U.S. persons located overseas. The presumption of non-U.S. person status for a communicant whose location is not known is also consistent with the presumptions allowed under the FBI and NSA's current and proposed Section 702 minimization procedures. See NSA Minimization Procedures § 2(k)(2); FBI Minimization Procedures § I.D. The Court finds the same framework reasonable as applied to NCTC's handling of Section 702 information and consistent with the requirements of Section 1801(h). See September 20, 2012 Opinion at 15-16 (approving parallel change to FBI Section 702 Minimization Procedures).[39]

Retention. The NCTC Minimization Procedures impose a retention schedule and framework that are consistent with those followed by FBI for Section 702-acquired information

[39] The NCTC Minimization Procedures also include provisions regarding unincorporated associations and aliens who have been admitted for lawful permanent residence (NCTC Minimization Procedures § A.4.c and d) that track current provisions in the NSA Minimization Procedures (§ 2(k)(3) and (4)). The Court sees no issue with these provisions.

and, with a few immaterial exceptions not warranting separate discussion, with corresponding provisions of the NCTC Title I Procedures. In brief, information that the NCTC retains on an electronic and data storage system, but has not reviewed, generally must be destroyed after five years from the expiration date of the certification authorizing the collection. NCTC Minimization Procedures § B.2.a. Information retained on such systems that has been reviewed, but not identified as information that reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime is generally subject to special access controls after ten years from such expiration date, and shall be destroyed after fifteen years from such date. Id. § B.2.b.[40]

In one respect, the proposed NCTC Minimization Procedures are more restrictive than the NCTC Title I Procedures: Unlike the NCTC Title I Procedures, the NCTC Minimization Procedures expressly provide that the prescribed time limits for retention apply to metadata repositories. NCTC Minimization Procedures § C.3; see October 4, 2016 Transcript at 7. They further require appropriate training and access controls for NCTC employees granted access to Section 702-acquired information. NCTC Minimization Procedures §§ B.1, F.1, F.2 and F.3. They also require that such information be maintained in secure systems that enable NCTC to mark or otherwise identify communications that meet the standards for retention. Id. Consistent with the procedures followed by other agencies, the NCTC Minimization Procedures require

---

[40] Generally speaking, information identified as meeting one of those criteria is not subject to the above-described temporal limitations on retention. Id. § B.3. See, however, the discussion on page 46 below regarding limitations on retention and use of evidence of a crime that is not foreign intelligence information.

destruction of information obtained under a reasonable, but mistaken, belief that the target was appropriate for Section 702 collection, subject to limited waiver provisions. Id. § B.4. Finally, they include provisions for retention of information reasonably believed to be necessary for, or potentially discoverable in, administrative, civil or criminal litigation. Id. § B.5. Analogous provisions already appear in NSA's and CIA's Minimization Procedures. See NSA Minimization Procedures § 3(c)(4); CIA Minimization Procedures § 11.

Processing. The NCTC Minimization Procedures set standards for queries of data obtained under Section 702, including requiring written justifications for queries using U.S. person identifiers that are subject to subsequent review and oversight by NSD and ODNI. NCTC Minimization Procedures § C.1; see also id. § C.3 (metadata queries "must be reasonably likely to return foreign intelligence information"). They apply heightened handling requirements to sensitive information and privileged communications. The provisions for sensitive information are essentially identical to those found in the NCTC Title I Procedures. Compare NCTC Minimization Procedures § C.4 with NCTC Title I Procedures § C.5.

The proposed procedures for NCTC's handling of privileged communications obtained under Section 702 closely track those found in NSA's and CIA's Section 702 minimization procedures. Compare NCTC Minimization Procedures § C.5 with NSA Minimization Procedures § 4; CIA Minimization Procedures § 7. The NCTC Minimization Procedures require, among other things, the destruction of attorney-client communications that are affirmatively determined not to contain foreign intelligence information or evidence of a crime. See NCTC Minimization Procedures § C.5.a. If an attorney-client communication appears to contain foreign

intelligence information or evidence of a crime, [redacted] See id. § C.5.b, c, and e. Communications containing privileged information will be segregated when such information pertains to a criminal charge in the United States, [redacted] See id. § C.5.c, d, e, and f. [redacted] See id. § C.5.i. [redacted] See id. § C.5.g and h.

The Court closely examined substantial revisions to the NSA and CIA procedures as they relate to privileged communications in 2015, and found that they "serve to enhance the protection of privileged information" and "present no concern under Section 1801(h)." See November 6, 2015 Opinion at 18. The Court now finds the same to be true with respect to the NCTC Minimization Procedures.

Dissemination. The dissemination provisions of the NCTC Minimization Procedures (§ D) provide for disseminations in a manner consistent with CIA's and NSA's handling of Section 702-acquired information. They also track in all material respects the NCTC Title I Procedures, which have been found to satisfy Section 1801(h).

Handling of Information in FBI General Indices. The NCTC Minimization Procedures, like the NCTC Title I Procedures, include a separate section that addresses NCTC's handling of minimized Section 702 information made available to it through FBI's general indices. This provision of the NCTC Minimization Procedures tracks the corresponding provision of the NCTC Title I Procedures. Compare NCTC Minimization Procedures § E with NCTC Title I Procedures § E. The government points out that the description of individuals who are expected to be allowed access to information in such systems ("NCTC personnel") is meant to be broader than the defined term "NCTC employees" that is used in all other instances throughout the proposed NCTC Minimization Procedures. The government explains that the broader term "NCTC personnel" is meant to encompass (in addition to the NCTC employees, detailees, and contractors who would qualify as "NCTC employees" as defined in the proposed procedures, see NCTC Minimization Procedures § A.3.b) NCTC assignees from other agencies. The government explains that, consistent with the current NCTC Section 702 minimization procedures, such assignees will continue to have access to minimized information in FBI general indices but will not be allowed to access raw Section 702-acquired information. September 26, 2016 Memorandum at 15 n.9. The Court assesses that is a sensible distinction.

Two Additional Issues. Two particular provisions in the agencies' proposed minimization procedures relating to NCTC represent departures from current practice under Section 702 and merit separate discussion. Those provisions pertain to NCTC's retention of evidence of a crime and receipt of information from FBI and NSA for collection avoidance purposes.

NCTC's Retention of Evidence of Crime. The predecessor procedures that regulated NCTC's retention, use, and dissemination of minimized Section 702 information obtained through FBI's general indices acknowledged that some of the information made available to NCTC might constitute evidence of a crime, but not foreign intelligence information or information necessary to understand such information or assess its importance. As a law enforcement agency, FBI would have a reason to maintain such information in its general indices, where NCTC employees might encounter it. NCTC, as a non-law-enforcement agency, was precluded under its previous Section 702 minimization procedures from retaining (in its own systems), using or disseminating such information. By contrast, under the new NCTC Minimization Procedures (and only with respect to information it receives in raw form),[41] NCTC may retain and disseminate evidence of a crime for law enforcement purposes. *See* NCTC Minimization Procedures §§ A.7, D.2. This proposed approach is consistent with Sections A.7 and D.2 of the NCTC Title I Procedures.

The government asserts that, under the proposed NCTC Minimization Procedures, NCTC might review raw information that has not been, and may never be, reviewed by any other agency. As such, the government posits, NCTC must disseminate evidence of a crime to meet its "crime reporting obligations" under Executive Order 12333 and other applicable law. See

---

[41] As noted above, the new NCTC Minimization Procedures incorporate (in Section E) the rules currently governing NCTC's retention, use, and dissemination of minimized information that it obtains through FBI's general indices. NCTC continues to be prohibited from retaining, using or disseminating information it obtains from those indices that constitutes evidence of a crime, but not foreign intelligence information, with anyone, including law enforcement, for reasons explained below. See NCTC Minimization Procedures § E.2

September 26, 2016 Memorandum at 16-17. Under NCTC's minimization procedures as now in effect, NCTC only has access to information from FBI indices that has already been reviewed and minimized by FBI, so it is presumed that FBI would have taken all necessary steps with respect to actionable law enforcement information. Under that construct, NCTC could, as required by its procedures, simply disregard and delete that information from its holdings (unless there was a foreign intelligence reason for NCTC to retain it). The government asserts that the same would not be true with respect to raw information passed to NCTC. See id.

It is less readily apparent, however, why NCTC would need to retain evidence of a crime after it has been passed to a law enforcement agency. The government asserts that NCTC needs to preserve original copies of the relevant information in order to be able to respond to potential follow-on requests for information or assistance from law enforcement. See October 4, 2016 Transcript at 4-6.[42] In other words, NCTC would have no reason to retain the information for its own purposes, but it would have a need for retention that derives from the needs of the law enforcement agency to which NCTC passed the information. The government further posits that NCTC may be the only agency that retains a copy of the relevant information and thus may be the only entity able to respond to follow-up requests from law enforcement. See October 4, 2016 Transcript at 5.

[42] The government correctly points out that in its opinion approving the NCTC's Title I Procedures, which contain identical provisions with respect to crime reporting and evidence of a crime, the Court found that those provisions met the statutory definition of minimization procedures in Section 1801(h)(3), which prescribes procedures that "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." See September 26, 2016 Memorandum at 16 n.10.

The Court credits the government's explanation of NCTC's derivative need to retain such information for law enforcement purposes. It bears emphasis, however, that NCTC may retain and disseminate evidence of a crime that is not foreign intelligence information or necessary to understand foreign intelligence information or assess its importance and otherwise would be subject to destruction under the generally applicable age-off schedule, see NCTC Minimization Procedures § B.2, only in furtherance of those law enforcement purposes. See id. § D.2. The Court understands and expects that NCTC will only retain such information – including after it has been disseminated in compliance with crime reporting obligations, see id. § A.7 – for so long as is reasonably necessary to respond to law enforcement requests of the kind posited by the government. In the interim, NCTC shall make no independent use of such information. The Court directs the government to take steps to ensure that NCTC abides by these limitations and that any failures to do so are appropriately identified and reported to the FISC.

Collection Avoidance. The FBI and NSA would also be allowed, under proposed amendments to their respective procedures, to share with NCTC for "collection avoidance" purposes information about domestic communications obtained under Section 702 that indicate that a targeted person is in the United States or otherwise should no longer be targeted under Section 702. See NSA Minimization Procedures § 5; FBI Minimization Procedures § III.A. These provisions now allow sharing of such information among FBI, NSA, and CIA. At first it was not clear to the Court why this provision should be extended to include NCTC, given that NCTC engages in no independent collection under Section 702, or, so far as the Court is aware, under any other authorities. [redacted]

[redacted] Indeed, it seemed counterintuitive to the Court that an agency not engaged in collection would need to receive information, otherwise subject to destruction, for "collection avoidance purposes."

The government's response is that NCTC, upon receipt of such information, might be in a position to "connect the dots" and identify other individuals who might not be viable targets for Section 702 collection (or perhaps other facilities that might be used by the same individual and should not be targeted). See September 26, 2016 Memorandum at 17-18. Such information would also put NCTC on notice that the selector, or related selectors, might not be viable for nomination to be targeted for collection by other agencies. Id. The government adds that FBI and NSA typically only share the minimum information necessary for collection avoidance purposes, such as technical information from the relevant communication or a mere notification that the communication triggered a flag regarding the propriety of targeting someone. Id.

Because the government offers a plausible explanation of the need for sharing such information with NCTC, the Court is prepared to approve the provisions in question, with the understanding that NCTC may not use or disclose this information except as needed for collection avoidance purposes.[43]

Subject to the above-described understandings, the Court finds that the proposed minimization procedures for NCTC's handling of raw information acquired under [redacted]

[43] NSA's procedures, for example, require that a domestic communication retained for collection avoidance purposes be placed on the NSA's "Master Purge List" ("MPL"), which prevents further analytical use or dissemination of the communication for any other reason. See NSA Minimization Procedures § 5.

[redacted], and the modifications to the other agencies' procedures relating to NCTC's receipt of such information, are reasonable. The NCTC Minimization Procedures address retention, use, and dissemination of Section 702-acquired information in ways that are consistent with logical analogues. Indeed, the FISC has approved all the major elements of those procedures in the context of other FISA minimization procedures, and the Court finds that, taken as a whole and as applied to raw information acquired under [redacted], the NCTC Minimization Procedures conform to 50 U.S.C. § 1801(h).

E. Other Changes to Targeting and Minimization Procedures in the September 26, 2016 Submission

1. Changes to FBI Minimization Procedures Permitting the Retention of Section 702-Acquired Information Subject to Preservation Obligations Arising from Litigation

In 2014, the FISC approved provisions permitting FBI, NSA, and CIA to retain Section 702-acquired information subject to specific preservation obligations arising in litigation concerning the lawfulness of Section 702. See August 26, 2014 Opinion at 21-25. Under those provisions, information otherwise subject to destruction under the agencies' respective minimization procedures would nonetheless be retained to satisfy litigation preservation obligations. Access to information retained under those provisions is tightly restricted. See id. at 21, 23.

The NSA and CIA minimization procedures accompanying the 2015 Certifications included revisions to these "litigation hold" provisions. Among other things, those procedures included new provisions whereby NSA and CIA may retain for litigation purposes Section 702-

acquired information otherwise subject to destruction requirements that are not set forth in the minimization procedures, provided that access to such information is strictly controlled as prescribed in the procedures.[44] The government must promptly notify the Court and seek its approval whenever this provision is invoked. See NSA Minimization Procedures § 3(c)(4)b; CIA Minimization Procedures § 11.b.

The litigation hold provisions also require NSA and CIA to provide DOJ with a summary of all litigation matters requiring preservation of Section 702-acquired information, a description of the Section 702-acquired information being retained, and, if possible based on the information available to the agencies, the status of each litigation matter. See NSA Minimization Procedures § 3(c)(4)a and b; CIA Minimization Procedures § 11.a and b.[45] The FISC, in considering the 2015 Certifications, appointed amicus curiae to help it evaluate these litigation hold provisions. The FISC agreed with the amicus's assessment that the revised litigation hold provisions "comport with the requirements of Section 1801(h) and strike a reasonable and appropriate

[44] As stated in the November 6, 2015 Opinion, the Court understands this provision to apply to destruction requirements arising under a FISC order, a FISC rule, or other FISC-approved procedures – e.g., the requirement that NSA destroy any communication acquired through the intentional targeting of a person reasonably believed to be a United States person or to be located in the United States, see NSA Targeting Procedures § IV.

[45] The FISC has ordered the government to submit a report at the end of each year identifying matters in which FBI, NSA or CIA is retaining Section 702-acquired information that would otherwise be subject to destruction in order to satisfy a litigation preservation obligation. See August 26, 2014 Opinion at 42. The Court has reviewed the litigation hold reports filed by the government in December 2015 and December 2016. The Court is reaffirming that reporting obligation and extending it to NCTC.

balance between the retention limitations reflected in FISA and the government's need to comply with its litigation-related obligations." November 6, 2015 Opinion at 16.

The proposed NCTC Minimization Procedures, like NSA's and CIA's, include litigation hold provisions that address departures from destruction requirements arising under NCTC's minimization procedures and from other sources. See NCTC Minimization Procedures § B.5. The government proposes now to expand the FBI Minimization Procedures to address the latter situation and to bring FBI's litigation hold provisions more closely into line with those of the other agencies. [redacted] In 2015, with the concurrence of a FISC-appointed amicus curiae, the FISC found these procedures appropriate as applied to NSA and CIA. November 6, 2015 Opinion at 16. The Court sees no basis for a contrary conclusion now with regard to the NCTC and FBI.

The Court emphasizes, however, the need promptly to notify and seek leave of the Court to retain information pursuant to such provisions. [redacted]

[redacted]

at 2-3. The Court will not look favorably on similarly lengthy delays in deciding whether to comply with an otherwise applicable destruction requirement or seek FISC approval to retain information in anticipation of bringing criminal charges.

2. Clarification of Age-off Requirements for Encrypted Information Under the FBI Minimization Procedures

In its 2015 Submission, the government added a new provision to the FBI Minimization Procedures permitting the FBI to retain Section 702-acquired information that is encrypted or believed to contain secret meaning for any period of time during which such material is subject to, or of use in, cryptanalysis or otherwise deciphering secret meaning. Access to such information is restricted to FBI personnel engaged in cryptanalysis or deciphering secret meaning. See FBI Minimization Procedures § III.G.5. Nonpublicly available information concerning unconsenting United States persons retained under the provision cannot be used for any other purpose unless such use is permitted under a different provision of the minimization procedures. See id. Once information retained under this provision is decrypted or its secret meaning is ascertained, the generally-applicable retention rules apply. The government stated that it would calculate the age-off date for such information from the later of the date of decryption or the date of expiration of the certification pursuant to which the information was

acquired. See Docket Nos. [redacted] July 15, 2015, Memorandum Regarding 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 at 18. But the procedures themselves were silent on this point.

When it approved the 2015 Certifications, the FISC encouraged the government to make this calculation methodology explicit in future versions of the procedures. November 6, 2015 Opinion at 20 n.19. The government has done so. The FBI Minimization Procedures now [redacted]

3. Revisions to Minimization Provisions Permitting Compliance with Judicial or Legislative Mandates

The NSA and CIA minimization procedures approved in the November 6, 2015 Opinion each state that "[n]othing in these procedures shall prohibit the retention, processing, or dissemination of information reasonably necessary to comply with specific constitutional, judicial, or legislative mandates." See November 6, 2015 Opinion at 21 (citing relevant provisions of procedures). The FISC took issue with the facial breadth of these provisions,

observing that "[a] provision that would allow the NSA and CIA to deviate from any of the[] restrictions [in their respective minimization procedures] based upon unspecified 'mandates' could undermine the Court's ability to find that the procedures satisfy" statutory requirements. Id. at 22. The FISC addressed this issue in three ways. First, in order to avoid finding a deficiency in the procedures, it applied an interpretive gloss that the government had previously articulated with regard to similar language in another set of minimization procedures, to the effect that such provisions would be invoked sparingly and applied only to directives specifically calling for the information at issue, and not to Executive Branch orders or directives. Id. at 22. The FISC emphasized that it "must construe the phrase 'specific constitutional, judicial, or legislative mandates' to include only those mandates containing language that clearly and specifically requires action in contravention of an otherwise-applicable provision of the requirement of the minimization procedures." Id. at 23. Second, to ensure that these provisions were actually applied in a manner consistent with the FISC's understanding, the government was directed to report any action in reliance on this provision to the FISC promptly and in writing, along with a written justification for each such action. Id. at 23-24.[46] Finally, the government was encouraged to consider replacing these broadly-worded provisions with language more narrowly tailored to the above-described intent. Id. at 24 n.20.

The government proffered revisions to these provisions in the September 26, 2016 Submission. The provisions, as revised and incorporated in all of the agencies' minimization

[46] This reporting requirement is carried forward by this Opinion and Order. The Court understands that this provision has not yet been invoked.

procedures, now require that the departure be "necessary to comply with a specific congressional mandate or order of a court within the United States." NSA Minimization Procedures § 1; FBI Minimization Procedures § I.G; CIA Minimization Procedures § 6.g; NCTC Minimization Procedures § A.6.d. The Court finds the revised language acceptable, but again wishes to emphasize that it expects this provision to be interpreted narrowly.

As described in the September 26, 2016 Memorandum at 6-7, the government has received requests from members of Congress, including 14 members of the House Judiciary Committee, for estimates of the number of communications of U.S. persons that have been acquired under Section 702. Responding to such requests would require NSA, and possibly other agencies, to structure queries designed to elicit information concerning U.S. persons with no foreign intelligence purpose, facially in violation of applicable minimization procedures. Such requests, which have not taken the form of a subpoena or other legal process, would not constitute legal mandates for purposes of the departure provision discussed above. Instead, the government submits that, in order to respond to such requests, it may take actions that contravene otherwise applicable minimization requirements pursuant to provisions of the minimization procedures that allow for performance of lawful oversight functions. For example, the NSA Minimization Procedures state that nothing in them shall restrict "NSA's performance of lawful oversight functions of its personnel or systems, or lawful oversight functions" of NSD, ODNI, or relevant Inspectors General. NSA Minimization Procedures § 1; see also FBI Minimization Procedures § I.G (same); CIA Minimization Procedures § 6.f (same); NCTC Minimization Procedures § A.6.e (same). The government also undertook to notify the Court

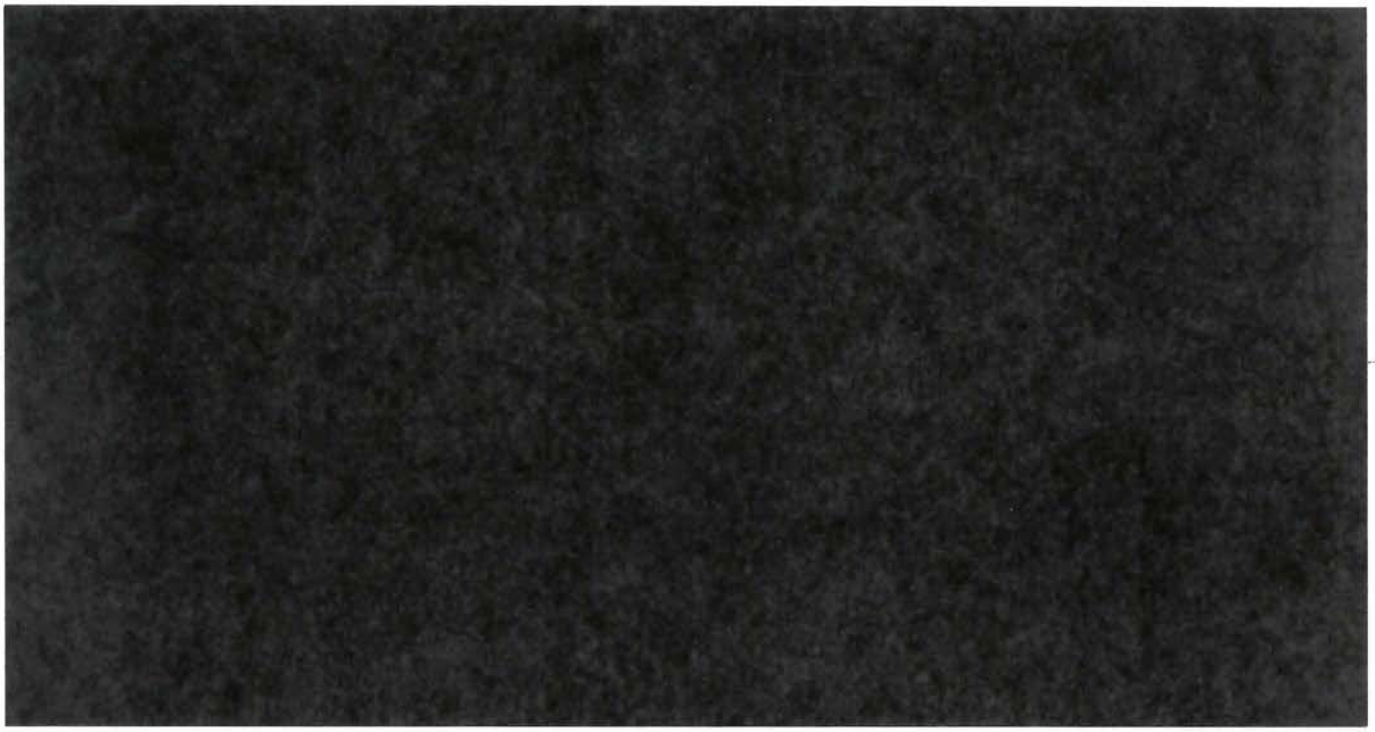
"promptly" if it "uses this provision to respond to such congressional oversight inquiries." September 26, 2016 Memorandum at 7.[47]

Although these provisions could more clearly address responses to requests from congressional overseers, the Court believes they can be fairly read to authorize actions necessary to respond to the requests described by the government. The Court directs the government to provide prompt written notification of any instance when an agency acts in contravention of otherwise applicable minimization requirements in order to respond to an oversight request from any outside entity other than those currently specified in its procedures. The Court expects the government to make such a submission regarding its response to the above-referenced congressional requests promptly upon completion of that response.

4. Amendment of FBI Targeting Procedures with Respect to [redacted]

[redacted]

[47] The government has since orally notified the Court that, in order to respond to these requests and in reliance on this provision of its minimization procedures, NSA has made some otherwise-noncompliant queries of data acquired under Section 702 by means other than upstream Internet collection.



The Court does not view this change, which deals with [redacted] agencies authorized to receive unminimized Section 702-acquired information, as problematic, provided that information is shared only with entities authorized to receive it (in the case of NCTC, information obtained pursuant to [redacted]). The legality of raw information sharing fundamentally rests on the foreign intelligence need to provide the information to the receiving agency and that agency's implementation of FISA-compliant minimization procedures. Accordingly, the Court concludes that this change does not preclude it from finding that the FBI Targeting Procedures meet the requirements of Section 1881a(d)(1).

F. Conclusions

1. The NSA and FBI Targeting Procedures Comply With Statutory Requirements and Are Reasonably Designed to Prevent the Targeting of United States Persons

To summarize, the proposed changes to NSA's targeting procedures now make clear that acquisitions thereunder will be limited to communications to or from persons targeted for acquisition under Section 702. FBI's revised targeting procedures allow it to [redacted] The Court has no difficulty finding that these changes, individually and taken together, do not detract from its earlier holdings with regard to the sufficiency and legality of the FBI and NSA targeting procedures.

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA Targeting Procedures and the FBI Targeting Procedures, as written, are reasonably designed, as required by Section 1881a(d)(1): (1) to ensure that any acquisition authorized under the 2016 Certifications is limited to targeting persons reasonably believed to be located outside the United States, and (2) 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. Moreover, for the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court concludes that the NSA and FBI Targeting Procedures, as written, are reasonably designed to prevent United States persons from

being targeted for acquisition – a finding that is relevant to the Court's analysis, which is set out below, of whether the procedures are consistent with the requirements of the Fourth Amendment.

2. The FBI, NSA, CIA, and NCTC Minimization Procedures Comply With Statutory Requirements

For the reasons stated above and in the Court's opinions in the Prior 702 Dockets, the Court similarly concludes that the NSA, FBI, CIA, and NCTC Minimization Procedures satisfy the definition of minimization procedures at Section 1801(h). In the November 6, 2015 Opinion, the FISC found that the minimization procedures accompanying the 2015 Certifications met statutory and constitutional standards. The FISC recommended two changes to the procedures in future submissions. In both instances, the government has acted on those suggestions, proposing changes to narrow the "legal mandate" exception to each agency's minimization procedures and define more precisely the time limits placed on FBI's retention of information believed to be encrypted or contain secret meaning. Both changes further cabin the relevant agencies' discretion and enhance the protection of nonpublicly available information concerning unconsenting United States persons.[48]

Other changes to minimization procedures pertain to FBI's retention of information for "litigation hold" purposes and enable sharing [redacted] with NCTC. (As noted above, NCTC's revised procedures incorporate

[48] As discussed above, the NSA Minimization Procedures have been revised to eliminate acquisition of "abouts" communications and the most problematic forms of MCTs. As a result of that change, the Court no longer views the prohibition on U.S.-person queries in NSA upstream collection to be necessary to comport with the statute or, as discussed below, the Fourth Amendment.

elements from various other procedures, with appropriate adaptations to fit the context of Section 702.) The Court concludes that none of the proposed changes to the agencies' minimization procedures, individually or collectively, precludes the Court from finding that such procedures comport with Section 1801(h).

Accordingly, the Court finds that the agencies' proposed minimization procedures meet the requirements of 50 U.S.C. § 1801(h). That finding is made in reliance on (1) the above-stated limitations on (a) the types of information that will, and will not, be shared in raw form with the FBI, CIA, and NCTC, and (b) NCTC's retention, use or disclosure of evidence of a crime and information received from other agencies for collection avoidance purposes; and (2) the expectation that the government will faithfully comply with the reporting requirements set forth below, in the procedures themselves, and in Rule 13 of the FISC Rules of Procedure.

G. The Targeting and Minimization Procedures Are Consistent with the Fourth Amendment

The Court must also assess whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A). The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

Reasonableness is "'the ultimate touchstone of the Fourth Amendment.'" In re Certified Question of Law, Docket No. 16-01, Opinion at 31 (FISA Ct. Rev. Apr. 14, 2016) (per curiam) ("In re Certified Question")[49] (quoting Riley v. California, 134 S. Ct. 2473, 2482 (2014)).[50] In assessing the reasonableness of a governmental intrusion under the Fourth Amendment, a court must "balance the interests at stake" under the "totality of the circumstances." In re Directives at 20. Specifically, a court must "balance . . . the degree of the government's intrusion on individual privacy" against "the degree to which that intrusion furthers the government's legitimate interest." In re Certified Question at 31. "The more important the government's interest, the greater the intrusion that may be constitutionally tolerated." In re Directives at 19-20.

> If the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in

[49] A declassified version of this opinion is available at: www.dni.gov/files/icotr/FISCR%Opinion%2016-01.pdf.

[50] Although "[t]he warrant requirement is generally a tolerable proxy for 'reasonableness' when the government is seeking to unearth evidence of criminal wrongdoing, . . . it fails properly to balance the interests at stake" when "the government is instead seeking to preserve the nation's security from foreign threats." In re Certified Question at 3. Accordingly, a warrant is not required to conduct surveillance "to obtain foreign intelligence for national security purposes . . . directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States." In re Directives Pursuant to Section 105B of FISA, Docket No. 08-01, Opinion at 18-19 (FISA Ct. Rev. Aug. 22, 2008) ("In re Directives"). (A declassified version of In re Directives is available at 551 F.3d 1004 (FISA Ct. Rev. 2008)). The FISC has repeatedly reached the same conclusion regarding Section 702 acquisitions. See, e.g., November 6, 2015 Opinion at 36-37; September 4, 2008 Opinion at 34-36; accord United States v. Hasbajrami, 2016 WL 1029500 at *7-*9 (E.D.N.Y. March 8, 2016); United States v. Mohamud, 2014 WL 2866749 at *15-*18 (D. Or. June 24, 2014).

> favor of upholding the government's actions. If, however, those protections are insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality.

Id. at 20.

"Collecting foreign intelligence with an eye toward safeguarding the nation's security serves . . . a particularly intense interest" that is "different from the government's interest in the workaday enforcement of the criminal law." In re Certified Question at 29 (internal quotation marks omitted); see also id. at 31 (noting "the paramount interest in investigating possible threats to national security"). For that reason, "the government's investigative interest in cases arising under FISA is at the highest level and weighs heavily in the constitutional balancing process." Id. at 32.

On the other side of the balance is the degree of intrusion on individual privacy interests protected by the Fourth Amendment. The degree of intrusion here is limited by restrictions on how the government targets acquisitions under Section 702 and how it handles information post-acquisition. For reasons explained above, the Court has found that the targeting procedures now before it are reasonably designed to limit acquisitions to targeted persons reasonably believed to be non-United States persons located outside the United States, whose privacy interests are not protected by the Fourth Amendment. See, e.g., November 6, 2015 Opinion at 38; September 4, 2008 Opinion at 37 (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990)). That is not to say, however, that targeting non-United States persons located outside the United States for acquisition under Section 702 never implicates interests protected by the Fourth Amendment. Under the revised procedures, the government may acquire communications to

which United States persons and persons within the United States are parties when such persons communicate with a Section 702 target.[51] Therefore it is necessary to consider how information from those communications will be handled.

Steps taken by the government to restrict the use or disclosure of information after it has been acquired can reduce the intrusiveness of the acquisition for purposes of assessing its reasonableness under the Fourth Amendment. See In re Certified Question at 35. In the Prior 702 Dockets, the FISC found that "earlier versions of the various agencies' targeting and minimization procedures adequately protected the substantial Fourth Amendment interests that are implicated by the acquisition of communications of such United States persons." November 6, 2015 Opinion at 38-39 (citing August 26, 2014 Opinion at 38-40; August 30, 2013 Opinion at 24-25). Specifically, "'the combined effect of these procedures'" was "'to substantially reduce the risk that non-target information concerning United States persons or persons inside the United States will be used or disseminated' and to ensure that 'non-target information that is subject to protection under FISA or the Fourth Amendment is not retained any longer than is reasonably necessary.'" November 6, 2015 Opinion at 39 (quoting August 26, 2014 Opinion at 40).

The November 6, 2015 Opinion included a careful analysis of the rules for querying Section 702 information using United States person identifiers under the minimization procedures for the NSA, the CIA, and especially the FBI. See November 6, 2015 Opinion at 24-

[51] NSA's elimination of "abouts" collection should reduce the number of communications acquired under Section 702 to which a U.S. person or a person in the United States is a party.

36, 39-45. After receiving briefing and oral argument from an amicus curiae appointed under 50 U.S.C. § 1803(i)(2)(B), the FISC concluded that, although its review did not involve treating each query as a separate action subject to a test for Fourth Amendment reasonableness, the querying rules were relevant to its assessment of whether the procedures as a whole were reasonable under the Fourth Amendment. November 6, 2015 Opinion at 40-41. The FISC further determined that the querying rules did not preclude a finding that the procedures were consistent with the requirements of the Fourth Amendment. Id. at 44-45.

In the procedures now before the Court, the relevant provisions of the CIA and FBI minimization procedures remain unchanged, see CIA Minimization Procedures at § 4; FBI Minimization Procedures at §§ III.D, IV.D, and the NCTC procedures generally track the pertinent requirements of the CIA Minimization Procedures. See NCTC Minimization Procedures at § C.3.[52]

With regard to the querying rules in the CIA and NCTC procedures, the Court adopts the analysis of the November 6, 2015 Opinion.

As discussed above, NSA's procedures now limit all acquisitions – including upstream Internet acquisitions – to communications to or from an authorized Section 702 target. That limitation places upstream Internet collection in a posture similar to other forms of Section 702 collection for the purpose of assessing reasonableness under the Fourth Amendment. The revised procedures subject NSA's use of U.S. person identifiers to query the results of its newly-

[52] Unlike the CIA procedures, the NCTC procedures require that queries of Section 702 metadata, as well as contents, be reasonably designed to return foreign intelligence information. NCTC Minimization Procedures at § C.3.

limited upstream Internet collection to the same limitations and requirements that apply to its use of such identifiers to query information acquired by other forms of Section 702 collection. See NSA Minimization Procedures § 3(b)(5). For that reason, the analysis in the November 6, 2015 Opinion remains valid regarding why NSA's procedures comport with Fourth Amendment standards of reasonableness with regard to such U.S. person queries, even as applied to queries of upstream Internet collection.

As discussed in the November 6, 2015 Opinion, the FBI's minimization procedures contemplate queries conducted to elicit foreign intelligence information and queries conducted to elicit evidence of crimes. With respect to the latter type of query, the FISC's approval of the FBI minimization procedures in 2015 was bolstered by the government's assessment that "FBI queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results" from Section 702 information. See November 6, 2015 Opinion at 44. To confirm the continued accuracy of that assessment, the FISC ordered the government to report on "each instance after December 4, 2015, in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information." Id. at 78.

The government has reported one set of queries as responsive to this requirement. On [redacted], an FBI analyst reviewing Section 702 information found an email message in which a person in the United States gave detailed descriptions of violent, abusive acts [redacted] committed [redacted] children. [redacted] Notice regarding FBI queries of Section 702-

acquired information designed to return evidence of a crime unrelated to foreign intelligence ("[redacted] Notice"), at 2. In an effort to identify additional evidence of abuse, the FBI ran queries of Section 702 information using the names of the suspected abuser, the apparent victims, and other terms derived from that e-mail message. Those queries only retrieved the previously reviewed e-mail message from which the query terms were derived. Id. Pursuant to Section I.F of its minimization procedures, the FBI disseminated information about the child abuse to a local child protective services agency, [redacted] Id.

The undersigned judge finds persuasive the November 6, 2015 Opinion's analysis of the FBI's querying rules. The single reported instance of queries that returned U.S. person information unrelated to foreign intelligence information does not detract from that analysis, especially since those queries did not result in any further intrusion on privacy: they merely retrieved information already known to the analyst who ran the queries.[53]

For the reasons stated above, neither the NCTC's receipt of unminimized information acquired regarding counterterrorism targets, subject to its applying the NCTC Minimization Procedures, nor the other above-described modifications to the targeting and minimization procedures, causes the Court to deviate from prior assessments that the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

---

[53] The Court notes, however, that the FBI did not identify those queries as responsive to the Court's reporting requirement until NSD asked whether any such queries had been made in the course of gathering information about the Section I.F dissemination. [redacted] Notice at 2. The Court is carrying forward this reporting requirement and expects the government to take further steps to ensure compliance with it.

IV. THE COMPLIANCE AND IMPLEMENTATION ISSUES REPORTED BY THE GOVERNMENT DO NOT WARRANT A FINDING THAT, AS IMPLEMENTED, THE TARGETING AND MINIMIZATION PROCEDURES ARE DEFICIENT.

The FISC has consistently understood its review of targeting and minimization procedures under Section 702 to include examining how the procedures have been and will be implemented. See, e.g., November 6, 2015 Opinion at 7; August 30, 2013 Opinion at 6-11, 19-22; April 7, 2009 Opinion at 22-25. As the Foreign Intelligence Surveillance Court of Review has noted, FISC "supervision of the execution of pen register orders further reduces the risk that such measures will be employed under circumstances, or in a manner, that unreasonably intrudes on individuals' privacy interests." In re Certified Question at 36-37. The same conclusion applies to FISC examination of how the government implements the Section 702 procedures.

For purposes of this examination, "the controlling norms are ones of reasonableness, not perfection," November 6, 2015 Opinion at 45, under both Section 702[54] and the Fourth Amendment.[55] The Court evaluates the reasonableness of "the program as a whole," not of individual actions in isolation. November 6, 2015 Opinion at 40-41. The assessment of

---

[54] See 50 U.S.C. § 1881a(d)(1) (requiring targeting procedures that are "reasonably designed to" limit targeting to "persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition" of communications to which all parties are known to be in the United States); § 1881a(e)(1) (requiring minimization procedures as defined in §§ 1801(h)(1) or 1821(4), i.e., procedures "reasonably designed" to minimize acquisition and retention, and to prohibit dissemination, of information concerning United States persons, consistent with foreign intelligence needs).

[55] See, e.g., United States v. Knights, 534 U.S. 112, 118 (2001) ("The touchstone of the Fourth Amendment is reasonableness . . . ."); In re Directives at 34 (surveillances found to be reasonable under the Fourth Amendment where "the risks of error and abuse are within acceptable limits and effective minimization procedures are in place").

reasonableness takes due account of the fact that implementing Section 702 is "a large and complex endeavor . . . effected through thousands of discrete targeting decisions for individual selectors,"[56] each of which implicates selector-specific pre-tasking and post-tasking requirements, November 6, 2015 Opinion at 45-46, and that for all information acquired under Section 702, minimization procedures impose "detailed rules concerning . . . retention, use, and dissemination . . . ." Id. at 46. As the FISC has previously observed:

> Given the number of decisions and volume of information involved, it should not be surprising that occasionally errors are made. Moreover, the government necessarily relies on [redacted] processes in performing post-tasking checks, see, e.g., August 30, 2013 Opinion at 7-9, and in acquiring, routing, storing, and when appropriate purging Section 702 information. See, e.g., April 7, 2009 Opinion at 17-22. Because of factors such as changes in communications technology or inadvertent error, these processes do not always function as intended.

Id.

Overall, the Court concludes that the targeting and minimization procedures satisfy applicable statutory requirements and are reasonable under the Fourth Amendment, despite the reported instances of non-compliance in prior implementation. The Court bases this conclusion in large measure on the extensive oversight conducted within the implementing agencies and by the DOJ and ODNI. Due to those efforts, it appears that compliance issues are generally

---

[56] For example, NSA "reports that, on average, approximately [redacted] facilities were under task at any given time between December 1, 2016 and February 28, 2017." March 17, 2016 Compliance Report at 1 (footnote omitted). Facilities tasked for acquisition include [redacted] Id. at 1 n.1. "Additionally, between December 1, 2016 and February 28, 2017, the [FBI] reports that it received and processed approximately [redacted] Id. at 1.

identified and remedied in a timely and appropriate fashion.[57] Nonetheless, the Court believes it beneficial to discuss certain ongoing or recent compliance issues and, in some cases, direct the government to provide additional information.

A. Resolution of Issues Addressed in the November 6, 2015 Opinion

The November 6, 2015 Opinion discussed several significant compliance problems that were then pending. See November 6, 2015 Opinion at 47-77. With the exception of non-compliance with minimization procedures related to attorney-client privileged communications, which are discussed separately, those compliance issues have been resolved as described below.

1. Failure of Access Controls in FBI's [redacted]

[redacted] while the 2015 Certifications were pending, the government filed a notice ("[redacted] Notice") indicating that a failure of access controls in an FBI database containing raw Section 702-acquired information resulted in [redacted] FBI employees improperly receiving access to such information. [redacted] Notice at 1. Specifically, [redacted]

[57] Too often, however, the government fails to meet its obligation to provide prompt notification to the FISC when non-compliance is discovered. See FISC Rule of Procedure 13(b). For example, it is unpersuasive to attribute – even "in part" – an eleven-month delay in submitting a preliminary notice to "NSA's efforts to develop remedial steps," see April 7, 2017 Preliminary Notice (Mislabeling) at 1 n.1, 2, when the purpose of a preliminary notice is to advise the Court while investigation or remediation is still ongoing. See also, e.g., February 28, 2017 Notice of a Compliance Incident Regarding Incomplete Purges of Information Obtained Pursuant to Multiple FISA Authorities ("February 28, 2017 Notice") at 1-2, n.3 (five-month delay attributed "to administrative issues surrounding the reorganization of NSA offices and personnel"). The Court intends to monitor closely the timeliness of the government's reporting of non-compliance regarding Section 702 implementation.

[redacted] allowed [redacted] users access to Section 702-acquired information, id., when only [redacted] were cleared for such access. Id. at 1, n.1. This resulted in violations of Sections III.A. and III.B of the FBI's minimization procedures.[58] The government provided testimony on this issue at a hearing on [redacted] filed a Supplemental Notice on [redacted] indicating that [redacted] FISA-acquired products were "exported" [redacted] users who were not authorized to access these products. [redacted] Notice at 2.

On [redacted], the government filed what was styled as a Final Notice on this issue [redacted] Notice"). That notice indicated that the FBI [redacted] had not disseminated the FISA-acquired products; and all [redacted] users had deleted from their systems the raw FISA-acquired information they had exported. [redacted]

[58] As then in effect and as now proposed, Section III.A of the FBI Minimization Procedures requires the FBI to "retain all FISA-acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with [the FBI Minimization Procedures] and other applicable FBI procedures." FBI Minimization Procedures § III.A. Section III.B of the FBI Minimization Procedures further requires the FBI to grant access to raw Section 702-acquired information in a manner that is "consistent with the FBI's foreign intelligence information-gathering and information-sharing responsibilities, . . . [p]ermitting access . . . only by individuals who require access in order to perform their job duties[.]" Id. § III.B. It also requires users with access to FISA-acquired information to receive training on minimization requirements. Id. § III.B.4.

[redacted] In the Court's assessment, the government has appropriately remedied this incident.

2. NSA Failures to Complete Required Purges

On July 13, 2015, the Government filed a notice regarding NSA's purge processes for FISA-acquired information in its mission management systems ("July 13, 2015 Notice"). That notice indicated that the NSA had not been removing records associated with Section 702 data subject to purge from its [redacted] database. July 13, 2015 Notice at 3.

On October 5, 2015, the government filed a Supplemental Notice regarding NSA's purge processes for FISA-acquired information ("October 5, 2015 Notice"). That notice indicated that NSA had now removed from [redacted] all Section 702-acquired records that were marked as subject to purge. October 5, 2015 Notice at 2. On October 28, 2015, however, the government filed another Supplemental Notice regarding NSA's purge processes ("October 28, 2015 Notice") in which it reported that a technical malfunction in [redacted] had rendered the aforementioned purges incomplete. October 28, 2015 Notice at 2.

On January 14, 2016, the government filed a Supplemental Notice ("January 14, 2016 Notice") indicating that as of October 30, 2015, [redacted] was properly configured to remove records subject to purge and corresponding to identifiers on the MPL. January 14, 2016

Notice at 2. At that time NSA had completed purging records that had been added to the MPL between 2011 and 2015. Id. On September 22, 2016, the government filed another Supplemental Notice ("September 22, 2016 Notice on [redacted] confirming that as of February 2016, the NSA had removed from [redacted] all historical Section 702-acquired records subject to purge.[59] September 22, 2016 Notice on [redacted] at 2.

The July 13, 2015 Notice also reported "a compliance incident regarding FISA-acquired information subject to purge or age off that [was] being retained in two of NSA's compliance mission management systems, [redacted] and [redacted] in a manner that is "potentially inconsistent with NSA's FISA-related minimization procedures." July 13, 2015 Notice at 2, 5. Subsequent communications between the government and FISC staff revealed that [redacted] and [redacted] may also have been retaining data, the use or disclosure of which could violate 50 U.S.C. § 1809(a)(2). The November 6, 2015 Opinion directed the government to provide additional information about NSA's retention of certain categories of information in [redacted] and [redacted] November 6, 2015 Opinion at 78.

On December 18, 2015, the government filed a detailed description of its plan and timeline for remedying improper retention in [redacted] and [redacted] See Prior 702 Dockets, Verified Response to the Court's Order Dated November 6, 2015, filed on Dec. 18,

[59] The government also disclosed in the January 14, 2016 Notice that [redacted] was not configured to age off all FISA-acquired information pursuant to relevant minimization procedures. January 14, 2016 Notice at 2. As of August 3, 2016, the NSA had removed from [redacted] all Section 702-acquired information identified as due for destruction under the retention periods set by the NSA Minimization Procedures, and prospectively, the NSA will remove Section 702-acquired information from [redacted] in compliance with those retention periods. September 22, 2016 Notice on [redacted] at 2.

2015. On September 22, 2016, the government provided a written update on the NSA's efforts to remove from [redacted] and [redacted] information that was subject to purge or age-off under the NSA Minimization Procedures ("September 22, 2016 Notice on [redacted] and [redacted] As of February 17, 2016, NSA had removed from [redacted] and [redacted] all Section 702-acquired information subject to age-off under the five- and two-year retention periods set by the NSA Minimization Procedures. September 22, 2016 Notice on [redacted] and [redacted] at 2. As of September 9, 2016, the NSA had deleted from [redacted] and [redacted] all historical Section 702-acquired data potentially subject to § 1809(a)(2), and it had developed a plan to deal prospectively with information potentially subject to § 1809(a)(2). Id. at 3. Finally, as of September 9, 2016, the NSA had removed from [redacted] and [redacted] other categories of information that the November 6, 2015 Opinion had identified as not permissible for retention in [redacted] and [redacted] (e.g., attorney-client communications that do not contain foreign intelligence information or evidence of a crime). Id. at 3-4.

B. Issues Arising Under the NSA Targeting Procedures

NSA's targeting procedures require that analysts, before tasking a selector for acquisition, make a reasonable assessment that the user of the selector is a non-U.S. person located outside the United States. See NSA Targeting Procedures § 1. Post-tasking, analysts are required to take reasonable steps to confirm that the selector continues to be used by a non-U.S. person located outside the United States. See NSA Targeting Procedures § 2. Those requirements directly bear on statutory limitations on Section 702 acquisitions. See 50 U.S.C. § 1881a(c)(1)(A), (d)(1)(A)

(targeting procedures must be reasonably designed to ensure that acquisitions are limited to targeting persons reasonably believed to be outside the United States); § 1881a(b)(3), (4) (government may not intentionally target a United States person reasonably believed to be outside the United States or intentionally acquire any communication as to which the sender and all intended recipients are known at time of acquisition to be in the United States).

Compliance and implementation issues have arisen regarding these pre-tasking assessments and post-tasking reviews. While those issues merit discussion, the Court does not believe they are sufficiently serious or pervasive to warrant finding that the targeting procedures do not meet the above-described statutory requirements or are inconsistent with the Fourth Amendment.

1. Scope of Pre-Tasking Review of [redacted]

One of the measures taken by NSA analysts to fulfill pre-tasking obligations is to check [redacted] for information that may be probative of [redacted] For example, [redacted].

According to a notice filed by the government on August 24, 2016, NSA analysts often relied on the above-referenced [redacted] tool to [redacted] as part of those pre-tasking checks. August 24, 2016 Update Regarding the Scope of Section 702 Pre-Tasking Review of [redacted] at 2 ("August 24, 2016 Update"). The data returned [redacted] was

limited, as [redacted] only [redacted] Id. In certain circumstances, the results from [redacted] could have provided an incomplete and misleading impression of [redacted]. The government acknowledges that the sufficiency of running a [redacted] as the sole basis for a pre-tasking assessment "depends upon the information known about the target from other sources and the nature of the information returned by the [redacted] Id. Subsequent investigation revealed [redacted] instances of improper taskings. See August 24, 2016 Update at 2, n.2. NSA placed on its MPL information obtained as a result of these taskings. Id. at 2.[60]

NSA has developed a new tool for analysts to use for pre-tasking checks [redacted] August 24, 2016 Update at 4. "In addition to [redacted], NSA's new tool is also [redacted] that will greatly enhance analysts' pre-tasking reviews." Id.

[60] For discussion of the government's processes for purging Section 702 information, see March 17, 2017 Compliance Report at 2-5.

While the described functionality of the new tool improves on some of the limitations of [redacted] it should not be seen as a panacea. In the Court's view, the fundamental cause of these improper taskings was not the limitations of [redacted] or other [redacted] tools, but rather the failure of analysts in these particular cases to pursue reasonable lines of inquiry regarding [redacted] See, e.g., August 24, 2016 Update at 3 [redacted]. It remains the obligation of analysts to exercise due diligence in the particular circumstances of each pre-tasking review, rather than to presume that using a given [redacted] tool or protocol will suffice. The government acknowledges that sometimes, after deploying the new tool, "additional research will be necessary to satisfy the totality of the circumstances test [for pre-tasking reviews] contained in the NSA Targeting Procedures," id. at 5, and addresses in its training efforts how NSA analysts should understand and comply with this requirement. See October 4, 2016 Transcript at 19-20.

2. Frequency of Post-Tasking Review of Contents

While the government did not report the following information as involving non-compliance with the NSA's targeting procedures, the Court believes it bears significantly on how those procedures are implemented and therefore merits discussion.

The NSA's targeting procedures do not require analysts to review the contents of communications acquired from tasking a particular selector at fixed intervals. Instead, they provide that such content review "will be conducted according to analytic and intelligence

requirements and priorities." See, e.g., NSA Targeting Procedures § II at 6.[61] As previously described to the FISC, however, NSA follows a policy whereby such content review is performed no later than [redacted] days after the first acquisition and at intervals of no more than [redacted] days thereafter. See September 13, 2016, Update Regarding Post-Targeting Content Reviews ("September 13, 2016 Update") at 2; Docket No. [redacted], Memorandum Opinion at 9-10 (FISA Ct. Oct. 24, 2014).

NSA and FBI analysts with access to Section 702 data are trained on this policy, while CIA analysts receive training that "is consistent with" the policy and are instructed "to review content as it is acquired." September 13, 2016 Update at 3.[62] According to a supplemental letter filed on March 13, 2017 ("March 13, 2017 Supp. Letter"), the government monitors compliance with the policy with regard to Section 702 data in an NSA repository called [redacted] but otherwise does not comprehensively monitor or verify whether analysts in fact conduct content reviews in conformance with that policy. March 13, 2017 Supp. Letter at 2.[63] For that reason,

---

[61] This content review is in addition to other post-tasking steps to ascertain whether a tasked facility is being used inside the United States, such as [redacted] Id. § II at 6-7.

[62] [redacted] See NSA Targeting Procedures § 2 at 7 n. 2-3.

[63] NSA routes most forms of Internet communications acquired under Section 702 to a repository called [redacted] March 13, 2017 Supp. Letter at 2. For review of communications in [redacted] NSA has [redacted] that monitors whether content checks are performed, sends prompts to analysts to conduct [redacted] and [redacted] reviews, and sends overdue notices. Id. at 1-2. NSA does not have such an alert system for other repositories containing (continued...)

deviations from the policy may not be detected unless and until the circumstances are examined for other purposes. See September 13, 2016 Update at 3.

To address this concern, the government undertakes "to notify the Court . . . when, in connection with compliance incidents, the government also learns that content was not reviewed in accordance with the applicable policy." Id. at 4. The government further undertakes to advise the FISC "of the total number of instances in which the government's investigation into a potential [non-compliance] incident revealed that content review was not timely conducted in accordance with [this policy]," even if the government determines that, strictly speaking, there was no violation of the targeting procedures themselves. See id. That figure will be included in each of the government's quarterly compliance reports. Id.

On March 13, 2017, the government reported the results of an examination of the performance of [redacted] and [redacted] content reviews for data in [redacted] during January-March 2016. March 13, 2017 Supp. Letter at 2. That examination revealed a compliance rate of approximately 79% for [redacted] reviews and 99% for [redacted] reviews. Id. NSA plans to issue an advisory to personnel reminding them of the policy. Id. at 3.

The Court intends to scrutinize the information submitted regarding future deviations from this policy. It also encourages the government to explore further measures, through

---

[63](...continued)
Section 702 information, though it has plans to develop systems for additional repositories by the end of 2017. Id. at 2-3. FBI and CIA do not have comparable systems. October 4, 2016 Transcript at 21, 24.

[redacted] processes or otherwise, to prompt analysts to conduct content reviews in accordance with this policy, and to monitor or verify adherence to it.

C. Issues Arising Under the NSA Minimization Procedures

In addition to the improper use of U.S.-person identifiers to query the results of upstream Internet data discussed above, noteworthy compliance issues have arisen with regard to NSA's upstream collection of Internet communications and querying of Section 702-acquired data.

1. NSA Upstream Collection of Internet Communications

Under the pre-2017 Amendments version of the NSA Minimization Procedures, NSA is required to "take reasonable steps post-acquisition to identify and segregate through technical means" those MCTs that are particularly likely to involve communicants in the United States; specifically, those for which "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." NSA Minimization Procedures § 3(b)(4)a. (prior to the 2017 Amendments). Those procedures permit only certain 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" to access MCTs that have been segregated in the manner described above. § 3(b)(4)a.2. Information in a segregated MCT "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." § 3(b)(4)a.2.(a).[64]

Starting in April 2015, a [redacted] error affected NSA's upstream collection [redacted] See September 30, 2016 Supplemental Notice of Compliance Incident Regarding Collection Pursuant to Section 702 ("September 30, 2016 Supp. Notice") at 1. The error was discovered on January 26, 2016, and corrected on a going-forward basis the next day. Id.

This [redacted] error led to two types of compliance problems. First, it resulted in the unauthorized acquisition of Internet "communications from facilities that only partially matched authorized Section 702 [selectors] (e.g., [redacted]" Id. at 1-2. It appears that the government has taken appropriate steps to identify and purge the improperly acquired information. Id. at 2-3. NSA has positively identified [redacted] "data objects" as having been subject to this over-collection. Id. In addition, based on the nature of the [redacted] error and the technical characteristics of information likely to have been improperly collected due to the error, NSA has identified in excess of [redacted] "data objects" that may have been over-collected. Id. at 3. Because it was not technically feasible for NSA to identify within that set any and all objects that actually had been over-collected, NSA has put [redacted]-plus objects, as well as the [redacted] objects positively identified as having been over-collected, on its MPL. Id.; see also March 17, 2017 Quarterly Report at 114-15.

[64] In practice, however, no analysts received the requisite training in order to work with the segregated MCTs. October 4, 2016 Transcript at 41-43.

Second, the [redacted] error resulted in failures in the technical processes whereby NSA identified MCTs that are subject to the segregation regime described above. Specifically, some MCTs may have been wrongly identified and labeled as ones in which the active user was the target, which would have resulted in those MCTs not being segregated. September 30, 2016 Supp. Notice at 3-4. To the extent wrongly-identified MCTs were actually ones for which the active user is reasonably believed to have been located in the United States or for whom the active user's location was unknown, they should have been segregated and subject to the above-described heightened access controls. Any large-scale failure to identify and segregate MCTs subject to those heightened access controls would have threatened to undermine one of the safeguards on which the FISC relied in 2011 when it approved the procedures adopted by the government in response to the FISC's prior finding of deficiency. See November 30, 2011 Opinion at 11-15.

The Court did not find entirely satisfactory the government's explanations of the scope of those segregation errors and the adequacy of its response to them and addressed some of its concerns at the October 4, 2016 Hearing. See, e.g., October 4, 2016 Transcript at 35-38.[65] Questions about the adequacy of steps previously taken to respond to the errors, however, are no longer material to the Court's review of the NSA Minimization Procedures. Under the revised

[65] The government later reported it had inadvertently misstated the percentage of NSA's overall upstream Internet collection during the relevant period that could have been affected by this [redacted] error (the government first reported the percentage as roughly 1.3%, when it was roughly 3.7%). April 11, 2017 Notice of Material Misstatement and Supplemental Notice of Compliance Incidents Regarding Collection Pursuant to Section 702 at 2.

NSA Minimization Procedures, the results of upstream Internet collection during the relevant timeframe must be segregated and destroyed.

2. Improper Querying [redacted] Communications

U.S. person identifiers may be used to query Section 702 data only if they are first "approved in accordance with [internal] NSA procedures, which must require a statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information." NSA Minimization Procedures § 3(b)(5).[66] In performing such queries, NSA analysts sometimes use a tool called "[redacted] can be used to query data repositories, including one called [redacted] September 30, 2016 Final Notice of Compliance Incidents Regarding Improper Queries ("September 30, 2016 Final Notice") at 1. [redacted] communications acquired pursuant to Section 702, as well as other FISA authorities. Id.

In May and June 2016, NSA reported to oversight personnel in the ODNI and DOJ that, since approximately 2012, use of [redacted] to query communications in [redacted] had resulted in inadvertent violations of the above-described querying rules for Section 702 information. Id. The violations resulted from analysts not recognizing the need to avoid querying datasets for which querying requirements were not satisfied or not understanding how to formulate [redacted] queries to exclude such datasets. Id. at 1-2.

---

[66] As previously noted, NSA may not use U.S.-person identifiers to query the results of upstream Internet collection until the 2017 Amendments take effect, but will be able to run such queries of the narrower form of upstream Internet collection contemplated under the 2017 Amendments, subject to the approval process described above.

NSA examined all queries using identifiers for "U.S. persons targeted pursuant to Sections 704 and 705(b) of FISA using the [redacted] tool in [redacted] . . . from November 1, 2015 to May 1, 2016." Id. at 2-3 (footnote omitted). Based on that examination, "NSA estimates that approximately eighty-five percent of those queries, representing [redacted] queries conducted by approximately [redacted] targeted offices, were not compliant with the applicable minimization procedures." Id. at 3. Many of these non-compliant queries involved use of the same identifiers over different date ranges. Id. Even so, a non-compliance rate of 85% raises substantial questions about the propriety of using of [redacted] to query FISA data. While the government reports that it is unable to provide a reliable estimate of the number of non-compliant queries since 2012, id., there is no apparent reason to believe the November 2015-April 2016 period coincided with an unusually high error rate.

The government reports that NSA "is unable to identify any reporting or other disseminations that may have been based on information returned by [these] non-compliant queries" because "NSA's disseminations are sourced to specific objects," not to the queries that may have presented those objects to the analyst. Id. at 6. Moreover, [redacted] query results are generally retained for just [redacted] Id.[67]

The NSA has taken steps to educate analysts on the proper use of [redacted] it has provided a "reminder" to all analysts about the need "to limit queries across authorities in [redacted] with

[67] Information retrieved by an improper query might nonetheless satisfy the requirements for dissemination; indeed, absent a second violation of the minimization procedures, separate from the improper query, one would expect any disseminated information to have satisfied those requirements.

an explanation of how different types of queries operate; it issued a separate "Compliance Advisory," which further addressed querying practices using [redacted] to all NSA target offices; and it revised a "banner" presented to users of [redacted] to emphasize that U.S. person identifiers should never be used for a type of query (called a "selector query") that runs "against all data [that] an analyst is authorized to access." Id. at 1, 6.

At the October 4, 2016 Hearing, the government represented that, based on ongoing oversight efforts, those measures appear to have been effective in improving how analysts use [redacted] to query Section 702 data. October 4, 2016 Transcript at 47-49. On April 3, 2017, the government reported to the Court that it had reaffirmed that assessment, based on discussions with NSA analysts and the absence of additional non-compliant queries using [redacted] April 3, 2017, Supplemental Notice of Compliance Incidents Regarding Improper Queries, at 3. In view of these remedial steps, the Court believes that, notwithstanding the above-described non-compliance, the NSA Minimization Procedures meet the statutory definition of "minimization procedures" and are consistent with the requirements of the Fourth Amendment.

D. Issues Arising Under the FBI Minimization Procedures

The following violations of the FBI's minimization procedures merit discussion.

1. Improper Disclosures of Raw Information

On March 9, 2016, DOJ oversight personnel conducting a minimization review at the FBI's [redacted] learned that the FBI had disclosed raw FISA information, including but not limited to Section 702-acquired information, to a [redacted] Compliance Report at 92. [redacted] is part of the [redacted]

[redacted] and "is largely staffed by private contractors" [redacted] certain [redacted] contractors had access to raw FISA information on FBI storage systems [redacted] Id. The apparent purpose for the FBI's granting such access was to receive analytical assistance from [redacted] Nonetheless, the [redacted] contractors had access to raw FISA information that went well beyond what was necessary to respond to the FBI's requests; [redacted] The FBI discontinued the above-described access to raw FISA information as of April 18, 2016. [redacted]

The contractors in question received training on the FBI minimization procedures, stored the raw information only on FBI systems, and did not disseminate it further. Id. at 93. Nonetheless, the above-described practices violated the governing minimization procedures. Section III.A of the FBI's minimization procedures (as then in effect and as now proposed) provides: "The FBI must retain all FISA-acquired information under appropriately secure conditions that limit access to such information only to authorized users in accordance with these and other applicable FBI procedures. These retention procedures apply to FISA-acquired information retained in any form." The FBI may disseminate Section 702-acquired information only in accordance with Section V of those procedures. FBI Minimization Procedures § III.C.1.

Under Section V.D of those procedures, personnel working for another federal agency such as [redacted] may receive raw information acquired under Section 702 in order to

provide technical or linguistic assistance to the FBI, but only if certain restrictions are followed. See id. § V.D. Those restrictions were not in place with regard to the [redacted] contractors: their access was not limited to raw information for which the FBI sought assistance and access continued even after they had completed work in response to an FBI request. See [redacted] Compliance Report at 93. At the October 4, 2016 Hearing, the government represented that it was investigating whether there have been similar cases in which the FBI improperly afforded non-FBI personnel access to raw FISA-acquired information on FBI systems. October 4, 2016 Transcript at 64.

In a separate violation of its minimization procedures, the FBI delivered raw Section 702-acquired information to a [redacted] contractor called [redacted] Compliance Report at 131. The information in question pertains to [redacted] accounts tasked under Section 702. Id. [redacted] as a federal agency, could receive raw Section 702-acquired information in order to provide technical assistance to the FBI, subject to the requirements of Section V.D of the FBI Minimization Procedures. See FBI Minimization Procedures § V.D ("FBI is authorized to

disclose FISA-acquired information to assisting federal agencies for further processing and analysis," subject to specified restrictions) (emphasis added). [redacted] however, is not a federal agency and the [redacted] personnel who worked with the information were "not directly supervised by or otherwise under the direction and control of [redacted] Compliance Report at 132. For these reasons, the government concluded that the FBI had given the information to the private entity [redacted], not to an assisting federal agency. See id.[68]

[redacted] The government has not explained why giving [redacted] personnel access to the raw information during installation of the tool would not involve a separate violation of the FBI Minimization Procedures. Accordingly, the Court is ordering the government to provide additional information regarding this second grant of access to raw Section 702 information.

These violations, when placed in the context of Section 702 acquisitions in their entirety, do not preclude a finding that the FBI Minimization Procedures meet the statutory definition of "minimization procedures" and are consistent with the requirements of the Fourth Amendment.

---

[68] In contrast, the above-described [redacted] contractors worked in a federal facility under the supervision of [redacted] Compliance Report at 93. It appears that the government views the above-described disclosures of information to the [redacted] contractors as disclosures to a federal agency, rather than to a private entity or private individuals. In any event, the government acknowledges that those disclosures were improper for other reasons, so the Court need not reach this question.

The improper access previously afforded the [redacted] contractors has been discontinued, while the information disclosed to [redacted] pertains to just [redacted] tasked selectors.

The Court is nonetheless concerned about the FBI's apparent disregard of minimization rules and whether the FBI may be engaging in similar disclosures of raw Section 702 information that have not been reported.[69] Accordingly, the Court is directing the government to provide additional as described below.

2. Potential Over-Retention of Section 702 Information

Last year, in the context of approving the standard minimization procedures employed by the FBI for electronic surveillance and physical search conducted under Titles I and III of FISA, a judge of the FISC observed:

> FBI personnel who develop storage systems for FISA-acquired information and decide under what circumstances FISA-acquired information is placed on those systems are bound by applicable minimization procedures and FISC orders, no less so than an agent conducting a FISC-authorized physical search or an analyst preparing a report for dissemination.

Docket No. [redacted], Opinion and Order at 45 (FISA Ct. May 17, 2016). Recent disclosures regarding [redacted] systems maintained by the FBI suggest that raw FISA

[69] The improper access granted to the [redacted] contractors was apparently in place [redacted] and seems to have been the result of deliberate decisionmaking. [redacted] Compliance Report at 92-93 ([redacted] access to FBI systems was the subject of an interagency memorandum of understanding entered into [redacted]). Despite the existence of an interagency memorandum of understanding (presumably prepared or reviewed by FBI lawyers), no notice of this practice was given to the FISC until 2016. Of course, such a memorandum of understanding could not override the restrictions of Section 702 minimization procedures.

information, including Section 702 information, may be retained on those systems in violation of applicable minimization requirements. [redacted][70]

[redacted]

The government has not identified the provisions of the FBI Minimization Procedures it believes are implicated by the above-described retention practices. Based on the information

70 [redacted]

provided, however, those practices appear inconsistent with the provisions governing retention on electronic and data storage systems, see FBI Minimization Procedures § III.G.1, on ad hoc systems, id. § IV.A-B, and in connection with litigation, id. § III.G.4. Nearly four months ago, the government undertook to address this indefinite retention of information on the above-described systems in a subsequent filing, see December 29, 2016 Report at 10-11, but has not done so. Accordingly, the Court is directing the government to provide pertinent information, as described below.

3. Review Teams for Attorney-Client Communications

The Section 702 minimization procedures

> have specific rules for handling attorney-client communications. Because the FBI has law enforcement responsibilities and often works closely with prosecutors in criminal cases, its procedures have detailed requirements for cases in which a target is known to be charged with a federal crime. Unless otherwise authorized by the [National Security Division of DOJ], the FBI must establish a separate review team whose members have no role in the prosecution of the charged criminal matter to conduct the initial review of such a target's communications. When that review team identifies a privileged communication concerning the charged criminal matter, the original record or portion thereof containing that privileged communication is sequestered with the FISC and other copies are destroyed (save only any electronic version retained as an archival backup, access to which is restricted).

November 6, 2015 Opinion at 47-48 (citations and internal quotation marks omitted).

Failures of the FBI to comply with this "review team" requirement for particular targets have been a focus of the FISC's concern since 2014. See id. at 48-52; August 26, 2014 Opinion at 35-36. The government generally ascribed those failures to misunderstanding or confusion on the part of individuals – for example, when an agent is generally aware of the review team requirement but mistakenly believes that it does not apply when the charging instrument is under

seal. November 6, 2015 Opinion at 50. The government advised that it was emphasizing the review team requirement in ongoing training and oversight efforts, and that such emphasis had resulted in the identification and correction of additional cases in which review teams had not been properly established. Id. at 51.

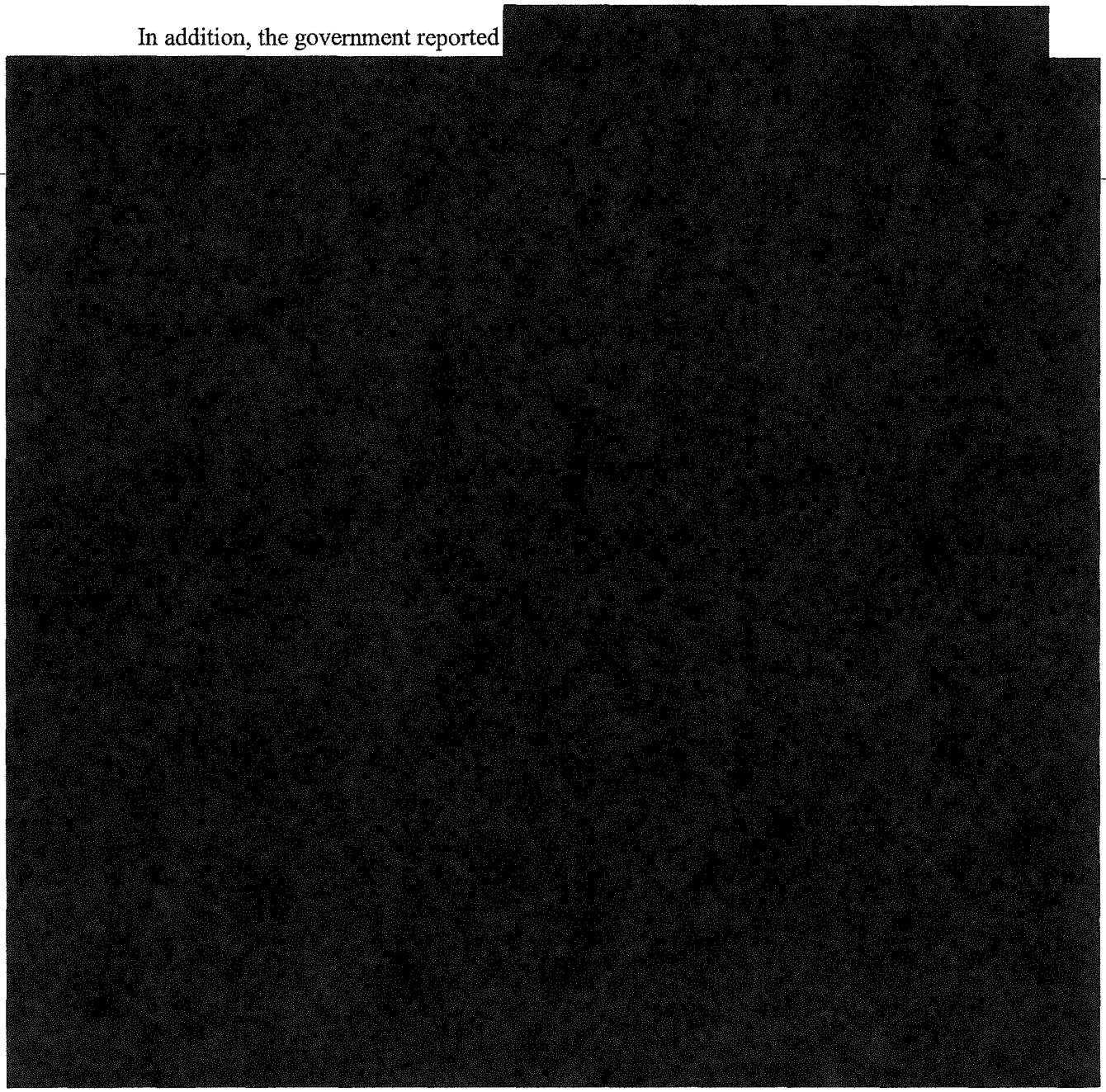
[redacted] targets who have been subject to criminal charges [redacted] there was a delay of over two years in establishing review teams. See [redacted] Preliminary Notice of Compliance Incident Regarding [redacted] Section 702-Tasked Facilities ("[redacted] Preliminary Notice") at 2-3. The primary cause of this delay was that the responsible case agent was unaware of the review team requirement. That agent took the appropriate steps after reviewing an advisory that reminded FBI personnel about the requirement in [redacted] Id. at 3.[71] The government also reported a delay of approximately one month during [redacted] before establishing a review team after a target was charged in a sealed complaint. The delay appears to have been the result of lack of coordination among FBI field offices. According to the government, the review teams have completed examination of communications acquired prior to

[redacted]

their creation for both incidents and did not discover any privileged communications. [redacted]

[redacted] Compliance Report at 77, 105.

In addition, the government reported [redacted]



[redacted]

A separate source of under-inclusiveness is when personnel do not identify and segregate communications for [redacted]

[redacted] FBI examination of the erroneously-excluded communications is ongoing and, so far, has not identified any attorney-client privileged communications concerning a charged matter. [redacted] Compliance Report at 119.

A different [redacted] problem affected [redacted] accounts during November 28-30, 2016. That problem has been solved prospectively. Although some communications for

those tasked accounts were accessed before being segregated for the review team, none of them contained privileged information. Id. at 83 n.58.

In order to address some of the sources of such under-inclusiveness, the FBI has implemented a new [redacted] process for [redacted] [redacted] In addition, the FBI and NSA have taken steps to address the difficulties encountered with regard to [redacted] Id. at 4.

It seems clear that the review team requirement should continue to be a point of emphasis in the government's training and oversight efforts. The measures taken to improve processes for identifying and routing information subject to the review team requirement appear well-suited to address the described under-inclusiveness problems. In view of those efforts, and the fact that lapses to date appear to have resulted in few, if any, privileged communications concerning charged matters being reviewed by investigators other than review team members, errors in implementing the review team requirements do not preclude a finding that the FBI Minimization Procedures meet the statutory definition of "minimization procedures" and are consistent with the requirements of the Fourth Amendment.

E. Issues Arising Under the CIA Minimization Procedures

In the course of investigating a separate compliance incident that occurred in December 2016,[72] the CIA discovered several problems with its purge practices. First, the software script used to identify communications subject to purge requirements within a storage system [redacted] had not been identifying all communications subject to purge that had been acquired by [redacted] December 28, 2016, Preliminary Notice of Compliance Incidents and Material Misstatements Regarding Collection Pursuant to Title I and Title III and Section 702 of FISA, at 4. As of March 29, 2017, CIA was in the process of remedying the incomplete purges. Supplemental Notice Regarding Incomplete Purges of Collection Acquired Pursuant to Section 702 of FISA, filed on March 29, 2017 ("March 29, 2017 Supp. Notice") at 2.

Further investigation of the December 2016 incident revealed similar problems with scripts used to purge metadata from [redacted] CIA repositories [redacted]. March 29, 2017 Supp. Notice at 2-3. The government reports CIA has corrected those script problems and completed the required purges, except for certain information relating [redacted] facilities, for which remedial efforts are ongoing. Id. at 3 & n.4.

[72] That incident appears to have been remedied, see id. at 3, and in and of itself does not merit discussion in this Opinion.

[73] [redacted]

In late March 2017, also in the course of investigating the December 2016 incident, CIA discovered another form of purging error affecting [redacted] March 24, 2017, Notice of Compliance Incident Regarding Incomplete Age Off of Data Acquired Pursuant to Section 702 of FISA at 2. The government is examining the scope of that error. Id.

The government has not advised the Court for how long these various purge-related problems persisted before CIA discovered them in the course of investigating the separate incident. It appears that, having recognized the problems, CIA is taking reasonable steps to address them. Nonetheless, the Court encourages the government to take proactive measures to verify that the automated processes upon which it relies to implement minimization requirements are functioning as intended.

V. CONCLUSION

For the foregoing reasons, the Court finds that: (1) the 2016 Certifications, as amended by the 2017 Amendments, as well as the certifications in the Prior 702 Dockets as amended by those documents, contain all the required statutory elements; (2) the targeting and minimization procedures to be implemented regarding acquisitions conducted pursuant to the 2016 Certifications, as amended by the 2017 Amendments, comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment; and (3) the minimization procedures to be implemented regarding information acquired under prior Section 702 certifications comply with 50 U.S.C. §1881a(d)-(e) and are consistent with the requirements of the Fourth Amendment. Orders approving the amended certifications and use of the accompanying procedures are being entered contemporaneously herewith.

For the reasons discussed above, it is HEREBY ORDERED as follows:

1. Raw information obtained by NSA's upstream Internet collection under Section 702 shall not be provided to FBI, CIA or NCTC unless it is done pursuant to revised minimization procedures that are adopted by the AG and DNI and submitted to the FISC for review in conformance with Section 702.

2. The government shall take steps to ensure that NCTC retains raw Section 702-acquired information that is determined to be evidence of a crime but not foreign intelligence information beyond the generally applicable age-off period specified in Section B.2 of the NCTC Minimization Procedures only as long as reasonably necessary to serve a law enforcement purpose and that NCTC does not use or disclose such information other than for a law enforcement purpose. The government shall report in writing on such steps when it seeks to renew or amend [redacted].

3. On or before December 31 of each calendar year, the government shall submit a written report to the FISC: (a) describing all administrative, civil or criminal litigation matters necessitating preservation by FBI, NSA, CIA or NCTC of Section 702-acquired information that would otherwise be subject to destruction, including the docket number and court or agency in which such litigation matter is pending; (b) describing the Section 702-acquired information preserved for each such litigation matter; and (c) describing the status of each such litigation matter.

4. The government shall promptly submit a written report describing each instance in which FBI, NSA, CIA or NCTC invokes the provision of its minimization procedures stating that

nothing in those procedures shall prohibit the "retention, processing, analysis or dissemination of information necessary to comply with a specific congressional mandate or order of a court within the United States[.]" See NSA Minimization Procedures § 1; CIA Minimization Procedures § 6.g; FBI Minimization Procedures § I.G; NCTC Minimization Procedures § A.6.d. Each such report shall describe the circumstances of the deviation from the procedures and identify the specific mandate on which the deviation was based.

5. The government shall promptly submit a written report describing any instance in which an agency departs from any provision in its minimization procedures in reliance in whole or in part on the provision therein for lawful oversight when responding to an oversight request by an entity other than the oversight entities expressly referenced in the agency's procedures. See NSA Minimization Procedures § 1; CIA Minimization Procedures § 6.f; FBI Minimization Procedures § I.G; NCTC Minimization Procedures § A.6.e. Each such report shall describe the circumstances of the deviation from the procedures and identify the specific oversight activity on which the deviation was based.

6. No later than June 16, 2017, the government shall submit a written report:

(a) describing the extent to which raw FISA information, including Section 702 information, is retained:



(b) assessing whether such retention complies with applicable minimization requirements; and

(c) to the extent that noncompliance is found, describing the steps the government is taking or plans to take to discontinue the above-described forms of retention or bring them into compliance with applicable minimization requirements.

7. No later than June 16, 2017, the government shall submit one or more written reports that provide the following:

(a) the results of the government's investigation of whether there have been additional cases in which the FBI improperly afforded non-FBI personnel access to raw FISA-acquired information on FBI systems; and

(b) a description of the installation of the [redacted] by [redacted] personnel on an FBI system, including:

[redacted]

8. At 90-day intervals, the government shall submit written updates on NSA's implementation of the above-described sequester-and-destroy process to information acquired on or before March 17, 2017, by upstream Internet collection under Section 702.

9. If the government intends not to apply the above-described sequester-and-destroy process to information acquired on or before March 17, 2017, by upstream Internet collection

under Section 702 because the information is not contained in an "institutionally managed repository," it shall describe the relevant circumstances in a written submission to be made no later than June 2, 2017; however, the government need not submit such a description for circumstances referenced in this Opinion and Order as ones in which NSA could retain such information.

10. The government shall promptly submit in writing a report concerning each instance in which FBI personnel receive and review Section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information. The report should include a detailed description of the information at issue and the manner in which it has been or will be used for analytical, investigative or evidentiary purposes. It shall also identify the query terms used to elicit the information and provide the FBI's basis for concluding that the query was consistent with applicable minimization procedures.

ENTERED this 26 day of April, 2017, in Docket Nos. [redacted].

ROSEMARY M. COLLYER
Judge, United States Foreign
Intelligence Surveillance Court

I, [redacted], Chief Deputy Clerk, FISC, certify that this document is a true and correct copy of the original.

[redacted]

DECLARATION OF SCOTT BRADNER

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

Appendix F

Privacy and Civil Liberties Oversight Board

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014



PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

JULY 2, 2014

Privacy and Civil Liberties Oversight Board

David Medine, Chairman

Rachel Brand

Elisebeth Collins Cook

James Dempsey

Patricia Wald

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

Part 1 INTRODUCTION 1

Part 2 EXECUTIVE SUMMARY 5

Part 3 DESCRIPTION AND HISTORY 16

Genesis of the Section 702 Program 16

Statutory Structure 20

Acquisition Process 32

Targeting Procedures 41

Post-Tasking Review 48

Minimization Procedures 50

Internal Agency Oversight 66

External Oversight 70

Compliance Issues 77

Part 4 LEGAL ANALYSIS 80

Statutory Analysis 80

Constitutional Analysis 86

Analysis of Treatment of Non-U.S. Persons 98

Part 5 POLICY ANALYSIS 103

Value of the Section 702 Program 104

Privacy and Civil Liberties Implications of the Section 702 Program 111

Part 6 RECOMMENDATIONS 134

Part 7 CONCLUSION 149

ANNEXES 150

A. Separate Statement by Chairman David Medine and Board Member Patricia Wald 151

B. Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook 161

C. July 9, 2013 Workshop Agenda and Link to Workshop Transcript 166

D. November 4, 2013 Hearing Agenda and Link to Hearing Transcript 169

E. March 19, 2014 Hearing Agenda and Link to Hearing Transcript 172

F. Request for Public Comments on Board Study 175

G. Reopening the Public Comment Period 177

H. Index to Public Comments on www.regulations.gov 178

Part 1:

INTRODUCTION

I. Background

Shortly after the Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board") began operation as a new independent agency, Board Members identified a series of programs and issues to prioritize for review. As announced at the Board's public meeting in March 2013, one of these issues was the implementation of the Foreign Intelligence Surveillance Act Amendments Act of 2008.[1]

Several months later, in June 2013, two classified National Security Agency ("NSA") collection programs were first reported about by the press based on unauthorized disclosures of classified documents by Edward Snowden, a contractor for the NSA. Under one program, implemented under Section 215 of the USA PATRIOT Act, the NSA collects domestic telephone metadata (i.e., call records) in bulk. Under the other program, implemented under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), the government collects the contents of electronic communications, including telephone calls and emails, where the target is reasonably believed to be a non-U.S. person[2] located outside the United States.

A bipartisan group of U.S. Senators asked the Board to investigate the two NSA programs and provide an unclassified report.[3] House Minority Leader Nancy Pelosi subsequently asked the Board to consider the operations of the Foreign Intelligence Surveillance Court ("FISA court").[4] Additionally, the Board met with President Obama, who asked the Board to "review where our counterterrorism efforts and our values come into

---

1 *See* Privacy and Civil Liberties Oversight Board, Minutes of Open Meeting of March 5, 2013, at 4-5, *available at* http://www.pclob.gov/SiteAssets/meetings-and-events/5-march-2013-public-meeting/5%20March%202013%20Meeting%20Minutes.pdf.

2 Under the statute, the term "U.S. persons" includes United States citizens, United States permanent residents, and virtually all United States corporations.

3 Letter from Tom Udall *et al*. to the Privacy and Civil Liberties Oversight Board (June 12, 2013), *available at* http://www.pclob.gov/SiteAssets/newsroom/6.12.13%20Senate%20letter%20to%20PCLOB.pdf. Response *available at* http://www.pclob.gov/SiteAssets/newsroom/PCLOB_TUdall.pdf.

4 Letter from Democratic Leader Nancy Pelosi to Chairman David Medine (July 11, 2013), *available at* http://www.pclob.gov/SiteAssets/newsroom/Pelosi%20Letter%20to%20PCLOB.pdf. Response *available at* http://www.pclob.gov/SiteAssets/newsroom/PCLOB%20Pelosi%20Response%20Final.pdf.

tension."[5] In response to the requests from Congress and the President, the Board began a comprehensive study of the two NSA programs. The Board held public hearings and met with the Intelligence Community and the Department of Justice, White House, and congressional committee staff, privacy and civil liberties advocates, academics, trade associations, and technology and communications companies.

During the course of this study, it became clear to the Board that each program required a level of review that was best undertaken and presented to the public in a separate report. As such, the Board released a report on the Section 215 telephone records program and the operation of the FISA court on January 23, 2014.[6] Subsequently, the Board held an additional public hearing and continued its study of the second program. Now, the Board is issuing the current report, which examines the collection of electronic communications under Section 702, and provides analysis and recommendations regarding the program's implementation.

The Section 702 program is extremely complex, involving multiple agencies, collecting multiple types of information, for multiple purposes. Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.

The Board has found that certain aspects of the program's implementation raise privacy concerns. These include the scope of the incidental collection of U.S. persons' communications and the use of queries to search the information collected under the program for the communications of specific U.S. persons. The Board offers a series of policy recommendations to strengthen privacy safeguards and to address these concerns.

II. Study Methodology

In order to gain a full understanding of the program's operations, the Board and its staff received multiple briefings on the operation of the program, including the technical

---

5 Remarks by the President in a Press Conference at the White House (Aug. 9, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

6 *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), *available at* http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

details and procedural rules that govern its implementation. The Board appreciates the responsiveness and open lines of communication that have been established with members of the Intelligence Community and the Department of Justice. These have enabled the Board to understand the operation of this complex program, and to fully consider the practical impact that the Board's recommendations will have.

Building upon the previous public hearings held in July and November 2013, the Board held an additional public hearing on March 19, 2014, focused exclusively on the Section 702 program.[7] This hearing was comprised of three panels. The first panel consisted of government representatives who provided the government's views on Section 702. The second panel consisted of academics and privacy advocates who addressed the legal issues related to Section 702, including both statutory and constitutional matters. The third panel consisted of representatives from private industry, academics, and human rights organizations who discussed the transnational and policy issues related to Section 702. Panelists, as well as the general public, were invited to submit written comments to the Board via www.regulations.gov.[8]

Since the unauthorized disclosures that began in 2013, much of the information that the Intelligence Community has declassified and released has related to the Section 215 program. In the preparation of this Report, the Board worked with the Intelligence Community to seek further declassification of information related to the Section 702 program. Specifically, the Board requested declassification of additional facts for use in this Report. Consistent with the Board's goal of seeking greater transparency where appropriate, the request for declassification of additional facts to be used in this Report was made in order to provide further clarity and education to the public about the Section 702 program. The Intelligence Community carefully considered the Board's requests and has engaged in a productive dialogue with PCLOB staff. The Board greatly appreciates the diligent efforts of the Intelligence Community to work through the declassification process, and as a result of the process, many facts that were previously classified are now available to the public.

In the course of preparing and finalizing this Report, the Board met with staff from the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, as well as staff from the House and Senate Judiciary Committees, to discuss the Section 702 program and the Board's preliminary recommendations. The Board also presented its preliminary recommendations to senior staff at the White House. In addition, the Board provided a draft of this Report to the Intelligence Community for classification review. While the Board's report was subject to classification review, and while the Board

---

7 *See* Annex E.

8 *See* Annex H.

considered the Intelligence Community's comments regarding the operation of the program to ensure accuracy, none of the changes resulting from that process affected the Board's substantive analysis and recommendations.

III. Report Organization

This Report consists of six parts. After this introduction and the Executive Summary, Part 3 contains a factual narrative that explains the development of the Section 702 program and how the program currently operates. Part 4 consists of legal analysis, including the Board's statutory and constitutional analyses, as well as a discussion of how the program affects the legal rights of non-U.S. persons. Part 5 examines the policy implications of the program, including an assessment of its efficacy and its effect on privacy, while Part 6 outlines and explains the Board's recommendations.

The Board presents this Report in an effort to provide greater transparency and clarity to the public regarding the government's activities with respect to the Section 702 program. The recommendations reflect the Board's best efforts to protect the privacy and civil liberties of the public while considering legitimate national security interests. The Board welcomes the opportunity for further discussion of these pressing issues.

Part 2:

EXECUTIVE SUMMARY

In 2008, Congress enacted the FISA Amendments Act, which made changes to the Foreign Intelligence Surveillance Act of 1978 ("FISA"). Among those changes was the addition of a new provision, Section 702 of FISA, permitting the Attorney General and the Director of National Intelligence to jointly authorize surveillance conducted within the United States but targeting only non-U.S. persons reasonably believed to be located outside the United States. The Privacy and Civil Liberties Oversight Board ("PCLOB") began reviewing implementation of the FISA Amendments Act early in 2013, shortly after the Board began operations as an independent agency.[9] The PCLOB has conducted an in-depth review of the program now operated under Section 702, in pursuit of the Board's mission to review executive branch actions taken to protect the nation from terrorism in order to ensure "that the need for such actions is balanced with the need to protect privacy and civil liberties."[10] This Executive Summary outlines the Board's conclusions and recommendations.

I. Overview of the Report

A. Description and History of the Section 702 Program

Section 702 has its roots in the President's Surveillance Program developed in the immediate aftermath of the September 11th attacks. Under one aspect of that program, which came to be known as the Terrorist Surveillance Program ("TSP"), the President authorized interception of the contents of international communications from within the United States, outside of the FISA process. Following disclosures about the TSP by the press in December 2005, the government sought and obtained authorization from the Foreign Intelligence Surveillance Court ("FISA court") to conduct, under FISA, the collection that had been occurring under the TSP. Later, the government developed a statutory framework specifically designed to authorize this collection program. After the enactment and expiration of a temporary measure, the Protect America Act of 2007, Congress passed the FISA Amendments Act of 2008, which included the new Section 702 of FISA. The statute

---

9 *See* Privacy and Civil Liberties Oversight Board, Minutes of Open Meeting of March 5, 2013, at 4-5, *available at* http://www.pclob.gov/SiteAssets/meetings-and-events/5-march-2013-public-meeting/5%20March%202013%20Meeting%20Minutes.pdf.

10 42 U.S.C. § 2000ee(c)(1).

provides a procedural framework for the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

Section 702 permits the Attorney General and the Director of National Intelligence to jointly authorize surveillance targeting persons who are not U.S. persons, and who are reasonably believed to be located outside the United States, with the compelled assistance of electronic communication service providers, in order to acquire foreign intelligence information. Thus, the persons who may be targeted under Section 702 cannot intentionally include U.S. persons or anyone located in the United States, and the targeting must be conducted to acquire foreign intelligence information as defined in FISA. Executive branch authorizations to acquire designated types of foreign intelligence under Section 702 must be approved by the FISA court, along with procedures governing targeting decisions and the handling of information acquired.

Although U.S. persons may not be targeted under Section 702, communications of or concerning U.S. persons may be acquired in a variety of ways. An example is when a U.S. person communicates with a non-U.S. person who has been targeted, resulting in what is termed "incidental" collection. Another example is when two non-U.S. persons discuss a U.S. person. Communications of or concerning U.S. persons that are acquired in these ways may be retained and used by the government, subject to applicable rules and requirements. The communications of U.S. persons may also be collected by mistake, as when a U.S. person is erroneously targeted or in the event of a technological malfunction, resulting in "inadvertent" collection. In such cases, however, the applicable rules generally require the communications to be destroyed.

Under Section 702, the Attorney General and Director of National Intelligence make annual certifications authorizing this targeting to acquire foreign intelligence information, without specifying to the FISA court the particular non-U.S. persons who will be targeted. There is no requirement that the government demonstrate probable cause to believe that an individual targeted is an agent of a foreign power, as is generally required in the "traditional" FISA process under Title I of the statute. Instead, the Section 702 certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information. The certifications that have been authorized include information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction.

Section 702 requires the government to develop targeting and "minimization" procedures that must satisfy certain criteria. As part of the FISA court's review and approval of the government's annual certifications, the court must approve these procedures and determine that they meet the necessary standards. The targeting procedures govern how the executive branch determines that a particular person is reasonably believed to be a non-U.S. person located outside the United States, and that

targeting this person will lead to the acquisition of foreign intelligence information. The minimization procedures cover the acquisition, retention, use, and dissemination of any non–publicly available U.S. person information acquired through the Section 702 program.

Once foreign intelligence acquisition has been authorized under Section 702, the government sends written directives to electronic communication service providers compelling their assistance in the acquisition of communications. The government identifies or "tasks" certain "selectors," such as telephone numbers or email addresses, that are associated with targeted persons, and it sends these selectors to electronic communications service providers to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as "PRISM" collection and "upstream" collection.

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.

Upstream collection differs from PRISM collection in several respects. First, the acquisition 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. Upstream collection also includes telephone calls in addition to Internet communications. Data from upstream collection is received only by the NSA: neither the CIA nor the FBI has access to unminimized upstream data. Finally, the upstream collection of Internet communications includes two features that are not present in PRISM collection: the acquisition of so-called "about" communications and the acquisition of so-called "multiple communications transactions" ("MCTs"). 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. 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.

Each agency that receives communications under Section 702 has its own minimization procedures, approved by the FISA court, that govern the agency's use,

retention, and dissemination of Section 702 data.[11] Among other things, these procedures include rules on how the agencies may "query" the collected data. The NSA, CIA, and FBI minimization procedures all include provisions permitting these agencies to query data acquired through Section 702, using terms intended to discover or retrieve communications content or metadata that meets the criteria specified in the query. These queries may include terms that identify specific U.S. persons and can be used to retrieve the already acquired communications of specific U.S. persons. Minimization procedures set forth the standards for conducting queries. For example, the NSA's minimization procedures require that queries of Section 702–acquired information be designed so that they are "reasonably likely to return foreign intelligence information."

The minimization procedures also include data retention limits and rules outlining circumstances under which information must be purged. Apart from communications acquired by mistake, U.S. persons' communications are not typically purged or eliminated from agency databases, even when they do not contain foreign intelligence information, until the data is aged off in accordance with retention limits.

Each agency's adherence to its targeting and minimization procedures is subject to extensive oversight within the executive branch, including internal oversight within individual agencies as well as regular reviews conducted by the Department of Justice ("DOJ") and the Office of the Director of National Intelligence ("ODNI"). The Section 702 program is also subject to oversight by the FISA court, including during the annual certification process and when compliance incidents are reported to the court. Information about the operation of the program also is reported to congressional committees. Although there have been various compliance incidents over the years, many of these incidents have involved technical issues resulting from the complexity of the program, and the Board has not seen any evidence of bad faith or misconduct.

B. Legal Analysis

The Board's legal analysis of the Section 702 program includes an evaluation of whether it comports with the terms of the statute, an evaluation of the Fourth Amendment issues raised by the program, and a discussion of the treatment of non-U.S. persons under the program.

In reviewing the program's compliance with the text of Section 702, the Board has assessed the operation of the program overall and has separately evaluated PRISM and upstream collection. On the whole, the text of Section 702 provides the public with transparency into the legal framework for collection, and it publicly outlines the basic

[11] As described in Part 3 of this Report, the National Counterterrorism Center ("NCTC") has some access to Section 702 data and therefore has its own minimization procedures as well. However, the NCTC's role in processing and minimizing Section 702 data is limited.

structure of the program. The Board concludes that PRISM collection is clearly authorized by the statute and that, with respect to the "about" collection, which occurs in the upstream component of the program, the statute can permissibly be interpreted as allowing such collection as it is currently implemented.

The Board also concludes that the core of the Section 702 program — acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court–approved targeting rules and multiple layers of oversight — fits within the "totality of the circumstances" standard for reasonableness under the Fourth Amendment, as that standard has been defined by the courts to date. Outside of this fundamental core, certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness. Such aspects include the unknown and potentially large scope of the incidental collection of U.S. persons' communications, the use of "about" collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific U.S. persons within the information that has been collected. With these concerns in mind, this Report offers a set of policy proposals designed to push the program more comfortably into the sphere of reasonableness, ensuring that the program remains tied to its constitutionally legitimate core.

Finally, the Board discusses the fact that privacy is a human right that has been recognized in the International Covenant on Civil and Political Rights ("ICCPR"), an international treaty ratified by the U.S. Senate, and that the treatment of non-U.S. persons in U.S. surveillance programs raises important but difficult legal and policy questions. Many of the generally applicable protections that already exist under U.S. surveillance laws apply to U.S. and non-U.S. persons alike. The President's recent initiative under Presidential Policy Directive 28 on Signals Intelligence ("PPD-28") will further address the extent to which non-U.S. persons should be afforded the same protections as U.S. persons under U.S. surveillance laws.[12] Because PPD-28 invites the PCLOB to be involved in its implementation, the Board has concluded that it can make its most productive contribution in assessing these issues in the context of the PPD-28 review process.

C. Policy Analysis

The Section 702 program has enabled the government to acquire a greater range of foreign intelligence than it otherwise would have been able to obtain — and to do so quickly and effectively. Compared with the "traditional" FISA process under Title I of the

[12] *See* Presidential Policy Directive — Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435 (Jan. 17, 2014) ("PPD-28"), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

statute, Section 702 imposes significantly fewer limits on the government when it targets foreigners located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted. The program has proven valuable in the government's efforts to combat terrorism as well as in other areas of foreign intelligence. Presently, over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. Monitoring terrorist networks under Section 702 has enabled the government to learn how they operate, and to understand their priorities, strategies, and tactics. In addition, the program has led the government to identify previously unknown individuals who are involved in international terrorism, and it has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries.

The basic structure of the Section 702 program appropriately focuses on targeting non-U.S. persons reasonably believed to be located abroad. Yet communications of, or concerning, U.S. persons can be collected under Section 702, and certain features of the program implicate privacy concerns. These features include the potential scope of U.S. person communications that are collected, the acquisition of "about" communications, and the use of queries that employ U.S. person identifiers.

The Board's analysis of these features of the program leads to certain policy recommendations.

The government is presently unable to assess the scope of the incidental collection of U.S. person information under the program. For this reason, the Board recommends several measures that together may provide insight about the extent to which communications involving U.S. persons or people located in the United States are being acquired and utilized.

With regard to the NSA's acquisition of "about" communications, the Board concludes that the practice is largely an inevitable byproduct of the government's efforts to comprehensively acquire communications that are sent to or from its targets. Because of the manner in which the NSA conducts upstream collection, and the limits of its current technology, the NSA cannot completely eliminate "about" communications from its collection without also eliminating a significant portion of the "to/from" communications that it seeks. The Board includes a recommendation to better assess "about" collection and a recommendation to ensure that upstream collection as a whole does not unnecessarily collect domestic communications.

The Report also assesses the impact of queries using "United States person identifiers." At the NSA, for example, these queries can be performed if they are deemed "reasonably likely to return foreign intelligence information." No showing of suspicion that

the U.S. person is engaged in any form of wrongdoing is required, but procedures are in place to prevent queries being conducted for improper purposes. The Board includes two recommendations to address the rules regarding U.S. person queries.

Overall, the Board finds that the protections contained in the Section 702 minimization procedures are reasonably designed and implemented to ward against the exploitation of information acquired under the program for illegitimate purposes. The Board has seen no trace of any such illegitimate activity associated with the program, or any attempt to intentionally circumvent legal limits. But the applicable rules potentially allow a great deal of private information about U.S. persons to be acquired by the government. The Board therefore offers a series of policy recommendations to ensure that the program appropriately balances national security with privacy and civil liberties.

II. Recommendations

A. Targeting and Tasking

Recommendation 1: *The NSA's targeting procedures should be revised to (a) specify criteria for determining the expected foreign intelligence value of a particular target, and (b) require a written explanation of the basis for that determination sufficient to demonstrate that the targeting of each selector is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. The NSA should implement these revised targeting procedures through revised guidance and training for analysts, specifying the criteria for the foreign intelligence determination and the kind of written explanation needed to support it. We expect that the FISA court's review of these targeting procedures in the course of the court's periodic review of Section 702 certifications will include an assessment of whether the revised procedures provide adequate guidance to ensure that targeting decisions are reasonably designed to acquire foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. Upon revision of the NSA's targeting procedures, internal agency reviews, as well as compliance audits performed by the ODNI and DOJ, should include an assessment of compliance with the foreign intelligence purpose requirement comparable to the review currently conducted of compliance with the requirement that targets are reasonably believed to be non-U.S. persons located outside the United States.*

B. U.S. Person Queries

Recommendation 2: *The FBI's minimization procedures should be updated to more clearly reflect the actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI*

assessments and investigations. Further, some additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non–foreign intelligence criminal matters.

Recommendation 3: *The NSA and CIA minimization procedures should permit the agencies to query collected Section 702 data for foreign intelligence purposes using U.S. person identifiers only if the query is based upon a statement of facts showing that it is reasonably likely to return foreign intelligence information as defined in FISA. The NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples.*

C. FISA Court Role

Recommendation 4: *To assist in the FISA court's consideration of the government's periodic Section 702 certification applications, the government should submit with those applications a random sample of tasking sheets and a random sample of the NSA's and CIA's U.S. person query terms, with supporting documentation. The sample size and methodology should be approved by the FISA court.*

Recommendation 5: *As part of the periodic certification process, the government should incorporate into its submission to the FISA court the rules for operation of the Section 702 program that have not already been included in certification orders by the FISA court, and that at present are contained in separate orders and opinions, affidavits, compliance and other letters, hearing transcripts, and mandatory reports filed by the government. To the extent that the FISA court agrees that these rules govern the operation of the Section 702 program, the FISA court should expressly incorporate them into its order approving Section 702 certifications.*

D. Upstream and "About" Collection

Recommendation 6: *To build on current efforts to filter upstream communications to avoid collection of purely domestic communications, the NSA and DOJ, in consultation with affected telecommunications service providers, and as appropriate, with independent experts, should periodically assess whether filtering techniques applied in upstream collection utilize the best technology consistent with program needs to ensure government acquisition of only communications that are authorized for collection and prevent the inadvertent collection of domestic communications.*

Recommendation 7: *The NSA periodically should review the types of communications acquired through "about" collection under Section 702, and study the extent to which it would be technically feasible to limit, as appropriate, the types of "about" collection.*

E. Accountability and Transparency

Recommendation 8: *To the maximum extent consistent with national security, the government should create and release, with minimal redactions, declassified versions of the FBI's and CIA's Section 702 minimization procedures, as well as the NSA's current minimization procedures.*

Recommendation 9: *The government should implement five measures to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program. Specifically, the NSA should implement processes to annually count the following: (1) the number of telephone communications acquired in which one caller is located in the United States; (2) the number of Internet communications acquired through upstream collection that originate or terminate in the United States; (3) the number of communications of or concerning U.S. persons that the NSA positively identifies as such in the routine course of its work; (4) the number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles, or other identifiers potentially associated with individuals; and (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers potentially associated with individuals. These figures should be reported to Congress in the NSA Director's annual report and should be released publicly to the extent consistent with national security.*

F. Efficacy

Recommendation 10: *The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs*.

III. Separate Statements

Following the Board's recommendations, the Report includes two separate statements.

A. Separate Statement of Chairman David Medine and Board Member Patricia Wald

Chairman David Medine and Member Patricia Wald wrote jointly to recommend requiring restrictions additional to those contained in Recommendation 3 with regard to U.S. person queries conducted for a foreign intelligence purpose. They also recommended that minimization procedures governing the use of U.S. persons' communications collected under Section 702 should require the following:

> (1) No later than when the results of a U.S. person query of Section 702 data are generated, U.S. persons' communications should be purged of information that does not meet the statutory definition of foreign intelligence information relating to U.S. persons.[13] This process should be subject to judicial oversight.[14]
>
> (2) Each U.S. person identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702, for a foreign intelligence purpose, other than in exigent circumstances or where otherwise required by law. The FISA court should determine, based on documentation submitted by the government, whether the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return foreign intelligence information as defined under FISA.[15]

In addition, they wrote to further explain their views regarding Recommendation 2. Specifically, they believe that the additional limits to be placed on the FBI's use and dissemination of Section 702 data in connection with non–foreign intelligence criminal matters should include the requirement that the FBI obtain prior FISA court approval before using identifiers to query Section 702 data to ensure that the identifier is reasonably likely to return information relevant to an assessment or investigation of a crime.

---

[13] U.S. person communications may also be responsive to queries using non-U.S. person identifiers.

[14] This review would not be necessary for queries seeking communications of U.S. persons who are already approved as targets for collection under Title I or Sections 703/704 of FISA and identifiers that have been approved by the FISA court under the "reasonable articulable suspicion" standard for telephony metadata under Section 215. It would also not be necessary if the query produces no results or the analyst purges all results from the given query as not containing foreign intelligence.

[15] Subsequent queries using a FISA court–approved U.S. person identifier would not require court approval.

The statement also responds to the separate statement by Members Brand and Cook.

B. Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook

Board Members Rachel Brand and Elisebeth Collins Cook wrote separately to emphasize the Board's unanimous bottom-line conclusion that the core Section 702 program is clearly authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective intelligence tool. They further wrote to explain their proposal for FBI queries of Section 702 data, which would not place limitations on the FBI's ability to include its FISA data within the databases *queried* in non–foreign intelligence criminal matters. They explain their view that querying information already in the FBI's possession is a relatively non-intrusive investigative tool, and the discovery of potential links between ongoing criminal and foreign intelligence investigations is potentially critical to national security. Instead, they would require an analyst who has not had FISA training to seek supervisory approval before *viewing* responsive 702 information, to ensure that the information continues to be treated consistent with applicable statutory and court-imposed restrictions. They also would require higher-level Justice Department approval before Section 702 information could be used in the investigation or prosecution of a non–foreign intelligence crime.

The statement also responds to the separate statement by Chairman Medine and Member Wald.

Part 3:

DESCRIPTION AND HISTORY

I. Genesis of the Section 702 Program

As it exists today, the Section 702 program can trace its lineage to two prior intelligence collection programs, both of which were born of counterterrorism efforts following the attacks of September 11, 2001. The first, and more well-known, of these two efforts was a program to acquire the contents of certain international communications, later termed the Terrorist Surveillance Program ("TSP"). In October 2001, President George W. Bush issued a highly classified presidential authorization directing the NSA to collect certain foreign intelligence by electronic surveillance in order to prevent acts of terrorism within the United States, based upon a finding that an extraordinary emergency existed because of the September 11 attacks. Under this authorization, electronic surveillance was permitted within the United States for counterterrorism purposes without judicial warrants or court orders for a limited number of days.[16] President Bush authorized the NSA to (1) collect the contents of certain international communications, a program that was later referred to as the TSP, and (2) collect in bulk non-content information, or "metadata," about telephone and Internet communications.[17] The acquisition of telephone metadata was the forerunner to the Section 215 calling records program discussed in a prior report by the Board.

The President renewed the authorization for the NSA's activities in early November 2001. Thereafter, the authorization was renewed continuously, with some modifications and constrictions to the scope of the authorized collection, approximately every thirty to sixty days until 2007. Each presidential authorization included the finding that an extraordinary emergency continued to exist justifying ongoing warrantless surveillance. Key members of Congress and the presiding judge of the Foreign Intelligence Surveillance Court ("FISC" or "FISA court") were briefed on the existence of the program. The collection of communications content and bulk metadata under these presidential authorizations became known as the President's Surveillance Program. According to a 2009 report by the inspectors general of several defense and intelligence agencies, over time, "the program

---

16 *See* DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013) ("Dec. 21 DNI Announcement"), *available at* http://icontherecord.tumblr.com/post/70683717031/dni-announces-the-declassification-of-the.

17 *See* Dec. 21 DNI Announcement, *supra*.

became less a temporary response to the September 11 terrorist attacks and more a permanent surveillance tool."[18]

In December 2005, the *New York Times* published articles revealing the TSP, i.e., the portion of the President's Surveillance Program that involved intercepting the contents of international communications. In response to these revelations, President Bush confirmed the existence of the TSP,[19] and the Department of Justice issued a "white paper" outlining the legal argument that the President could authorize these interceptions without obtaining a warrant or court order.[20] Notwithstanding this legal argument, the government decided to seek authorization under the Foreign Intelligence Surveillance Act ("FISA") to conduct the content collection that had been occurring under the TSP.[21] In January 2007, the FISC issued orders authorizing the government to conduct certain electronic surveillance of telephone and Internet communications carried over listed communication facilities where, among other things, the *government* made a probable cause determination regarding one of the communicants, and the email addresses and telephone numbers to be tasked were reasonably believed to be used by persons located outside the United States.[22]

The FISC's order, referred to as the "Foreign Telephone and Email Order," in effect replaced the President's authorization of the TSP, and the President made no further reauthorizations of the TSP.[23] When the government sought to renew the January 2007 Foreign Telephone and Email Order, however, a different judge on the FISC approved the program, but on a different legal theory that required changes in the collection program.[24] Specifically, in May 2007 the FISC approved a modified version of the Foreign Telephone and Email Order in which the *court*, as opposed to the *government*, made probable cause determinations regarding the particular foreign telephone numbers and email addresses that were to be used to conduct surveillance under this program.[25] Although the modified

---

18 *See* UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, PREPARED BY THE OFFICE OF INSPECTORS GENERAL OF THE DEPARTMENT OF DEFENSE, DEPARTMENT OF JUSTICE, CENTRAL INTELLIGENCE AGENCY, NATIONAL SECURITY AGENCY, AND THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, at 31 (2009).

19 *See, e.g.*, President's Radio Address (Dec. 17, 2005), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html.

20 Legal Authorities Supporting the Activities of the National Security Agency Described by the President (January 19, 2006), *available at* http://www.justice.gov/olc/opiniondocs/nsa-white-paper.pdf.

21 *See* Dec. 21 DNI Announcement, *supra*.

22 Declassified Certification of Attorney General Michael B. Mukasey, at ¶ 37, *In re National Security Agency Telecommunications Records Litigation*, MDL Dkt. No. 06-1791-VRW (N.D. Cal. Sept. 19, 2008) ("2008 Mukasey Decl."), *available at* http://www.dni.gov/files/documents/0505/AG%20Mukasey%202008%20Declassified%20Declaration.pdf.

23 2008 Mukasey Decl., *supra*, at ¶ 37.

24 2008 Mukasey Decl., *supra*, at ¶ 38 & n.20.

25 2008 Mukasey Decl., *supra*, at ¶ 38.

Foreign Telephone and Email Order permitted the government to add newly discovered telephone numbers and email addresses without an individual court order in advance,[26] the government assessed that the restrictions of the order, particularly after the May 2007 modifications, was creating an "intelligence gap."[27]

Separate from, but contemporaneous with, the TSP and the Foreign Telephone and Email Orders, a second collection effort was being undertaken. Specifically, the government used the then-existing FISA statute to obtain individual court orders to compel private companies to assist the government in acquiring the communications of individuals located overseas who were suspected of engaging in terrorism and who used United States–based communication service providers.[28] The government stated that it and the Foreign Intelligence Surveillance Court (FISC) expended "considerable resources" to obtain court orders based upon a probable cause showing that these overseas individuals met the legal standard for electronic surveillance under FISA,[29] i.e., that the targets were agents of a foreign power (such as an international terrorist group) and that they used the specific communication facilities (such as email addresses) regarding which the government was seeking to conduct electronic surveillance.[30] The persons targeted by these efforts were located outside the United States, and the communications being sought were frequently with others who were also located outside the United States.[31]

Drafting applications that demonstrated satisfaction of this probable cause standard, the government has asserted, slowed and in some cases prevented the acquisition of foreign intelligence information.[32] The government has not disclosed the scale of this second effort to target foreign individuals using traditional FISA electronic surveillance authorities, but in the years following the passage of the Protect America Act of 2007 and the FISA Amendments Act of 2008, which eliminated the requirement for the

---

26 2008 Mukasey Decl., *supra*, at ¶ 38.

27 *See* S. Rep. No. 110-209, at 5 (2007) (stating that "the DNI informed Congress that the decision . . . had led to degraded capabilities"); Eric Lichtblau, James Risen, and Mark Mazzetti, *Reported Drop in Surveillance Spurred a Law*, NEW YORK TIMES (Aug. 11, 2007) (reporting on Administration interactions with Congress that led to the enactment of the Protect America Act, including reported existence of an "intelligence gap").

28 Statement of Kenneth L. Wainstein, Assistant Attorney General, *Senate Select Committee on Intelligence Hearing On Modernization of the Foreign Intelligence Surveillance Act*, at 6-7 (May 1, 2007) ("May 2007 Wainstein Statement"), *available at* http://www.intelligence.senate.gov/070501/wainstein.pdf.

29 May 2007 Wainstein Statement, *supra*, at 6-7.

30 50 U.S.C. § 1805(a)(2).

31 May 2007 Wainstein Statement, *supra*, at 7.

32 *See, e.g.,* May 2007 Wainstein Statement, *supra*, at 7.

government to seek such individual orders, the total number of FISA electronic surveillance applications approved by the FISC dropped by over forty percent.[33]

In light of the perceived growing inefficiencies of obtaining FISC approval to target persons located outside the United States, in the spring of 2007 the Bush Administration proposed modifications to FISA.[34] Reports by the Director of National Intelligence to Congress that implementation of the FISC's May 2007 modifications to the Foreign Telephone and Email Order had resulted in "degraded" acquisition of communications, combined with reports of a "heightened terrorist threat environment," accelerated Congress' consideration of these proposals.[35] In August 2007, Congress enacted and the President signed the Protect America Act of 2007,[36] a legislative forerunner to what is now Section 702 of FISA. The Protect America Act was a temporary measure that was set to expire 180 days after its enactment.[37]

The government transitioned the collection of communications that had been occurring under the Foreign Telephone and Email Orders (previously the TSP) and some portion of the collection targeting persons located outside the United States that had been occurring under individual FISA orders to directives issued under the Protect America Act.[38] The Protect America Act expired in February 2008,[39] but existing Protect America Act certifications remained in effect until they expired.[40]

Shortly after passage of the Protect America Act, efforts began to replace it with a more permanent statute.[41] After substantial debate, in July 2008 Congress enacted and President Bush signed into law the FISA Amendments Act of 2008.[42] The FISA Amendments

---

33 *Compare* 2007 ANNUAL FISA REPORT (2,371 Title I FISA applications in 2007), *available at* http://www.fas.org/irp/agency/doj/fisa/2007rept.pdf *with* 2009 ANNUAL FISA REPORT (1,329 Title I FISA applications in 2009), *available at* http://www.fas.org/irp/agency/doj/fisa/2009rept.pdf.

34 *See* S. Rep. No. 110-209, at 2, 5 (noting Administration's submission of proposed modifications in April 2007); *see generally* May 2007 Wainstein Statement, *supra*; Statement of J. Michael McConnell, Director of National Intelligence, Before the Senate Select Committee on Intelligence (May 1, 2007), *available at* http://www.intelligence.senate.gov/070501/mcconnell.pdf.

35 *See* S. Rep. No. 110-209, at 5.

36 Pub. L. No. 110-55; 121 Stat. 552 (2007) ("Protect America Act").

37 Protect America Act § 6(c).

38 2008 Mukasey Decl., *supra*, at ¶ 13 & n.22.

39 *See* Protect America Act—Extension, Pub. L. No. 110-182, 122 Stat. 605 (2008) (extending Protect America Act for two weeks).

40 Protect America Act § 6.

41 *See, e.g.*, Press Release, The White House, President Bush Discusses the Protect America Act of 2007 (Sept. 19, 2007), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2007/09/20070919.html; S. Rep. No. 110-209, at 5.

42 Pub L. No. 110-261, 122 Stat. 2436 (2008).

Act replaced the expired Protect America Act provisions with the new Section 702 of FISA. The authorities and limitations of Section 702 are discussed in detail in this Report. In addition to Section 702, the FISA Amendments Act of 2008 also enacted Sections 703 and 704 of FISA, which required judicial approval for targeting U.S. persons located abroad in order to acquire foreign intelligence information.[43]

After passage of the FISA Amendments Act, the government transitioned the collection activities that had been conducted under the Protect America Act to Section 702.[44] Section 702, as well as the other provisions of FISA enacted by the FISA Amendments Act, were renewed in December 2012, and are currently set to expire in December 2017.[45]

II. Statutory Structure: What Does Section 702 Authorize?

The Foreign Intelligence Surveillance Act is a complex law, and Congress' authorization of surveillance under Section 702 of FISA is no exception. In one sentence, the statutory scope of Section 702 can be defined as follows: Section 702 of FISA permits the Attorney General and the Director of National Intelligence to jointly authorize the (1) targeting of persons who are not United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service provider, (4) in order to acquire foreign intelligence information.[46] Each of these terms is, to various degrees, further defined and limited by other aspects of FISA. Congress also imposed a series of limitations on any surveillance conducted under Section 702. The statute further specifies how the Attorney General and Director of National Intelligence may authorize such surveillance, as well as the role of the FISC in reviewing these authorizations. This section describes this complex statutory framework.

A. Statutory Definitions and Limitations

Our description of Section 702's statutory authorization begins by breaking down the four-part sentence above.

First, Section 702 authorizes the *targeting of persons*.[47] FISA does not define what constitutes "targeting," but it does define what constitutes a "person." Persons are not only

---

43 50 U.S.C. §§ 1881b, 1881c.

44 2008 Mukasey Decl., *supra*, at ¶ 40 & n.22.

45 FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012).

46 50 U.S.C. § 1881a(a), (b)(3), (g)(2)(A)(vi).

47 50 U.S.C. § 1881a(a).

individuals, but also groups, entities, associations, corporations, or foreign powers.[48] The definition of "person" is therefore broad, but not limitless: a foreign government or international terrorist group could qualify as a "person," but an entire foreign country cannot be a "person" targeted under Section 702.[49] In addition, the persons whom may be targeted under Section 702 may not intentionally include United States persons.[50] "United States persons" or "U.S. persons" are United States citizens, United States permanent residents (green card holders), groups substantially composed of United States citizens or permanent residents, and virtually all United States corporations.[51] As is discussed in detail below, the NSA targets persons by tasking "selectors," such as email addresses and telephone numbers. The NSA must make determinations (regarding location, U.S. person status, and foreign intelligence value) about the users of each selector on an individualized basis. It cannot simply assert that it is targeting a particular terrorist group.

Second, under Section 702 the non-U.S. person target *must also be "reasonably believed to be located outside the United States."* A "reasonable belief" is not defined in FISA, but Section 702 does require that targeting procedures (described in further detail below) be adopted to ensure that Section 702 acquisition is limited to targets reasonably believed to be located outside the United States.[52] Electronic surveillance targeting persons believed to be located in the United States is not permitted by Section 702, whether the persons in question are U.S. persons or not.[53]

Third, under Section 702 this targeting of non-U.S. persons reasonably believed to be located outside the United States *occurs with the compelled assistance of an "electronic communication service provider."*[54] FISA defines electronic communication service providers to include a variety of telephone, Internet service, and other communications providers.[55] As further described below, electronic communication service providers are

---

48 50 U.S.C. §§ 1801(m), 1881(a). The term "foreign power" is a defined term in FISA; it includes international terrorist groups, foreign governments, and entities not substantially composed of United States persons that are engaged in the proliferation of weapons of mass destruction.

49 *See* Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 71 (Mar. 19, 2014) ("PCLOB March 2014 Hearing Transcript") (statement of Rajesh De, General Counsel, NSA, in response to questions by James Dempsey, Board Member, PCLOB), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

50 50 U.S.C. § 1881a(b)(3).

51 50 U.S.C. § 1801(i).

52 50 U.S.C. § 1881a(d)(1)(A).

53 50 U.S.C. §§ 1881(b)(1).

54 50 U.S.C. § 1881a(g)(2)(A)(vi).

55 50 U.S.C. § 1881(b)(4).

compelled to provide this assistance in conducting Section 702 acquisition through directives issued by the Attorney General and the Director of National Intelligence. Given the nature of the Internet, communications generated and delivered through communication services offered directly to individuals by one entity may be acquired as they cross the network of another provider without the knowledge of the consumer-facing provider. This concept is further described in the discussion below regarding upstream collection.

Fourth, and finally, this targeting of non-U.S. persons reasonably believed to be located outside the United States *must be conducted "to acquire foreign intelligence information."*[56] Non-U.S. persons may be targeted under Section 702 only if the government has reason to believe that those persons possess, are expected to receive, or are likely to communicate foreign intelligence information.[57] Foreign intelligence information concerning non-U.S. persons is defined in FISA as information that relates to the ability of the United States to protect against an actual or potential attack by a foreign power; sabotage, international terrorism, or the proliferation of weapons of mass destruction by a foreign power; or clandestine intelligence activities by a foreign power.[58] Foreign

---

[56] There is some conflicting language in Section 702 on the precise standard on this point. Section 1881a(a) states that a Section 702 authorization must be "…to acquire foreign intelligence information." This authority, however, must be governed by a certification, and the certification need only state that "a significant purpose of the acquisition is to obtain foreign intelligence information." 50 U.S.C. § 1881a(g)(2)(A)(v). *See also* SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, AUGUST 2013, at A-2 ("AUGUST 2013 SEMIANNUAL ASSESSMENT") (noting that the Section 702 Attorney General Guidelines implement the statutory requirement that a "significant purpose of [Section 702] acquisition is to obtain foreign intelligence information," 50 U.S.C. § 1881a(g)(2)(A)(v), by requiring that Section 702 targeting occur only with respect to persons assessed to possess foreign intelligence information or who are reasonably likely to receive or communicate foreign intelligence information), *available at* http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf; *see also* NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 5 (April 16, 2014) ("NSA DCLPO REPORT"), *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

[57] NSA DCLPO REPORT, *supra*, at 3.

[58] 50 U.S.C. § 1801(e)(1). For information concerning a U.S. person, the information must be "necessary" for this purpose. Specifically, this provision states foreign intelligence information is defined as:

> [I]nformation that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against —
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or agent of a foreign power; or
>
> (C) Clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

intelligence information concerning non-U.S. persons is also defined as information that relates to the national defense or security of the United States or the conduct of the foreign affairs of the United States, but only insofar as that information concerns a foreign power (such as international terrorist groups or foreign governments) or foreign territory.[59] The term "foreign territory" is undefined by the statute. As noted below, in authorizing Section 702 acquisition, the Attorney General and Director of National Intelligence specify the categories of foreign intelligence information that the United States government is seeking to acquire.

In addition to defining the scope of the Section 702 authorization, Congress specified limitations on the government's authority to engage in Section 702 targeting. As previously mentioned, U.S. persons may not be intentionally targeted. In addition, the government is prohibited under the law from intentionally targeting "any person known at the time of acquisition to be located in the United States."[60] These two rules taken together — that the target must be both a non-U.S. person and someone reasonably believed to be located abroad — are often referred to as the "foreignness" requirement.

The government is also prohibited from engaging in what is generally referred to as "reverse targeting," which would occur if the government were to intentionally target persons reasonably believed to be located outside the United States "if the purpose of the acquisition is to target a particular, known person reasonably believed to be in the United States."[61] In addition to this explicit prohibition against reverse targeting persons located in the United States, the government reads the statutory prohibition against targeting U.S. persons to also prohibit the reverse targeting of U.S. persons.[62] In other words, the ban on reverse targeting prohibits the government from targeting a non-U.S. person outside the United States when the real interest is to collect the communications of a person in the United States or of any U.S. person, regardless of location.

Under Section 702, the government also "may not intentionally acquire communications as to which the sender and all intended recipients are known at the time

---

59 50 U.S.C. § 1801(e)(2). Specifically, this provision states foreign intelligence information is also defined as:

> [I]nformation with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

60 50 U.S.C. § 1881a(b)(1).

61 50 U.S.C. § 1881a(b)(2).

62 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 89-92.

of the acquisition to be located in the United States."[63] Finally, Section 702 contains a limitation (and a reminder) that any acquisition must always be conducted consistent with the requirements of the Fourth Amendment to the Constitution.[64]

B. Section 702 Certifications

The Attorney General and the Director of National Intelligence authorize Section 702 targeting in a manner substantially different than traditional electronic surveillance under FISA. To authorize traditional FISA electronic surveillance, an application approved by the Attorney General must be made to the FISC.[65] This individualized application must include, among other things, the identity (if known) of the specific target of the electronic surveillance; facts justifying a probable cause finding that this target is a foreign power or agent of a foreign power and uses (or is about to use) the communication facilities or places at which electronic surveillance is being directed;[66] minimization procedures governing the acquisition, retention, and dissemination of non-publicly available U.S. person information acquired through the electronic surveillance; and a certification regarding the foreign intelligence information sought.[67] If the FISC judge who reviews the government's application determines that it meets the required elements — including that there is probable cause that the specified target is a foreign power or agent of a foreign power and that the minimization procedures meet the statutory requirements — the judge will issue an order authorizing the requested electronic surveillance.[68]

Section 702 differs from this traditional FISA electronic surveillance framework both in the standards applied and in the lack of individualized determinations by the FISC. Under the statute, the Attorney General and Director of National Intelligence make annual certifications authorizing the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information, without specifying to the FISC the particular non-U.S. persons who will be targeted.[69] Instead of identifying particular individuals to be targeted under Section 702, the certifications identify categories of foreign intelligence information regarding which the Attorney

---

63 50 U.S.C. § 1881a(b)(4).

64 50 U.S.C. § 1881a(b)(5).

65 50 U.S.C. § 1804(a). FISA also grants additional authority to conduct emergency electronic surveillance without first making an application to the FISC. 50 U.S.C. § 1805(e).

66 *But see* 50 U.S.C. § 1805(c)(3) (permitting electronic surveillance orders "in circumstances where the nature and location of each of the facilities or places at which surveillance will be directed is unknown")

67 50 U.S.C. §§ 1804(a), 1805(a).

68 50 U.S.C. § 1805(a), (c), (d).

69 50 U.S.C. § 1881a(a); NSA DCLPO REPORT, *supra*, at 2 (noting that Section 702 certifications do not require "individualized determination" by the FISC).

General and Director of National Intelligence authorize acquisition through the targeting of non-U.S. persons reasonably believed to be located abroad.[70] There also is no requirement that the government demonstrate probable cause to believe that a Section 702 target is a foreign power or agent of a foreign power, as is required under traditional FISA. Rather, the categories of information being sought must meet the definition of foreign intelligence information described above. The government has not declassified the full scope of the certifications that have been authorized, but officials have stated that these certifications have authorized the acquisition of information concerning international terrorism and other topics, such as the acquisition of weapons of mass destruction.[71]

While individual targets are not specified, Section 702 certifications must instead contain "targeting procedures" approved by the Attorney General that must be "reasonably designed" to ensure that any Section 702 acquisition is "limited to targeting persons reasonably believed to be located outside the United States" and prevents the "intentional acquisition" of wholly domestic communications.[72] The targeting procedures specify the manner in which the Intelligence Community must determine whether a person is a non-U.S. person reasonably believed to be located outside the United States who possesses (or is likely to possess or receive) the types of foreign intelligence information authorized by a certification. The process by which individuals are permitted to be targeted pursuant to the targeting procedures is discussed in detail below. In addition, the Attorney General and Director of National Intelligence must also attest in the certification that the Attorney General has adopted additional guidelines to ensure compliance with both these and the other statutory limitations on the Section 702 program.[73] Most critically, these Attorney General Guidelines explain how the government implements the statutory prohibition against reverse targeting.

While only non-U.S. persons may be intentionally targeted, the information of or concerning U.S. persons may be acquired through Section 702 targeting in a variety of ways, such as when a U.S. person is in communication with a non-U.S. person Section 702

---

70 *See* 50 U.S.C. § 1881a(g)(2)(A)(v) (requiring Attorney General and Director of National Intelligence to attest that a significant purpose of the acquisition authorized by the certification is to acquire foreign intelligence information); PCLOB March 2014 Hearing Transcript, *supra*, at 8-9 (statement of Robert Litt, General Counsel, ODNI) (stating that certifications "identify categories of information that may be acquired"); NSA DCLPO REPORT, *supra*, at 2 (noting the "annual topical certifications" authorized by Section 702).

71 PCLOB March 2014 Hearing Transcript at 13 (statement of Robert Litt, General Counsel, ODNI) (stating that the Section 702 program has been an important source of information "not only about terrorism, but about a wide variety of other threats to our nation"); *id*. at 59 (statement of Rajesh De, General Counsel, NSA) (stating that there are certifications on "counterterrorism" and "weapons of mass destruction"); *id*. at 68 (statement of James A. Baker, General Counsel, FBI) ("[T]his program is not limited just to counterterrorism.").

72 50 U.S.C. § 1881a(d)(1), (g)(2)(A)(i), (g)(2)(B).

73 50 U.S.C. § 1881a(f), (g)(2)(A)(iii).

target, because two non-U.S. persons are discussing a U.S. person, or because a U.S. person was mistakenly targeted. Section 702 therefore requires that certifications also include "minimization procedures" that control the acquisition, retention, and dissemination of any non–publicly available U.S. person information acquired through the Section 702 program.[74] As discussed below, the minimization procedures include different procedures for handling U.S. person information depending on the circumstances of how it was acquired. Along with the targeting procedures, the minimization procedures contain the government's core privacy and civil liberties protections and are more fully discussed throughout this Report.

C. FISC Review

The government's Section 702 certifications, targeting procedures, and minimization procedures (but not the Attorney General Guidelines) are all subject to review by the FISC.[75] In addition to the required procedures and guidelines, the Section 702 certifications are accompanied by affidavits of national security officials[76] that further describe to the FISC the government's basis for assessing that the proposed Section 702 acquisition will be consistent with the applicable statutory authorization and limits.[77] Through court filings or the testimony of witnesses at hearings before the FISC, the government also submits additional information explaining how the targeting and minimization procedures will be applied and describing the operation of the program in a way that defines its scope.[78]

The FISC's review of the Section 702 certifications has been called "limited" by scholars,[79] privacy advocates,[80] and in one instance, shortly after the FISA Amendments Act

---

74 50 U.S.C. § 1881a(e)(1), (g)(2)(A)(ii), (g)(2)(B).

75 50 U.S.C. § 1881a(d)(2), (e)(2), (i). The Attorney General Guidelines must, however, be submitted to the FISA court. 50 U.S.C. § 1881a(f)(2)(C). Section 702 does have a provision permitting the Attorney General and the Director of National Intelligence to authorize acquisition prior to judicial review of a certification under certain exigent circumstances. 50 U.S.C. § 1881a(c)(2). To date, the Attorney General and the Director of National Intelligence have never exercised this authority.

76 50 U.S.C. § 1881a(g)(2)(C); *see, e.g.*, Memorandum Opinion at 3, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011) ("Bates October 2011 Opinion") (noting submitted affidavits by the Director or Acting Director of NSA and the Director of FBI), *available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

77 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-1 to A-2.

78 *See, e.g.,* Bates October 2011 Opinion, *supra*, at 5-9, 2011 WL 10945618, at *2-4 (describing 2011 government filings with, and testimony before, the FISA court); *id*. at 15-16, 2011 WL 10945618, at *5 (describing representations made to the FISA court in prior Section 702 certifications).

79 *See, e.g.*, Laura K. Donohue, Section 702 and the Collection of International Telephone and Internet Content, at 15, 18, 30-34, *available at* http://justsecurity.org/wp-content/uploads/2014/05/donahue.702.pdf.

was passed, by the FISC itself.[81] In certain respects, this characterization is accurate. Unlike traditional FISA applications, the FISC does not review the targeting of particular individuals. Specifically, although the Section 702 certifications identify the foreign intelligence subject matters regarding which information is to be acquired, the FISC does not see or approve the specific persons targeted or the specific communication facilities that are actually tasked for acquisition. As such the government does not present evidence to the FISC, nor does the FISC determine — under probable cause or any other standard — that the particular individuals being targeted are non-U.S. persons reasonably believed to be located outside the United States who are being properly targeted to acquire foreign intelligence information.[82] Instead of requiring judicial review of these elements, Section 702 calls upon the FISA court only to decide whether the targeting procedures are reasonably designed to ensure compliance with certain limitations and that the minimization procedures satisfy certain criteria (described below). The FISC is not required to independently determine that a significant purpose of the proposed acquisition is to obtain foreign intelligence information,[83] although the foreign intelligence purpose of the collection does play a role in the court's Fourth Amendment analysis.[84]

In other respects, however, the FISC's role in the Section 702 program is more extensive. The FISC reviews both the targeting procedures and the minimization procedures, the core set of documents that implement Section 702's statutory requirements and limitations.[85] With respect to the targeting procedures, the FISC must

---

80 *See, e.g.*, Submission of Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union Foundation, Privacy and Civil Liberties Oversight Board Public Hearing on Section 702 of the FISA Amendments Act, at 9 (Mar. 19, 2014), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf.

81 Memorandum Opinion, *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, Docket Misc. No. 08-01, 2008 WL 9487946, at *5 (FISA Ct. Aug. 27, 2008).

82 *See* The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, at 2 (2012) (describing differences between targeting individuals under traditional FISA electronic surveillance provisions and targeting pursuant to Section 702). This document accompanied a 2012 letter sent by the Department of Justice and the Office of the Director of National Intelligence to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence urging the reauthorization of Section 702. *See* Letter from Kathleen Turner, Director of Legislative Affairs, ODNI, and Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, DOJ to the Honorable Dianne Feinstein, Chairman, Senate Committee on Intelligence, et. al. (May 4, 2012), *available at* http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf.

83 50 U.S.C. § 1881a(i)(2).

84 Additionally, if the FISC determines that a Section 702 certification and related documents are insufficient on Constitutional or statutory grounds, the FISC cannot itself modify the certification and related documents governing the Section 702 program, but instead must issue an order to the government to either correct any deficiencies identified by the FISC within 30 days or to cease (or not begin) implementation of the certification. 50 U.S.C. § 1881a(i)(3)(B).

85 50 U.S.C. § 1881a(d)(2), (e)(2), (i)(1)(A).

determine that they "are reasonably designed" to "ensure" that targeting is "limited to targeting persons reasonably believed to be located outside the United States."[86] The FISC also must determine that the targeting procedures are reasonably designed to prevent the intentional acquisition of wholly domestic communications.[87] In addition, the FISC must also review the proposed minimization procedures under the same standard of review that is required in traditional FISA electronic surveillance and physical search applications.[88] The FISC must find that such minimization procedures are "specific procedures" that are "reasonably designed" to control the acquisition, retention, and dissemination of non–publicly available U.S. person information.[89] Each time the FISC reviews a Section 702 certification, the FISC must also determine whether the proposed Section 702 acquisition as provided for, and restricted by, the targeting and minimization procedures complies with the Fourth Amendment.[90] After conducting its analysis, the FISC must issue a written opinion explaining the reasons why the court has held that the proposed targeting and minimization procedures do, or do not, comply with statutory and Fourth Amendment requirements.[91]

The FISC has held that it cannot make determinations in a vacuum regarding whether targeting and minimization procedures are "reasonably designed" to meet the statutory requirements and comply with the Fourth Amendment. To the contrary, the FISC "has repeatedly noted that the government's targeting and minimization procedures must be considered in light of the communications actually acquired," and that "[s]ubstantial implementation problems can, notwithstanding the government's intent, speak to whether the applicable targeting procedures are 'reasonably designed' to acquire only the communications of non-U.S. persons outside the United States.'"[92] Therefore, although the FISC reviews the targeting procedures, minimization procedures, and related affidavits that

---

86 50 U.S.C. § 1881a(i)(2)(B)(i).

87 50 U.S.C. § 1881a(i)(2)(B)(ii).

88 *Compare* 50 U.S.C. § 1881a(i)(2)(C) (requirement to evaluate Section 702 minimization procedures) *with* 50 U.S.C. § 1805(a)(3) (requirement to evaluate FISA electronic surveillance minimization procedures) *and* 50 U.S.C. § 1824(a)(3) (requirement to evaluate FISA physical search minimization procedures).

89 50 U.S.C. § 1801(h).

90 50 U.S.C. § 1881a(i)(3)(A), (i)(3)(B).

91 50 U.S.C. § 1881a(i)(3)(C). While FISC judges may write opinions explaining their orders with regard to other aspects of FISA, the statutory requirement for an opinion explaining the rationale of all orders approving Section 702 certifications is unique within FISA. Though not required by FISA, FISC Rule of Procedure 18(b)(1) also requires FISC judges to provide a written statement of reasons for any denials of the government's other FISA applications. *See* United States Foreign Intelligence Surveillance Court Rules of Procedure ("FISC Rule of Procedure"), Rule 18(b)(1), *available at* http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.

92 Bates October 2011 Opinion, *supra*, at 28, 2011 WL 10945618, at *9 (quoting FISC opinion with redacted docket number).

are submitted with a Section 702 certification, the court's review is not limited to the four corners of those documents. The FISC also takes into consideration additional filings by the government to supplement or clarify the record, responses to FISC orders to supplement the record,[93] and the sworn testimony of witnesses at hearings.[94]

Commitments regarding how the targeting and minimization procedures will be implemented that are made to the FISC in these representations have been found to be binding on the government. For example, during the consideration of the first Section 702 certification in 2008, the government stated that that the targeting procedures impose a requirement that analysts conduct "due diligence" in determining the U.S. person status of any Section 702 target, even though the phrase "due diligence" is not explicitly found in the text of the NSA targeting procedures. The FISC incorporated the government's representation regarding due diligence into its opinion, and the government has subsequently reported to Congress and the FISC — as incidents of noncompliance — instances in which the Intelligence Community conducted insufficient due diligence that resulted in the targeting of a U.S. person.[95]

In evaluating the Section 702 certifications, the court also considers additional filings required by the FISC's Rules of Procedure. One such rule requires the government to notify the FISA court whenever the government discovers a material misstatement or omissions in a prior filing with the court.[96] Another rule mandates that the government report to the FISA court incidents of noncompliance with targeting or minimization procedures previously approved by the court.[97] In a still-classified 2009 opinion, the FISC held that the judicial review requirements regarding the targeting and minimization procedures required that the FISC be fully informed of every incident of noncompliance

---

93 *See* FISC Rule of Procedure 5(c) (stating that the FISC Judges have the authority to order any party to a proceeding to supplement the record by "furnish[ing] any information that the Judge deems necessary").

94 FISC Rule of Procedure 17.

95 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 29 (describing incidents and stating "In each of these incidents, all Section 702–acquired data was purged. Together, these [redacted] instances represent isolated instances of insufficient due diligence that do not reflect the [redacted] of taskings that occur during the reporting period.").

96 *See* FISC Rule of Procedure 13(a).

97 *See* FISC Rule of Procedure 13(b); SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, MAY 2010, at 22 ("MAY 2010 SEMIANNUAL ASSESSMENT") (discussing requirements under Rule 10(c), the predecessor to Rule 13(b) in the prior set of FISC Rules of Procedure), *available at* http://www.dni.gov/files/documents/FAA/SAR%20May%202010%20Final%20Release%20with%20Exemptions.pdf. The government also provides the FISC the Semiannual Section 702 Joint Assessment, portions of the Section 707 Semiannual report, and a separate quarterly report to the FISC, all of which describe scope, nature, and actions taken in response to compliance incidents. *See* The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 5; 50 U.S.C. § 1881a(l)(1).

with those procedures. In the 2009 opinion, the court analyzed whether several errors in applying the targeting and minimization procedures that had been reported to the court undermined either the court's statutory or constitutional analysis. (The court concluded that they did not.)

In addition to identifying errors that could impact the sufficiency of the targeting and minimization procedures, these compliance notices play an additional role in informing the FISC regarding how the government is in fact applying the targeting and minimization procedures. Specifically, the compliance notices must state both the type of noncompliance that has occurred and the facts and circumstances relevant to the incident.[98] In doing so, representations to the FISA court have in essence created a series of precedents regarding how the government is interpreting various provisions of its targeting and minimization procedures, which informs the court's conclusions regarding whether those procedures — as actually applied by the Intelligence Community to particular, real-life factual scenarios — comply with Section 702's statutory requirements and the Fourth Amendment. For example, while the 2008 FISC opinion incorporated the government's commitment to apply due diligence in determining the U.S. person status of potential targets, notices of non-compliance filed by the government reflect that the government interprets the targeting procedures to also require due diligence in determining the *location* of potential targets. Similarly, the government has filed letters clarifying aspects of its "post-tasking" process, which are discussed further below, and it has reported — as compliance incidents — instances when its performance of the post-tasking process has not complied with those representations. The government's interpretations of the targeting and minimization procedures reflected in these compliance filings, however, are not necessarily formally endorsed or incorporated into the FISC's subsequent opinions. In the Board's opinion Intelligence Community personnel applying these procedures months or years later may not be aware of the interpretive gloss arising from prior interactions between the government and the FISC on these procedures.

Former FISC Presiding Judge John Bates' October 3, 2011 opinion provides both an example of the scope of the FISA court's review of Section 702 certifications in practice and an illustration of what actions the court can take if it determines that the government has not satisfied the court's expectations to be kept fully, accurately, and timely informed. In April 2011, the government filed multiple Section 702 certifications with the FISC.[99] In early May 2011, however, the government filed a letter with the court (under a FISC procedural rule regarding material misstatements or omissions) acknowledging that the scope of the NSA's "upstream" collection (described below) was more expansive than

---

98 FISC Rule of Procedure 13(b).

99 Bates October 2011 Opinion, *supra*, at 3, 2011 WL 10945618, at *1.

previously represented to the court.[100] As a result of the filing, the FISC expressed serious concern that the upstream collection, as described by the government, may have exceeded the scope of collection previously approved by the FISC and what could be authorized under Section 702. The FISC therefore ordered the government to respond to a number of questions regarding the upstream collection program.[101] Throughout the summer of 2011, the government continued to supplement the record in response to the FISA court's concerns with a number of filings, including by conducting and reporting to the court the results of a statistical sample of the NSA's acquisition of upstream collection.[102] The government's supplemental filings discussed both factual matters, such as how many domestic communications were being acquired as a result of the manner in which the government was conducting upstream collection, as well as the government's legal interpretations regarding how the NSA's minimization procedures should be applied to such acquisition.[103] The FISA court also met with the government and held a hearing to ask additional questions of NSA and Department of Justice personnel.[104]

Based on this record, Judge Bates ultimately held that in light of the new information, portions of the NSA minimization procedures met neither the requirements of FISA nor the Fourth Amendment and ordered the government to correct the deficient procedures or cease Section 702 upstream collection.[105] The government subsequently modified the NSA minimization procedures to remedy the deficiencies identified by the FISA court.[106] The FISC continued to have questions, however, regarding upstream collection that had been acquired prior to the implementation of these modified NSA minimization procedures.[107] The government took several actions with regard to this past upstream collection, and ultimately decided to purge it all.[108]

---

100 Bates October 2011 Opinion, *supra*, at 5, 2011 WL 10945618, at *2.

101 Bates October 2011 Opinion, *supra*, at 7, 2011 WL 10945618, at *2.

102 Bates October 2011 Opinion, *supra*, at 10, 2011 WL 10945618, at *3-4.

103 Bates October 2011 Opinion, *supra*, at 33-35, 50, 54-56, 2011 WL 10945618, at *11, *17, *18-19.

104 Bates October 2011 Opinion, *supra*, at 7-9, 2011 WL 10945618, at *4.

105 Bates October 2011 Opinion, *supra*, at 59-63, 67-80, 2011 WL 10945618, at *20-28.

106 *See generally* Memorandum Opinion, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10947772 (FISA Ct. Nov. 30, 2011) ("Bates November 2011 Opinion"), *available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

107 *See* Memorandum Opinion at 26-30, [*Caption Redacted*], [Docket No. Redacted], 2012 WL 9189263, at *1-4 (FISA Ct. Sept. 25, 2012) ("Bates September 2012 Opinion"), *available at* http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf.

108 Bates September 2012 Opinion, *supra*, at 30-32, 2012 WL 9189263, at *3-4.

D. Directives

As noted above, Section 702 targeting may occur only with the assistance of electronic communication service providers. Once Section 702 acquisition has been authorized, the Attorney General and the Director of National Intelligence send written directives to electronic communication service providers compelling the providers' assistance in the acquisition.[109] Providers that receive a Section 702 directive may challenge the legality of the directive in the FISC.[110] The government may likewise file a petition with the FISC to compel a provider that does not comply with a directive to assist the government's acquisition of foreign intelligence information.[111] The FISC's decisions regarding challenges and enforcement actions regarding directives are appealable to the Foreign Intelligence Surveillance Court of Review ("FISCR"), and either the government or a provider may request that the United States Supreme Court review a decision of the FISCR.[112]

III. Acquisition Process: How Does Section 702 Surveillance Actually Work?

Once a Section 702 certification has been approved, non-U.S. persons reasonably believed to be located outside the United States may be targeted to acquire foreign intelligence information within the scope of that certification. The process by which non-U.S. persons are targeted is detailed in the next section. This section describes how Section 702 acquisition takes place once an individual has been targeted.

A. Targeting Persons by Tasking Selectors

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, such as the target's email address or telephone number.[113] 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

---

109 50 U.S.C. § 1881a(h).

110 50 U.S.C. § 1881a(h)(4).

111 50 U.S.C. § 1881a(h)(5).

112 50 U.S.C. § 1881a(h)(6). However, as noted in the Board's Section 215 report, to date, only two cases have been appealed to the FISCR. One, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act,* 551 F.3d 1004 (FISA Ct. Rev. 2008), involved a directive under the Protect America Act, the predecessor to Section 702, but none have involved Section 702. Nor has the U.S. Supreme Court ever considered the merits of a FISA order or ruled on the merits of any challenge to FISA.

113 *See* AUGUST 2013 JOINT ASSESSMENT, *supra*, at A-2; NSA DCLPO REPORT, *supra*, at 4; The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

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").[114] 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.[115]

Although targeting decisions must be individualized, this does not mean that a substantial number of persons are not targeted under the Section 702 program. The government estimates that 89,138 persons were targeted under Section 702 during 2013.[116]

Once a selector has been tasked under the targeting procedures, it is sent to an electronic communications service provider to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as "PRISM" collection and "upstream" collection. PRISM collection is the easier of the two acquisition methods to understand.

B. PRISM Collection

In PRISM collection, the government (specifically, the FBI on behalf of the NSA) sends selectors — such as an email address — to a United States–based electronic communications service provider (such as an Internet service provider, or "ISP") that has been served a directive.[117] Under the directive, the service provider is compelled to give the communications sent to or from that selector to the government (but not communications that are only "about" the selector, as described below).[118] As of mid-2011, 91 percent of the

---

114 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

115 NSA DCLPO REPORT, *supra*, at 6.

116 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013, at 1 (June 26, 2014), a*vailable at* http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf. In calculating this estimate, the government counted two known people using one tasked email address as two targets and one person known to use two tasked email addresses as one target. The number of targets is an estimate because the government may not be aware of all of the users of a particular tasked selector.

117 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3. *See also* PCLOB March 2014 Hearing Transcript at 70 (statement of Rajesh De, General Counsel, NSA) (noting any recipient company "would have received legal process").

118 PCLOB March 2014 Hearing Transcript at 70; *see also* NSA DCLPO REPORT, *supra*, at 5.

Internet communications that the NSA acquired each year were obtained through PRISM collection.[119]

The government has not declassified the specific ISPs that have been served directives to undertake PRISM collection, but an example using a fake United States company ("USA-ISP Company") may clarify how PRISM collection works in practice: The NSA learns that John Target, a non-U.S. person located outside the United States, uses the email address "johntarget@usa-ISP.com" to communicate with associates about his efforts to engage in international terrorism. The NSA applies its targeting procedures (described below) and "tasks" johntarget@usa-ISP.com to Section 702 acquisition for the purpose of acquiring information about John Target's involvement in international terrorism. The FBI would then contact USA-ISP Company (a company that has previously been sent a Section 702 directive) and instruct USA-ISP Company to provide to the government all communications to or from email address johntarget@usa-ISP.com. The acquisition continues until the government "detasks" johntarget@usa-ISP.com.

The NSA receives all PRISM collection acquired under Section 702. In addition, a copy of the raw data acquired via PRISM collection — and, to date, only PRISM collection — may also be sent to the CIA and/or FBI.[120] The NSA, CIA, and FBI all must apply their own minimization procedures to any PRISM-acquired data.[121]

Before data is entered into systems available to trained analysts or agents, government technical personnel use technical systems to help verify that data sent by the provider is limited to the data requested by the government. To again use the John Target example above, if the NSA determined that johntarget@usa-ISP.com was not actually going to be used to communicate information about international terrorism, the government would send a detasking request to USA-ISP Company to stop further Section 702 collection on this email address. After passing on the detasking request to USA-ISP Company, the government would use its technical systems to block any further Section 702 acquisition from johntarget@usa-ISP.com to ensure that Section 702 collection against this address was immediately terminated.

---

119 Bates October 2011 Opinion, *supra*, at 29-30 and n.24, 2011 WL 10945618, at *25 & n.24.

120 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, § 6(c) (Oct. 31, 2011) ("NSA 2011 Minimization Procedures"), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

121 NSA 2011 Minimization Procedures, *supra*, § 6(c).

C. Upstream Collection

The NSA acquires communications from a second means, which is referred to as upstream collection. Upstream collection is different from PRISM collection because the acquisition occurs not with the compelled assistance of the United States ISPs, but instead with the compelled assistance (through a Section 702 directive) of the providers that control the telecommunications backbone over which communications transit.[122] The collection therefore does not occur at the local telephone company or email provider with whom the targeted person interacts (which may be foreign telephone or Internet companies, which the government cannot compel to comply with a Section 702 directive), but instead occurs "upstream" in the flow of communications between communication service providers.[123]

Unlike PRISM collection, raw upstream collection is not routed to the CIA or FBI, and therefore it resides only in NSA systems, where it is subject to the NSA's minimization procedures. [124] CIA and FBI personnel therefore lack any access to raw data from upstream collection. Accordingly, they cannot view or query such data in CIA or FBI systems.

The upstream acquisition of telephone and Internet communications differ from each other, and these differences affect privacy and civil liberty interests in varied ways.[125] Each type of Section 702 upstream collection is discussed below. In conducting both types of upstream acquisition, NSA employs certain collection monitoring programs to identify anomalies that could indicate that technical issues in the collection platform are causing data to be overcollected.[126]

---

122 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4; *see also* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA) ("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.").

123 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA) ("This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.").

124 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 4.

125 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 27 (statement of Rajesh De, General Counsel, NSA).

126 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 29.

1. Upstream Collection of Telephone Communications

Like PRISM collection, the upstream collection of telephone communications begins with the NSA's tasking of a selector.[127] The same targeting procedures that govern the tasking of an email address in PRISM collection also apply to the tasking of a telephone number in upstream collection.[128] Prior to tasking, the NSA therefore is required to assess that the specific telephone number to be tasked is used by a non-U.S. person reasonably believed to be located outside the United States from whom the NSA assesses it may acquire the types of foreign intelligence information authorized under one of the Section 702 certifications. Once the targeting procedures have been applied, the NSA sends the tasked telephone number to a United States electronic communication service provider to initiate acquisition.[129] The communications acquired, with the compelled assistance of the provider, are limited to telephone communications that are either to or from the tasked telephone number that is used by the targeted person. Upstream telephony collection therefore does not acquire communications that are merely "about" the tasked telephone number.[130]

2. Upstream Collection of Internet "Transactions"

The process of tasking selectors to acquire Internet transactions is similar to tasking selectors to PRISM and upstream telephony acquisition, but the actual acquisition is substantially different. Like PRISM and upstream telephony acquisition, the NSA may only target non-U.S. persons by tasking specific selectors to upstream Internet transaction collection.[131] And, like other forms of Section 702 collection, selectors tasked for upstream Internet transaction collection must be specific selectors (such as an email address), and may not be key words or the names of targeted individuals.[132]

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

---

127 PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA); *id*. at 51-53 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

128 NSA DCLPO REPORT, *supra*, at 6.

129 PCLOB March 2014 Hearing Transcript, *supra*, at 53-54 (statements of Rajesh De, General Counsel, NSA, and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

130 Bates October 2011 Opinion, *supra*, at 15, 2011 WL 10945618, at *5.

131 NSA DCLPO REPORT, *supra*, at 5-6.

132 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

communications, what is referred to as the "Internet backbone."[133] 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.[134]

Upstream collection acquires Internet transactions that are "to," "from," or "about" a tasked selector.[135] With respect to "to" and "from" communications, the sender or a recipient is a user of a Section 702–tasked selector. This is not, however, necessarily true for an "about" communication. An "about" communication is one in which the tasked selector is referenced within the acquired Internet transaction, but the target is not necessarily a participant in the communication.[136] If the NSA therefore applied its targeting procedures to task email address "JohnTarget@example.com," to Section 702 upstream collection, the NSA would potentially acquire communications routed through the Internet backbone that were sent from email address JohnTarget@example.com, that were sent to JohnTarget@example.com, and communications that mentioned JohnTarget@example.com in the body of the message. The NSA would not, however, acquire communications simply because they contained the name "John Target." In a still-classified September 2008 opinion, the FISC agreed with the government's conclusion that the government's target when it acquires an "about" communication is not the sender or recipients of the communication, regarding whom the government may know nothing, but instead the targeted user of the Section 702–tasked selector. The FISC's reasoning relied upon language in a congressional report, later quoted by the FISA Court of Review, that the

---

133 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4.

134 Bates October 2011 Opinion, *supra*, at 73, 2011 WL 10945618, at *26.

135 *See, e.g.*, October 2011 Opinion, *supra*, at 15-16, 2011 WL 10945618, at *5-6 (describing the government's representations regarding upstream collection in the first Section 702 certification the FISC reviewed).

136 Bates October 2011 Opinion, *supra*, at 15, 2011 WL 10945618, at *5; Joint Statement of Lisa O. Monaco, Assistant Attorney General, National Security Division, Dept. of Justice, et. al., *Hearing Before the House Permanent Select Comm. on Intelligence: FISA Amendments Act Reauthorization*, at 7 (Dec. 8, 2011) ("December 2011 Joint Statement") (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ), *available at* http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf; PCLOB March 2014 Hearing Transcript, *supra*, at 55.

"target" of a traditional FISA electronic surveillance "is the individual or entity . . . about whom or from whom information is sought."[137]

There are technical reasons why "about" collection is necessary to acquire even some communications that are "to" and "from" a tasked selector. In addition, some types of "about" communications actually involve Internet activity of the targeted person.[138] The NSA cannot, however, distinguish in an automated fashion between "about" communications that involve the activity of the target from communications that, for instance, merely contain an email address in the body of an email between two non-targets.[139]

In order to acquire "about" communications while complying with Section 702's prohibition on intentionally acquiring known domestic communications, the NSA is required to take additional technical steps that are not required for other Section 702 collection. 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.[140] If, for example, a person located in Chicago sent an email to a friend in Miami that mentioned the tasked selector "JohnTarget@example.com," the IP filters (or comparable technical means) are designed to prevent the acquisition of this communication. The IP filters, however, do not operate perfectly,[141] and may fail to filter out a domestic communication before it is screened against tasked selectors. A United States-based user, for example, may send a communication (intentionally or otherwise) via a foreign server even if the intended recipient is also in the United States.[142] As such, the FISC has noted the government's concession that in the ordinary course of acquiring single communications, wholly domestic communications could be acquired as much as 0.197% of the time.[143] While this percentage is small, the FISA court estimated in 2011 that the

---

137 *See In re Sealed Case*, 310 F. 3d 717, 740 (FISA Ct. Rev. 2002) (quoting H.R. Rep. 95-1283, at 73 (1978)); *see also* PCLOB March 2014 Hearing Transcript, *supra*, at 55 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (confirming the FISC had held that targeting includes communications about a particular selector that are not necessarily to or from that selector).

138 Bates October 2011 Opinion, *supra*, at 37-38, 2011 WL 10945618, at *12 (describing the types of acquired Internet transactions and noting that a subset involve transactions of the target).

139 Bates October 2011 Opinion, *supra*, at 31, 43, 2011 WL 10945618, at *10, *14 (describing limitations on what can be distinguished at the acquisition stage).

140 Bates October 2011 Opinion, *supra*, at 33, 2011 WL 10945618, at *11 (regarding the "technical measures" that NSA uses to prevent the acquisition of upstream collection of domestic communications); NSA DCLPO REPORT, *supra*, at 5-6 (acknowledging that IP filters are used to prevent the acquisition of domestic communications).

141 December 2011 Joint Statement, *supra*, at 7 (acknowledging measures to prevent acquisition of domestic communications "are not perfect").

142 Bates October 2011 Opinion, *supra*, at 34-35 n.33, 2011 WL 10945618, at *11 n.33.

143 Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11 n.32.

overall number of communications the government acquires through Section 702 upstream collection could result in the government acquiring as many as tens of thousands of wholly domestic communications per year.[144]

In addition, wholly domestic communications could also be acquired because they were embedded in a larger multi-communication transaction ("MCT"), the subject of the next section.

3. Upstream Collection of Internet Communications: Multi-Communication Transactions ("MCTs")

While the NSA's upstream collection is intended to acquire Internet *communications*, it does so through the acquisition of Internet *transactions*. The difference between *communications* and *transactions* is a significant one, and the government's failure to initially distinguish and account for this distinction caused the FISA court to misunderstand the nature of the collection for over two years, and later to find a portion of the Section 702 program to be unconstitutional.

The NSA-designed upstream Internet collection devices acquire transactions as they cross the Internet. An Internet transaction refers to any set of data that travels across the Internet together such that it may be understood by a device on the Internet.[145] An Internet transaction could consist of a single discrete communication, such as an email that is sent from one server to another. Such communications are referred to as single communication transactions (SCTs).[146] Of the upstream Internet transactions that the NSA acquired in 2011, approximately ninety percent were SCTs.[147]

In other instances, however, a single Internet transaction might contain multiple discrete communications. These transactions are referred to as MCTs.[148] If a single discrete communication within an MCT is to, from, or about a Section 702–tasked selector, and at least one end of the transaction is foreign, the NSA will acquire the entire MCT.[149]

If the acquired MCT is a transaction between the Section 702 target (who is assessed to be a non-U.S. person located outside the United States and is targeted to acquire foreign intelligence information falling under one of the approved certifications) and a server, then

---

144 Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11 n.32; December 2011 Joint Statement, *supra*, at 7.

145 *See* Bates October 2011 Opinion, *supra*, at 28 n.23, 2011 WL 10945618, at *9 n.23 (quoting government characterization of what constitutes an Internet transaction).

146 Bates October 2011 Opinion, *supra*, at 27-28, 2011 WL 10945618, at *9.

147 Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11 n.32.

148 Bates October 2011 Opinion, *supra*, at 28, 2011 WL 10945618, at *9.

149 December 2011 Joint Statement, *supra*, at 7.

all of the discrete communications acquired within the MCT are also communications to or from the target. Based on a statistical sample conducted by the NSA, the FISC estimated that as of 2011 the NSA acquired between 300,000 and 400,000 such MCTs every year (i.e., MCTs where the "active user,"[150] was the target him or herself).[151]

When the acquired MCT is not a transaction between the target and the server, but instead a transaction between another individual and a server that happens to include a Section 702 tasked selector, the MCT may "include communications that are not about a tasked selector and may have no relationship, or no more than an incidental relationship to the [tasked] selector."[152] These non-target MCTs break down into three categories. Based on the NSA's statistical study, the FISC estimated that (as of 2011) the NSA acquired at least 1.3 million MCTs each year where the user who caused the transaction to occur was not the target, but was located outside the United States.[153] Using this same statistical analysis, the FISA court estimated that the NSA would annually acquire an additional approximately 7,000 to 8,000 MCTs of non-targeted users who were located in the United States, and between approximately 97,000 and 140,000 MCTs each year where NSA would not be able to determine whether the user who caused the transaction to occur was located inside or outside the United States.[154]

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."[155] While some distinction between SCTs and MCTs can be made with respect to some communications in conducting acquisition, the government has not been able to design a filter that would acquire only the single discrete communications within transactions that contain a Section 702 selector. This is due to the constant changes in the protocols used by Internet service providers and the services provided.[156] If time

---

150 The "active user" is the actual human being who is interacting with a server to engage in an Internet transaction.

151 Bates October 2011 Opinion, *supra*, at 38, 2011 WL 10945618, at *12.

152 December 2011 Joint Statement, *supra*, at 7.

153 Bates October 2011 Opinion, *supra*, at 39, 2011 WL 10945618, at *12.

154 Bates October 2011 Opinion, *supra*, at 38-40, 2011 WL 10945618, at *12. With respect to this last category, the unidentified user could be the Section 702 target. *Id.* at 38, 40-41, 2011 WL 10945618, at *12.

155 Bates October 2011 Opinion, *supra*, at 31, 2011 WL 10945618, at *10. In 2011, the NSA was able to determine that approximately 90 percent of all upstream Internet transactions consisted of SCTs as the result of a post-acquisition statistical sample that required a manual review. *Id.* at 34 n.32, 2011 WL 10945618, at *11.

156 Bates October 2011 Opinion, *supra*, at 32, 2011 WL 10945618, at *10.

were frozen and the NSA built the perfect filter to acquire only single, discrete communications, that filter would be out-of-date as soon as time was restarted and a protocol changed, a new service or function was offered, or a user changed his or her settings to interact with the Internet in a different way. Conducting upstream Internet acquisition will therefore continue to result in the acquisition of some communications that are unrelated to the intended targets.

The fact that the NSA acquires Internet communications through the acquisition of Internet transactions, be they SCTs or MCTs, has implications for the technical measures, such as IP filters, that the NSA employs to prevent the intentional acquisition of wholly domestic communications. With respect to SCTs, wholly domestic communications that are routed via a foreign server for any reason are susceptible to Section 702 acquisition if the SCT contains a Section 702 tasked selector.[157] With respect to MCTs, wholly domestic communications also may be embedded within Internet transactions that also contain foreign communications with a Section 702 target. The NSA's technical means for filtering domestic communications cannot currently discover and prevent the acquisition of such MCTs.[158]

Because of the greater likelihood that upstream collection of Internet transactions, in particular MCTs, will result in the acquisition of wholly domestic communications and extraneous U.S. person information, there are additional rules governing the querying, retention, and use of such upstream data in the NSA minimization procedures. These additional procedures are discussed below.

IV. Targeting Procedures: Who May Be Targeted? How? And Who Decides?

As is discussed above, the government targets persons under Section 702 by tasking selectors — communication facilities, such as email addresses and telephone numbers — that the government assesses will be used by those persons to communicate or receive foreign intelligence information that falls within one of the authorized Section 702 certifications.[159] Under Section 702, this targeting process to determine which persons are (1) non-U.S. persons, that are (2) reasonably believed to be located outside the United States, who will (3) use the tasked selectors to communicate or receive foreign intelligence

---

157 Bates October 2011 Opinion, *supra*, at 34-35, n.32 & n.33; *id*. at 45, 2011 WL 10945618, at *11 ("[T]he government readily concedes that NSA will acquire a wholly domestic "about" communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server.")

158 Bates October 2011 Opinion, *supra*, at 45, 47, 2011 WL 10945618, at *15.

159 *See, e.g.*, AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-2.

information is governed by targeting procedures.[160] While the targeting procedures are subject to judicial review by the FISC,[161] individual targeting determinations made under these targeting procedures are not reviewed by the FISC (but are subject to internal Executive oversight, as detailed below).[162]

Both the NSA and FBI have targeting procedures that govern the process by which persons may be targeted under Section 702.[163] While some information has been released by the government, neither the NSA nor the FBI targeting procedures have been declassified in full. The NSA's Section 702 targeting procedures take primary importance because only the NSA may initiate Section 702 collection.[164] The FBI's Section 702 targeting procedures, which are discussed further below, are applied to certain selectors only after the NSA has previously determined under the NSA targeting procedures that these selectors qualify for Section 702 targeting.[165] Although the NSA initiates all Section 702 targeting, and thus makes all initial decisions pursuant to its targeting procedures regarding whether a person qualifies for Section 702 targeting under one of the Section 702 certifications, the CIA and FBI have processes to "nominate" targets to the NSA for Section 702 targeting.[166] It is the NSA, however, that must make the determination whether to initiate targeting.

Section 702 targeting begins when an NSA analyst discovers or is informed of a foreign intelligence lead — specifically, information indicating that a particular person may possess or receive the types of foreign intelligence information described within one of the Section 702 certifications.[167] Lead information could come from any of multiple sources, including human intelligence, signals intelligence or other sources such as law enforcement information. Because Section 702 acquisition is selector-based, the NSA analyst must also

---

160 *See* 50 U.S.C. § 1881a(d)(1) (requirement for targeting procedures); AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-1 (general scope of what is covered by those targeting procedures).

161 50 U.S.C. § 1881a(d)(2).

162 NSA DCLPO REPORT, *supra*, at 2, 4-5.

163 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 6, 9.

164 *See* The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3 (noting that "NSA takes the lead in targeting and tasks both telephone and electronic communications selectors to acquire communications); AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 6 ("[A]ll Section 702 targeting is initiated pursuant to the NSA's targeting procedures.").

165 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

166 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-8, A-12.

167 NSA DCLPO REPORT, *supra*, at 4.

discover or be informed of a specific selector used by this potential target that could be tasked to PRISM and/or upstream collection.[168]

Having identified a potential person to target through the tasking of a selector, the NSA analyst must then apply the targeting procedures. These procedures require the NSA analyst to make a determination regarding the assessed location and non-U.S. person status of the potential target (the *foreignness determination*)[169] and whether the target possesses and/or is likely to communicate or receive foreign intelligence information authorized under an approved certification (the *foreign intelligence purpose determination*).[170]

A. Foreignness Determination

With respect to the *foreignness determination*, the NSA analyst is required to assess whether the target of the acquisition is a non-U.S. person reasonably believed to be located outside the United States based upon the totality of the circumstances available.[171] This analysis begins with a review of the initial lead information, which must be examined to determine whether it indicates either the location or the U.S. person status of the potential target.[172] At times, the lead information itself will state where the target is assessed to be located and their U.S. person status. In other instances, this information may only enable an analyst to infer location or U.S. person status. In either case, the Section 702 targeting determination may not be made upon the lead information alone. Instead, the NSA analyst must check multiple sources and make a determination based on the totality of the circumstances available to the analyst.[173]

The government has stated that in making this foreignness determination the NSA targeting procedures inherently impose a requirement that analysts conduct "due diligence" in identifying these relevant circumstances. What constitutes due diligence will

---

168 NSA DCLPO REPORT, *supra*, at 4.

169 PCLOB March 2014 Hearing Transcript, *supra*, at 41 (statement of Rajesh De, General Counsel, NSA) (stating that "foreignness determination" is a "shorthand for referring to the determination that [the target] is a non-U.S. person reasonably located to be abroad").

170 PCLOB March 2014 Hearing Transcript, *supra*, at 61 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (describing individualized foreign intelligence purpose determination which must be documented as part of the tasking process).

171 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 42 (statement of Rajesh De, General Counsel, NSA) (noting that foreignness determination is a "totality of the circumstances" test).

172 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

173 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 41 (statement of Rajesh De, General Counsel, NSA) (in describing foreignness determination, stating that "an analyst must take into account all available information. . . [A]n analyst cannot ignore any contrary information to suggest that that is not the correct status of the person.")

vary depending on the target; tasking a new selector used by a foreign intelligence target with whom the NSA is already quite familiar may not require deep research into the target's (already known) U.S. person status and current location, while a great deal more effort may be required to target a previously unknown, and more elusive, individual. As previously discussed above, a failure by an NSA analyst to conduct due diligence in identifying relevant circumstances regarding the location and U.S. person status of a Section 702 target is a reportable compliance incident to the FISC.

After conducting due diligence and reviewing the totality of the circumstances, the NSA analyst is required to determine whether the information indicates that the target is a non-U.S. person reasonably believed to be located outside the United States.[174] The government has stated, and the Board's review has confirmed, that this is not a "51% to 49% test."[175] If there is conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved and the user must be determined to be a non-U.S. person reasonably believed to be located outside the United States prior to targeting.[176]

While conflicting information must be resolved, the standard for making the foreignness determination is not a probable cause standard. Through the application of the NSA targeting procedures over the years and interactions with and between and among NSA personnel and external DOJ/Office of the Director of National Intelligence ("ODNI") overseers, a common understanding has been developed regarding what constitutes a sufficient basis for determining that a potential Section 702 target is a non-U.S. person reasonably believed to be located outside the United States. The NSA targeting procedures include a process for assessing non-U.S. person's status. This determination may not be made unless the analyst has first undertaken due diligence.

In 2013, the DOJ undertook a review designed to assess how often the foreignness determinations that the NSA made under the targeting procedures as described above turned out to be wrong — i.e., how often the NSA tasked a selector and subsequently realized after receiving collection from the provider that a user of the tasked selector was either a U.S. person or was located in the United States. The DOJ reviewed one year of data and determined that 0.4% of NSA's targeting decisions resulted in the tasking of a selector that, as of the date of tasking, had a user in the United States or who was a U.S. person. As is discussed in further detail below, data from such taskings in most instances must be

---

174 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 40-42 (statement of Rajesh De, General Counsel, NSA).

175 PCLOB March 2014 Hearing Transcript, *supra*, at 40-41 (statement of Rajesh De, General Counsel, NSA).

176 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 40-42 (statement of Rajesh De, General Counsel, NSA).

purged. The purpose of the review was to identify how often the NSA's foreignness determinations proved to be incorrect. Therefore, the DOJ's percentage does not include instances where the NSA correctly determined that a target was located outside the United States, but post-tasking, the target subsequently traveled to the United States.

B. Foreign Intelligence Purpose Determination

In addition to the foreignness determination, the NSA analyst must also make a *foreign intelligence purpose determination*. Specifically, the NSA targeting procedures require that the NSA determine that tasking the selector will be likely to acquire one of the types of foreign intelligence information identified in a Section 702 certification.[177] In making this determination, the NSA analyst must identify the specific foreign power or foreign territory concerning which the foreign intelligence information is being sought.[178] The NSA targeting procedures include a non-exclusive list of factors that the NSA will consider in determining whether the tasking of a selector will be likely to result in foreign intelligence information falling within one of the Section 702 certifications.

C. Documentation Requirements

The NSA targeting procedures contain documentation requirements with respect to aspects of the foreignness and foreign intelligence purpose determinations. Analysts are required under the NSA targeting procedures to cite the specific documents and communications that led them to assess that the Section 702 target is located outside the United States.[179] As a practical matter, these citations are accompanied by a narrative explaining what the documents and communications indicate with regard to the location of the target. In other words, with respect to the determination regarding the location of the target, analysts must "show their work." Although analysts are required under the targeting procedures to conduct an analysis regarding why the targeting of the individual will result in obtaining foreign intelligence information under the Section 702 certifications, analysts are not required to document (i.e., show their work) this foreign intelligence purpose determination in the same manner as they are required to document the foreignness determination. With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to "identify" the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired.[180] By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence

---

177 NSA DCLPO REPORT, *supra*, at 4.

178 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-5 (noting that the identified foreign power or foreign territory must be documented).

179 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-5; *see also* NSA DCLPO REPORT, *supra*, at 4-5.

180 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-5.

long) that further explains the analyst's rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certifications.[181]

In the Board's view, this reduced documentation regarding the foreign intelligence purpose determination results in a less rigorous review by the NSA's external overseers of the foreign intelligence purpose determinations than the NSA's foreignness determination. Also as a matter of NSA policy, as opposed to a requirement in the NSA targeting procedures, NSA analysts document the assessed non-U.S. person status of the target, but analysts do not separately document the basis for this non-U.S. person determination. In general, however, the non-U.S. person analysis is based upon same information that underlies the determination regarding the target's location.

D. Approvals

Once analysts have documented their determinations in an NSA tasking database,[182] the tasking request undergoes two layers of review before actual Section 702 acquisition is initiated.[183] Two different senior NSA analysts must review the documentation accompanying the tasking request to ensure that it meets all of the requirements of the NSA targeting procedures.[184] Both NSA senior analysts receive additional training to review tasking requests.[185] Both senior analysts may also request additional information prior to approving or denying the Section 702 tasking request.[186] Both senior analysts are required to review all aspects of the tasking before approving the tasking request.[187]

Once the tasking request receives all of the necessary approvals, it is sent to one or more electronic communication service providers that have received a Section 702 directive in order to initiate Section 702 acquisition.[188] The tasking request, however, is subjected to further post-tasking review by the DOJ/ODNI review team,[189] as is discussed in the "External Oversight" section below.

---

181 *See generally* PCLOB March 2014 Hearing Transcript, *supra*, at 59 (statement of Rajesh De, General Counsel, NSA) (discussing foreign intelligence purpose determination and noting that it must be "documented in a targeting rationale document").

182 August 2013 Semiannual Assessment, *supra*, at A-5.

183 NSA DCLPO REPORT, *supra*, at 5.

184 NSA DCLPO REPORT, *supra*, at 5.

185 NSA DCLPO REPORT, *supra*, at 5.

186 NSA DCLPO REPORT, *supra*, at 5.

187 NSA DCLPO REPORT, *supra*, at 5.

188 NSA DCLPO REPORT, *supra*, at 5.

189 NSA DCLPO REPORT, *supra*, at 5; AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 6-7.

E. CIA and FBI Nominations

The CIA and FBI have both developed processes to nominate selectors to the NSA to be tasked for Section 702 acquisition.[190] The NSA evaluates the CIA and FBI nominations under the same targeting procedures and using the same processes that are described above. It is the NSA that is ultimately responsible for the tasking of such facilities. In order to ensure that the NSA's foreignness and foreign intelligence purpose determinations regarding the CIA and FBI nominations are made on accurate and current information, both the CIA and FBI have implemented internal requirements prior to formally nominating a selector to the NSA for acquisition. For example, the CIA nominations are reviewed and approved by the targeting officer's first line manager, a legal officer, a senior operational manager, and the CIA's FISA Program office prior to being exported to the NSA.[191] These internal procedures are in addition to the NSA documentation and approval requirements required for all taskings.

F. FBI Targeting Procedures

The FBI's targeting procedures govern certain aspects of the PRISM program; specifically, requests for certain communications for selectors that have already been determined by the NSA to have met its targeting procedures. As the NSA has already made a foreignness determination with respect to any selector for which the FBI will be acquiring communications, the FBI's role in targeting is substantially different than that of the NSA.[192] Instead of establishing the required information to indicate that a Section 702 target is a non-U.S. person reasonably believed to be located outside the United States who is likely to communicate or receive foreign intelligence information, the FBI targeting procedures are intended to "provide additional assurance that the users of tasked accounts are non-United States persons located outside the United States."[193] The FBI targeting procedures therefore require the FBI to both review the NSA's foreignness determinations[194] and review information available to the FBI. FBI personnel who process tasking requests receive training in both the FBI targeting procedures and a detailed set of standard operating procedures that describe the steps that the FBI must take to ensure that they

---

190 *See supra* footnote 1664 and accompanying text.

191 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-8; *see also* AUGUST 2013 SEMIANNUAL ASSESSMENT at 36 (describing compliance incident related to an FBI nomination that stemmed from reliance on an unsupported fact).

192 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

193 Bates October 2011 Opinion, *supra*, at 22, 2011 WL 10945618, at *7.

194 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

have conducted due diligence in looking for information that may alter or affect the NSA's foreignness assessment.[195]

V. Post-Tasking Review and Related Reporting and Purging Requirements

In addition to defining the process by which Section 702 tasking will be initiated, the NSA targeting procedures also impose additional post-tasking requirements designed to ensure that the users of tasked selectors remain non-U.S. persons located outside the United States and that acquisition against the selector continues only insofar as the government assesses that the tasking is likely to acquire foreign intelligence information within one of the authorized Section 702 certifications. The manner in which the post-tasking checks required by the NSA targeting procedures will be implemented has been supplemented by additional filings by the government with the FISC. The government has reported to the FISA court and Congress as compliance incidents instances in which its implementation of the required post-tasking checks did not correspond with these additional representations to the court.

NSA analysts are required to routinely review at least a sample of the Section 702–acquired communications for selectors that they have tasked to ensure that the selectors remain properly tasked.[196] The NSA has developed automated systems to remind analysts to review collection from email addresses and comparable selectors within five business days after the first instance that data is acquired for a particular tasked selector, and at least every 30 days thereafter; comparable systems have to-date not been implemented with respect to Section 702 acquisition of upstream telephony collection. The analysts review the content to verify that the selector is associated with the foreign intelligence target, as well as look for any information indicating that a user of the selector is a U.S. person or located in the United States.[197] The NSA also requires analysts to re-verify at least once a year that each selector continues to be tasked in order to acquire the types of foreign intelligence information specified in the certification under which the selector is tasked. The CIA and FBI have each implemented their own comparable policies and practices mandating that analysts, agents, and officers initially review and periodically verify data acquired from selectors nominated by the CIA and FBI to ensure the selectors remain properly tasked for Section 702 acquisition.

---

195 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 36, A-11 to A-12.

196 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-4; NSA DCLPO REPORT, *supra*, at 6.

197 NSA DCLPO REPORT, *supra*, at 6; *see also* PCLOB March 2014 Hearing Transcript, *supra*, at 42 (statement of Rajesh De, General Counsel, NSA) (noting that "analysts have an affirmative obligation to periodically revisit the foreignness determination")

In addition to this content review, the NSA is required to conduct routine post-tasking checks of all Section 702–tasked selectors.[198]

If it is determined that a user of a tasked selector is either in the United States or is a U.S. person, the selector is required to be promptly detasked from Section 702 acquisition (i.e., all Section 702 acquisition directed at that selector must be terminated).[199] Any other Section 702–tasked selectors assessed to be used by the individual determined to be a U.S. person or located in the United States must also be promptly detasked.[200] Additionally, selectors must be detasked if the government determines that it will not obtain the types of foreign intelligence information authorized under the Section 702 certifications.[201] Failure to detask a selector from Section 702 acquisition after it has been (or, based on the available information, should have been) determined to be ineligible for further Section 702 acquisition is a compliance incident that must be reported first to the DOJ and ODNI, and in turn to the FISC and Congress.[202]

If it is learned that a tasked selector is being used by a U.S. person or person located in the United States, the data acquired from the selector while it was being used by the U.S. person or person located in the United States is subject to purge, with limited exceptions.[203] If the data was acquired as a result of a compliance incident — because, for example, there was an error in the tasking (e.g., typographical error, lack of due diligence tasking, etc.); an error in detasking (insufficiently prompt detasking); or an overproduction by the provider — the acquired communications must be purged.[204] In cases where there is no underlying compliance incident but a user is determined to be a U.S. person or a person located in the United States (e.g., the government had a reasonable, but ultimately mistaken, belief that a target was located outside the United States), a purge of acquired communications is also required.[205]

---

198 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 6.

199 NSA DCLPO REPORT, *supra*, at 6; *see also* NSA October 2011 Minimization Procedures, *supra*, § 3(d)(1).

200 NSA DCLPO REPORT, *supra*, at 6; *see also* NSA October 2011 Minimization Procedures, *supra*, § 3(d)(1).

201 NSA DCLPO REPORT, *supra*, at 6.

202 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7 (noting that the NSA must report all instances in which a target is found to be located in the United States, but that such incidents are only compliance incidents if the NSA "knew or should have known the target was in the United States during the collection period"); *id*. at 25-27, 29, 33 (describing the category of detasking incidents and specific detasking incidents); NSA DCLPO REPORT, *supra*, at 3 (summarizing reporting process).

203 NSA DCLPO REPORT, *supra*, at 8.

204 *See, e.g.,* PCLOB March 2014 Hearing Transcript, *supra*, at 72.

205 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-12 (noting that all of the agency minimization procedures require purges when a target is discovered to be a U.S. person or person located in the United States, with limited exceptions).

Certain exceptions apply, however, in instances where the communications were not acquired as the result of a violation of the targeting or minimization procedures. The NSA minimization procedures permit the Director (or Acting Director) of the NSA to waive, on a communication-by-communication basis, specific communications determined to contain "significant foreign intelligence information" or information that is not foreign intelligence information but is "evidence of a crime."[206] The CIA and FBI standards for executing a waiver are similar. Additionally, and notwithstanding the general purge requirement and the specific waiver exceptions, the NSA may also inform the FBI that a target has entered the United States so that the FBI make seek traditional FISA electronic surveillance of the target or take other lawful investigative steps.[207] The NSA may also retain and disclose to the FBI and CIA certain technical data for collection avoidance purposes.[208]

VI. Minimization and Related Requirements: What Are the Limitations Regarding How the Data is Acquired, Who May View It, How Long It Is Retained, and with Whom It May be Shared?

Minimization is one of the most confusing terms in FISA. Like traditional FISA electronic surveillance and physical search,[209] Section 702 requires that all acquired data be subject to "minimization procedures."[210] Minimization procedures are best understood as a set of controls on data to balance privacy and national security interests. Specifically, under FISA, minimization procedures must be "specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance *to minimize the acquisition and retention, and prohibit the dissemination,* of nonpublicly available information concerning unconsenting United States persons *consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.*"[211] Minimization procedures must also contain special limitations on the dissemination of U.S.

---

206 NSA October 2011 Minimization Procedures, *supra*, § 5(1) and (2). The NSA's minimization procedures also allow for the Director of the NSA to waive the purge of a communication that is assessed to contain "technical data base information," "information necessary to understand or assess a communications security vulnerability," or "information pertaining to a threat of serious harm to life or property." NSA October 2011 Minimization Procedures § 5(3), (4). To date, no waivers have been granted under these additional provisions.

207 NSA October 2011 minimization procedures, *supra*, § 5.

208 NSA October 2011 minimization procedures, *supra*, § 5.

209 *See* 50 U.S.C. §§ 1805(a)(3) and 1824(a)(3).

210 50 U.S.C. § 1881a(e).

211 50 U.S.C. 1801(h)(1) (emphasis added).

person identities with respect to certain types of foreign intelligence information,[212] as well as allow for the retention and dissemination of evidence of a crime to law enforcement entities.[213] These statutory requirements obligate the Attorney General to adopt procedures that balance the at times competing interests in protecting the privacy of U.S. persons and the Intelligence Community's production of foreign intelligence information to meet national security requirements. In addition, although the minimization procedures must be designed to protect U.S. persons' privacy, the procedures will at times provide controls on data that protect the privacy of non-U.S. persons as well.

This section describes the controls imposed by the Section 702 minimization procedures on acquisition, access (and related training requirements), querying, retention (and purging), and dissemination. The NSA's 2011 Section 702 minimization procedures have been publicly released.[214] Minimization procedures for the CIA, FBI, and National Counterterrorism Center ("NCTC")[215] have not been publicly released to date, though some information regarding these procedures has been declassified. Although the minimization procedures for each agency have many similarities, there are differences between the agencies' minimization procedures that are related to the different authorities of the respective agencies and the way each uses the Section 702–acquired data.[216] Some of these differences impact privacy concerns.

All Section 702–acquired data, both content and metadata, is subject to the Section 702 minimization procedures.[217]

A. Acquisition

The minimization procedures of agencies that conduct acquisition — in the case of Section 702, the NSA and FBI — must contain provisions that minimize the acquisition of U.S. person information consistent with the authorized purpose of the collection. The first minimization of the acquisition of U.S. person information, however, stems from the targeting requirements imposed by the statute itself. As an initial matter, Section 702

---

212 50 U.S.C.§ 1801(h)(2) (further limiting dissemination of U.S. person identities with regard to foreign intelligence information as defined by § 1801(e)(2), but not § 1801(e)(1)).

213 50 U.S.C.§ 1801(h)(3).

214 *See* NSA 2011 Minimization Procedures, *supra*, *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

215 As described below, the NCTC's role in processing and minimizing Section 702 data is limited. *See* AUGUST 2013 JOINT ASSESSMENT, *supra*, at 4 n.2.

216 PCLOB March 2014 Hearing Transcript, *supra*, at 18-19 (discussion between David Medine, Chairman, PCLOB, and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

217 PCLOB March 2014 Hearing Transcript, *supra*, at 19.

prohibits the intentional targeting of U.S. persons, the intentional targeting of persons located in the United States, reverse targeting, or the intentional acquisition of communications known to be wholly domestic at the time of acquisition.[218] Each of these statutory requirements is designed to reduce, though not eliminate, the acquisition of U.S. person information.

The NSA minimization procedures therefore start with a requirement that Section 702 collection be conducted in accordance with the Section 702 certification, and "in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose."[219] This mandate applies to both the NSA's acquisition and the technical assistance provided by the FBI in acquiring communications.[220] Affidavits accompanying the certifications, witness testimony in hearings before the FISC, and additional filings before the court describe how the NSA and FBI will actually conduct the acquisition in a manner that the government believes will be reasonably designed to minimize the acquisition of information that is irrelevant to the acquisition of the foreign intelligence information specified in the Section 702 certifications.[221] These representations detail the method and techniques by which the collection of PRISM and upstream collection is conducted, as described above. A failure to implement the acquisition in a manner that reasonably limits the collection to the authorized purpose of the Section 702 certifications can, and has, led to incidents of noncompliance with the minimization procedures that have been reported to the FISC and Congress.[222]

In addition to actually acquiring the data, certain technical actions must be undertaken at or just after the acquisition stage in order to facilitate later compliance with other minimization rules. For example, data-tagging Section 702–acquired data at, or just after, acquisition is also employed to effectuate other access and routing controls, certain

---

218 50 U.S.C. § 1881a(a), (b).

219 NSA October 2011 Minimization Procedures, *supra*, § 3(a).

220 *See* NSA October 2011 Minimization Procedures, *supra*, § 2(a) (defining "acquisition" as "the collection by NSA or the FBI through electronic means of a non-public communication to which it is not an intended party").

221 *See, e.g.,* Bates October 2011 Opinion, *supra*, at 5-10, 2011 WL 10945618, at *2-3 (describing various government submissions regarding how the government conducts Section 702 upstream collection); *id*. at 15-16, 2011 WL 10945618, at *5 (describing comparable descriptions in prior dockets); *id*. at 29-41, 2011 WL 10945618, at *9-13 (further describing government descriptions regarding how the government conducts Section 702 upstream collection).

222 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 31 (describing "compliance incidents during this reporting period [that] resulted in NSA's systems overcollecting data beyond what was authorized under the Section 702 certifications").

controls limiting the scope of queries, and age-off and purge requirements. Each of these controls is discussed further below.

B. Access and Training

Although the minimization process begins with acquisition, FISA-acquired data that has yet to be reviewed and evaluated by a human being is still referred to by the government as being "unminimized" or "raw" data. The NSA, CIA, and FBI are the three Intelligence Community agencies that have access to such unminimized Section 702–acquired data.[223] Each agency limits access to unminimized Section 702–acquired data to personnel who have been trained to apply their respective agency's minimization procedures. To enforce these restrictions, all unminimized Section 702–acquired data must be stored in repositories with access controls designed to prevent unauthorized access of the data by those within or outside of the relevant agency.

The NSA's core access and training requirements are found in the NSA's targeting procedures, which have not been released to the public. NSA analysts are required to undergo mandatory training and must pass a test regarding the requirements of the Section 702 minimization procedures (among other legal requirements) prior to receiving access to unminimized Section 702–acquired data.[224]

The CIA's minimization procedures similarly limit access to unminimized Section 702–acquired data to analysts who have received training in the CIA minimization procedures.[225] The CIA conducts in-person training regarding its minimization procedures before its personnel receive access to Section 702 data repositories and also embeds FISA-trained attorneys with CIA personnel to answer questions on the application of those minimization procedures to actual collection.[226]

The FBI has created a mandatory online training course that must be taken before FBI agents or analysts are granted access to repositories of unminimized Section 702–acquired data.[227] The Department of Justice's National Security Division ("NSD") and the FBI also conduct in-person trainings at FBI field offices.[228]

---

223 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-12.

224 NSA DCLPO REPORT, *supra*, at 4.

225 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

226 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

227 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 14 and A-12; *see also* PCLOB March 2014 Hearing Transcript at 86 (statement of James A. Baker, General Counsel, FBI) (confirming that access controls exists for FBI systems holding Section 702–acquired data).

228 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 14.

When an analyst, agent, or officer is granted access to unminimized Section 702–acquired data after receiving the requisite training, this does not mean that the agent or analyst has access to all such data. Agencies separate acquired data as a security measure. Furthermore, the CIA and FBI do not have copies of all Section 702–acquired data as neither agency receives all PRISM data acquired by the NSA, nor does either agency receive upstream collection.[229]

In addition to these general access and training requirements, the NSA's minimization procedures impose supplemental requirements with respect to certain Internet transactions. When the "active user" (i.e., the actual human being who is interacting with a server to engage in an Internet transaction) associated with an MCT is either reasonably believed to be located in the United States, or when the NSA cannot determine where the active user is located, the NSA must segregate the MCT in a special access-controlled repository.[230] Only analysts who have been trained in how to review such communications to identify any wholly domestic communications within such MCTs are permitted access to this repository.[231] A multi-communication transaction may not be moved out of the special-access repository or otherwise used unless it has been determined that none of the discrete communications that make up the MCT are wholly domestic communications.[232] If an MCT within this repository is determined to contain a wholly domestic communication, it must be destroyed upon recognition.[233] The CIA and FBI do not have access to any unminimized Section 702–acquired upstream collection.[234]

Separately, certain access and training requirements are imposed by the NCTC's Section 702 minimization procedures. The NCTC does not have access to unminimized Section 702–acquired data.[235] The NCTC has, however, been provided access to certain FBI systems that contain Section 702–acquired data that has been minimized to meet the FBI's dissemination standard. Minimization in this context means that any nonpublicly available Section 702–acquired U.S. person information in these FBI systems has been determined to either to be foreign intelligence information, necessary to understand or assess the importance of foreign intelligence information, or evidence of a crime.[236] U.S. person information that is evidence of a crime but is not otherwise foreign intelligence

---

229 Bates October 2011 Opinion, *supra*, at 18 n.17, 2011 WL 10945618, at *6 n.17.

230 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(a).

231 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(a)(1).

232 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(a)(1)(a).

233 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(a)(1)(a).

234 Bates October 2011 Opinion, *supra*, at 18 n.17, 2011 WL 10945618, at *6 n.17.

235 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 4 n.2.

236 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 4 n.2.

information, however, may only be disseminated for law enforcement purposes,[237] and the NCTC is not a law enforcement agency.[238] The NCTC Section 702 minimization procedures require NCTC personnel who have been granted access to these FBI systems to first be trained to not use, retain, or disseminate purely law enforcement information, and to purge any such Section 702–acquired information from NCTC systems if it has been ingested.[239]

C. Querying the Acquired Data

The NSA, CIA, and FBI's Section 702 minimization procedures all permit these agencies to query unminimized Section 702–acquired information. A "query" refers to any instance where data is searched using a specific term or terms for the purpose of discovering or retrieving unminimized Section 702–acquired content or metadata. A query "term" or "identifier" is just like a search term that is used in an Internet search engine — the term could be, for example, an email address, a telephone number, a key word or phrase, or a specific identifier that an agency has assigned to an acquired communication.[240] Queries are conducted using one or more of such terms or identifiers. Section 702 queries are of data that has already been acquired through the tasking of selectors as described above. A query therefore does not cause the government to collect any new communications, but queries do permit the government to more efficiently search through and discover information in the data the government has already acquired.[241]

An aspect common to the implementation of the query provisions in all of the Section 702 minimization procedures is that an analyst or agent only receives unminimized Section 702–acquired data as a result of a query if that analyst or agent has the appropriate training and authorization to access the Section 702 data. Different agencies accomplish this in different ways. For example, the CIA limits access to the database containing unminimized Section 702–acquired data to personnel who have received training in the CIA's Section 702 minimization procedures, thereby preventing untrained individuals from conducting queries of this data. The NSA, on the other hand, often stores data acquired from multiple legal authorities in a single data repository. Instead of limiting access to whole databases, the NSA tags each acquired communication with the legal authority under which it was acquired, and then has systems that prevent an analyst from accessing or querying data acquired under a legal authority for which the analyst does not have the

---

237 50 U.S.C. § 1801(h)(3).

238 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 4 n.2.

239 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 4 n.2.

240 *See, e.g.,* NSA DCLPO REPORT, *supra*, at 6; NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6).

241 PCLOB March 2014 Hearing Transcript, *supra*, at 29-31 (statements of Rajesh De, General Counsel, NSA and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

requisite training.[242] At the FBI, an agent or analyst who conducts a "federated query" across multiple databases, but who does not have Section 702 training, would not receive the Section 702–acquired information as the result of a query. The agent or analyst would, however, be notified in their query results of the fact that there is responsive information to their query in a database containing unminimized Section 702–acquired information to which he or she does not have access. In order to gain access to this information, the analyst or agent would need to either take the requisite training to gain access to the Section 702 information or contact a fellow agent or analyst who had the requisite training to determine whether the responsive results can be disseminated pursuant to the minimization procedures.

The NSA's intelligence analysts conduct at times complex queries across large data sets. The NSA's minimization procedures require that queries of unminimized Section 702–acquired information be designed such that they are "reasonably likely to return foreign intelligence information."[243] This prohibition against overbroad queries (such as a query for the term "river" across all Section 702–acquired data with no other limiting query terms) or queries conducted for purposes other than to identify foreign intelligence information (such as an analyst's query to find information about a girlfriend) applies to all of the NSA queries of unminimized Section 702–acquired information, not just queries containing U.S. person identifiers.[244] NSA analysts receive training regarding how to use multiple query terms or other query discriminators (like a date range) to limit the information that is returned in response to their queries of the unminimized data.[245] Through various means, the NSA systems record all queries of unminimized Section 702–acquired data, and these records are subject to audit.[246]

Additional rules apply when an NSA analyst wants to use a U.S. person identifier — i.e., a query term associated with a specific U.S. person, such as an email address or telephone number — to query unminimized Section 702–acquired data. U.S. person identifiers are prohibited from being used to query the NSA's Section 702 upstream collection of Internet transactions.[247] In contrast, the NSA's upstream telephony collection

---

242 *See* NSA DCLPO REPORT, *supra*, at 6-7.

243 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6).

244 *See* NSA DCLPO REPORT, *supra*, at 6-7 (discussing general query restrictions prior to detailing the additional requirements with regard to U.S. person identifiers).

245 NSA DCLPO REPORT, *supra*, at 6-7; *see also* NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6) (noting that "other discriminators" may be used in constructing queries).

246 NSA DCLPO REPORT, *supra*, at 7.

247 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6).

and PRISM data may be queried using U.S. person identifiers if those U.S. person identifiers have been approved pursuant to internal NSA procedures.[248]

The NSA's internal procedures treat queries of metadata and content using U.S. person identifiers differently.[249] The NSA's internal procedures require that queries of metadata using a U.S. person identifier be conducted only in a system or systems that require analysts to document the basis for their metadata query prior to conducting the query. Analysts are trained prior to using such systems. The NSA reported that it conducted approximately 9,500 metadata queries using U.S. person identifiers in 2013. In reviewing these queries, the NSD and ODNI have found that this number is likely substantially overinclusive of the actual number of U.S. person metadata queries conducted because many query terms that had been labeled as U.S. person identifiers proved on further analysis to not be identifiers of U.S. persons.

With respect to content queries using U.S. person identifiers, the NSA's internal procedures take a white-listing approach. Specifically, content queries using U.S. person identifiers are not permitted unless the U.S. person identifiers have been pre-approved (i.e., added to a white list) through one of several processes, several of which incorporate other FISA processes. For example, the NSA has approved the use of content queries using identifiers of U.S. persons currently subject to FISC-approved electronic surveillance under Section 105 or targeting under Section 704. U.S. person identifiers can also be approved by NSA's Office of General Counsel after a showing is made regarding why the proposed use of the U.S. person identifier would be "reasonably likely to return foreign intelligence information;" all approvals to use U.S. person identifiers to query content must be documented.[250] In 2013, the NSA approved 198 U.S. person identifiers to be used as content query terms. The NSA minimization procedures mandate that the DOJ's National Security Division and ODNI conduct oversight of the NSA's U.S. person queries. The NSD and ODNI's oversight of the NSA and other agencies queries is further detailed below.

The CIA's minimization procedures similarly permit the CIA to query unminimized Section 702–acquired data using U.S. person identifiers to discover foreign intelligence information.[251] The CIA's minimization procedures require that all queries of unminimized content, whether or not a U.S. person identifier is used in the query, must be "reasonably designed to find and extract foreign intelligence information." The CIA minimization procedures state that the CIA must keep records of all such content queries.

---

248 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6).

249 NSA DCLPO REPORT, *supra*, at 7.

250 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6); NSA DCLPO REPORT, *supra*, at 7.

251 Bates October 2011 Opinion, *supra*, at 25, 2011 WL 10945618, at *8; AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 13.

In implementing its query provision, the CIA has not required its personnel to seek pre-approval of U.S. person content queries, but it does record who conducts those queries and requires analysts to both identify any U.S. person identifiers used as query terms and to write a contemporaneous foreign intelligence justification for any query of unminimized Section 702–acquired content using a U.S. person identifier.[252] The CIA's content queries, for example, involve U.S. persons located overseas that intelligence indicates may be engaged in facilitating international terrorism.

In 2013, the CIA conducted approximately 1,900 content queries using U.S. person identifiers. Approximately forty percent of these content queries were at the request of other U.S. intelligence agencies. Some identifiers were queried more than once; the CIA has advised that approximately 1,400 unique identifiers were queried during this period. The NSD and ODNI are required under the CIA minimization procedures to review these records.

Metadata queries are treated differently under the CIA's minimization procedures. The CIA minimization procedures do not contain a standard for conducting metadata queries, although the statute and internal CIA procedures do require that queries may not be conducted for an unauthorized purpose (such as trying to find information about a love interest). If the CIA did identify any metadata associated with the individual, however, the CIA is permitted to conduct a further query into the underlying content only if the query is to identify foreign intelligence information, and the CIA may only disseminate the results of content or metadata queries to the requesting entity if the dissemination of information was otherwise permissible under the CIA's minimization procedures, as described below. The CIA does not track how many metadata-only queries using U.S. person identities have been conducted.

The FBI minimization procedures also permit the FBI to query unminimized Section 702–acquired data.[253] Stemming from its role as both a foreign intelligence and a law enforcement agency, the FBI's minimization procedures differ from the NSA and CIA's procedures insofar as they permit the FBI to conduct reasonably designed queries "to find and extract" both "foreign intelligence information" and "evidence of a crime." Although, consistent with 50 U.S.C. § 1806(a), any use of Section 702–acquired information regarding United States or non-U.S. persons may only be used for lawful purposes, the requirement that queries be reasonably designed to identify foreign intelligence information or evidence

---

252 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8 ("NSD and ODNI also review CIA's written justifications for all queries using United States person identifiers of the content of unminimized Section 702-acquired communications.").

253 PCLOB March 2014 Hearing Transcript, *supra*, at 86 (statement of James A. Baker, General Counsel, FBI) (noting that the FBI queries such data).

of a crime applies only to U.S. person information. The "reasonably designed" standard applies to both content and metadata queries.

The FBI is required under its minimization procedures to maintain records of all terms used to query content. These records identify the agent or analyst who conducted the query, but do not identify whether the query terms are U.S. person identifiers. Although the FBI's minimization procedures do not require the FBI to keep records of metadata-only queries, such queries are conducted in the same databases that contain the content collection; therefore, such metadata queries are also recorded. The NSD and ODNI conduct oversight reviews of both the content and metadata queries, as described below.

Because they are not identified as such in FBI systems, the FBI does not track the number of queries using U.S. person identifiers. The number of such queries, however, is substantial for two reasons.

First, the FBI stores electronic data obtained from traditional FISA electronic surveillance and physical searches, which often target U.S. persons, in the same repositories as the FBI stores Section 702–acquired data, which cannot be acquired through the intentional targeting of U.S. persons. As such, FBI agents and analysts who query data using the identifiers of their U.S. person traditional FISA targets will also simultaneously query Section 702–acquired data.

Second, whenever the FBI opens a new national security investigation or assessment, FBI personnel will query previously acquired information from a variety of sources, including Section 702, for information relevant to the investigation or assessment. With some frequency, FBI personnel will also query this data, including Section 702–acquired information, in the course of criminal investigations and assessments that are unrelated to national security efforts. In the case of an assessment, an assessment may be initiated "to detect, obtain information about, or prevent or protect against federal crimes or threats to the national security or to collect foreign intelligence information."[254] If the agent or analyst conducting these queries has had the training required for access to unminimized Section 702–acquired data, any results from the Section 702 data would be returned in these queries. If an agent or analyst does not have access to unminimized Section 702–acquired data — typically because this agent or analyst is assigned to non-national security criminal matters only — the agent or analyst would not be able to view the unminimized data, but would be notified that data responsive to the query exists and could request that an agent or analyst with the proper training and access to review the unminimized Section 702–acquired data. Anecdotally, the FBI has advised the Board that it

254 The Attorney General's Guidelines for Domestic FBI Operations § II.A, *available at* http://www.justice.gov/ag/readingroom/guidelines.pdf.

is extremely unlikely that an agent or analyst who is conducting an assessment of a non-national security crime would get a responsive result from the query against the Section 702–acquired data.

D. Retention and Purging

FISA also requires that the retention of nonpublicly available U.S. person information be minimized consistent with the need of the United States to obtain, produce, and disseminate information.[255] As such, the NSA, CIA, and FBI's minimization procedures contain provisions regarding when unminimized data must be aged off agency systems, what data must be purged upon recognition, and what types of evaluated information may be retained indefinitely.[256] Data that has been evaluated and determined to contain either no U.S. person information or only U.S. person information that meets the standard for permanent retention is referred to as "minimized information."

With a notable exception, unminimized Section 702–acquired data must be aged off of the NSA and CIA systems no later than five years after the expiration of the Section 702 certification under which that data was acquired.[257] Unminimized Internet transactions acquired through the NSA's upstream collection, however, must be aged off of the NSA systems no later than two years after the expiration of the Section 702 certification under which the data has been acquired.[258] The CIA and FBI do not receive, and therefore do not retain, such upstream collection. The FBI's minimization procedures alone distinguish between acquired data that have not been reviewed and those that have not been determined to meet the retention standard. As with the NSA and CIA, Section 702–acquired communications that have not been reviewed must be aged off FBI systems no later than five years after the expiration of the Section 702 certifications under which the data was acquired. Data that was reviewed but not yet determined to meet the retention standard in the FBI minimization procedures may be kept for a longer retention period subject to additional access controls.

With respect to all of the agencies, extensions from these age-off requirements may be sought from a high-level agency official. Other limited exceptions apply, such as to communications that are still being decrypted.[259]

---

255 50 U.S.C. § 1801(h)(1).

256 Although the minimization procedures themselves do not place an outer limit regarding how long such information may be retained, general rules regarding the retention of federal records apply to this data.

257 *See, e.g.*, NSA October 2011 Minimization Procedures, *supra*, § 3(c)(1); NSA DCLPO REPORT, *supra*, at 8.

258 NSA October 2011 Minimization Procedures, *supra*, § 3(c)(1); NSA DCLPO REPORT, *supra*, at 8.

259 *See, e.g.*, NSA October 2011 Minimization Procedures, *supra*, § 6(a)(1)(a).

As government personnel engage in the process of evaluating communications, the minimization procedures impose certain requirements requiring communications to be purged upon recognition. As described above, if data has been acquired as a result of a compliance incident, such as a typographical error in the tasking or a failure to detask a selector before a target's known travel to the United States, any identifiable data acquired as a result of the compliance incident is purged.[260] When a compliance incident is discovered, each agency has a process to discover and destroy data subject to purge.[261] The agencies also must coordinate such purges to ensure that all agencies are both aware of instances when a purge is required and use the same parameters to identify data subject to purge.[262]

Whether or not the communications were acquired as a result of a compliance incident, purges are required whenever a user of a tasked selector has been determined to be a U.S. person or located in the United States at any point during the acquisition.[263] These purge requirements, and the exceptions to these requirements, have been detailed above. In addition, the NSA's minimization procedures include additional purge-upon-recognition requirements due to the possibility that the NSA's upstream collection of Internet transactions could acquire domestic communications to which a user of a tasked selector is not a communicant. Such upstream-acquired Internet transactions must be destroyed upon recognition if it is determined that the transactions contain U.S. person information but do not contain any information that meets the NSA's long-term retention standards (discussed further below).[264] MCTs must also be destroyed upon recognition if it is determined that a single, discrete communication within the MCT is a wholly domestic communication.[265]

The NSA's minimization procedures also contain the following provision:

> Personnel will exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently

---

260 *See, e.g.,* PCLOB March 2014 Hearing Transcript, *supra*, at 72.

261 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-13.

262 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-13.

263 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-12 (noting that all of the agency minimization procedures require purges when a target is discovered to be a U.S. person or person located in the United States, with limited exceptions).

264 NSA October 2011 Minimization Procedures, *supra*, § 3(c)(2).

265 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(a)(1)(a) (requiring destruction of segregated MCTs determined to contain a wholly domestic communication) and § 3(b)(5)(b)(1) (requiring a determination regarding whether a single communication within an MCT is a wholly domestic communication before it is used); Bates November 2011 Opinion, *supra*, at 9, 2011 WL 10947772, at *4 (incorporating government's representation in a filing that if the discrete communication within an MCT is determined to be a wholly domestic communication, it must be destroyed).

> acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures.[266]

While it is not entirely clear what constitutes an "inadvertently acquired communication" here, the NSA's general counsel has stated that "[i]f information is determined to not have foreign intelligence value then it is required to be purged."[267] The NSA's general counsel, however, clarified that it is often "difficult to determine the foreign intelligence value of any particular piece of information."[268] An NSA analyst would need to determine not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need. Thus, in practice, this requirement rarely results in actual purging of data.

Neither the CIA nor FBI's minimization procedures have comparable requirements that a communication containing U.S. person information be purged upon recognition that the communication contains no foreign intelligence information; instead the CIA and FBI rely solely upon the overall age-off requirements found in their minimization procedures.

Section 702–acquired data that is not subject to purge upon recognition may be retained effectively indefinitely (i.e., need not be aged off of agency systems) if an agency determines that the data meets the retention standard in its minimization procedures. A communication is sometimes described as having been "minimized" or "retained" if the communication has been determined to meet this retention standard.

The NSA's minimization procedures permit the NSA to retain communications (other than wholly domestic communications) in generally the same situations where the NSA is permitted to disseminate (i.e., disclose) these communications to the consumers of the NSA's intelligence reports.[269] Specifically, the NSA may retain communications where the information identifiable to a U.S. person is, for example, "necessary to understand the foreign intelligence information or assess its importance," indicates that U.S. person "may be the target of intelligence activities" by a foreign government, or "the communication indicates that the United States person may be engaging international terrorist

---

266 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(1).

267 PCLOB March 2014 Hearing Transcript, *supra*, at 44; *see also id*. at 45-46 (referencing above quoted provision in the minimization procedures by stating that this determination must be made "as early as possible in . . . the processing cycle").

268 PCLOB March 2014 Hearing Transcript, *supra*, at 46.

269 NSA October 2011 Minimization Procedures, *supra*, § 6(a).

activities."[270] The NSA may also retain a communication containing U.S. person information if the communication is reasonably believed to contain evidence of a crime and the NSA has or will disseminate that evidence to a federal law enforcement entity.[271] The NSA may also retain communications beyond the normal age-off period if it is still decrypting the communication or using the communication to decrypt other communications.[272]

The NSA minimization procedures do not separately place any limitations on the retention of communications that contain no U.S. person information, but they do contain a reminder that any such communications may be retained only in accordance with other laws, regulations, and policy (for example, the general definitions and restrictions regarding the NSA's authorities provided in Executive Order 12333 and related documents).[273]

The retention standard in the CIA's Section 702 minimization procedures is comparable to the standard found in the NSA's minimization procedures. The CIA may indefinitely retain "minimized" communications. In order to "minimize" the communication, the CIA must remove any U.S. person information from the communication unless the information is publicly available, the U.S. person has consented to retention of the information, or the CIA must determine that the U.S. person information is necessary or may reasonably become necessary to understand foreign intelligence information. The CIA minimization procedures contain various categories of information considered to either be foreign intelligence information or information that is necessary to understand foreign intelligence information. Once "minimized," the communications may be retained in repositories that are still restricted to CIA personnel, but not necessarily CIA personnel who have been trained in the CIA minimization procedures. The CIA minimization procedures also permit the retention of data that is retained because it has been reported to a federal law enforcement agency as evidence of a crime.

The FBI Section 702 minimization procedures permit acquired communications to be retained indefinitely if the communications either contain no U.S. person information or if the communications contain information that "reasonably appears to be foreign intelligence information, [is] necessary to understand foreign intelligence information or assess its importance, or [is] evidence of a crime." Before further using this communication, the FBI is required to "mask" any U.S. person information within the communication that does not satisfy one of these three criteria. The FBI is also separately required to retain

---

270 NSA October 2011 Minimization Procedures, *supra*, § 6(a)(2), (b).

271 NSA October 2011 Minimization Procedures, *supra*, § 6(a)(3), (b)(8).

272 NSA October 2011 Minimization Procedures, *supra*, § 6(a)(1).

273 NSA October 2011 Minimization Procedures, *supra*, § 7.

reviewed information that reasonably appears to be exculpatory or that reasonably appears to be discoverable in a criminal proceeding.

E. Use and Dissemination

Restrictions in FISA and the minimization procedures contain limitations on the use and dissemination of Section 702–acquired information. "Dissemination" of FISA-acquired information generally refers to the reporting of acquired information outside of an intelligence agency, though broad accessibility of information within an agency can also constitute dissemination.[274]

Section 702 acquisition is governed by almost all of the same restrictions on use that apply to traditional FISA electronic surveillance.[275] These statutory restrictions apply to both U.S. person information and non-U.S. person information. Specifically, all Section 702 information may be used or disclosed only for lawful purposes.[276] Use of Section 702–acquired information in a criminal proceeding must be authorized by the Attorney General.[277] Any person whose communications have been acquired pursuant to Section 702, whether or not he or she was a target of the acquisition and whether or not he or she is a U.S. person, must be notified by the government before any information obtained from or derived from Section 702 acquisition is used against him or her in any legal proceeding in the United States.[278] Such an individual is referred to as an "aggrieved person." An aggrieved person may move to suppress the evidence that was obtained from or derived from Section 702 acquisition on the grounds that the information was unlawfully acquired or that the Section 702 acquisition otherwise did not conform with the Attorney General and Director of National Intelligence's authorization.[279]

The agencies' minimization procedures and practices impose additional restrictions on the use and dissemination of Section 702–acquired data. The NSA's minimization procedures permit the NSA to disseminate U.S. person information if the NSA deletes any information that could identify the U.S. person (a process referred to as "masking").[280] Alternatively, the NSA may disseminate the U.S. person's identity for one of a specific list of reasons, including that the U.S. person has consented to the dissemination, the specific

---

274 *See* H.R. Rep. No. 95-1283, at 59 (discussing minimization within agencies).

275 50 U.S.C. § 1881e(a) (stating that information acquired under Section 702 shall be governed under virtually all of the use restrictions found in 50 U.S.C. § 1806).

276 50 U.S.C. § 1806(a).

277 50 U.S.C. § 1806(b).

278 50 U.S.C. § 1806(c), (d).

279 50 U.S.C. § 1806(e).

280 NSA October 2011 Minimization Procedures, *supra*, § 6 (b).

information about the U.S. person is already publicly available, the U.S. person's identity is necessary to understand foreign intelligence information, or the communication contains evidence of a crime and is being disseminated to law enforcement authorities. As a matter of practice and policy, the NSA typically masks all information that could identify a U.S. person in its reports.[281] Consumers of NSA reports, such as other federal agencies, may then request that the U.S. person identity be "unmasked," a request that the NSA approves if the user has a "need to know" and disseminating the U.S. person identity would be consistent with the NSA's minimization procedures.[282]

Generally, dissemination of communications that contain no U.S. person information are governed by other laws, regulation, and policies (such as Executive Order 12333 and related implementing regulations), but not by the minimization procedures.[283] These further restrictions outside the minimization procedures, for example, require that the NSA generate intelligence reports only to meet specific intelligence requirements established by the government.[284] These regulations and policies also contain restrictions regarding what information (U.S. person information or otherwise) may be shared with foreign governments.[285]

In response to Judge Bates' opinion finding that a previous version of the NSA's minimization procedures did not meet Fourth Amendment or statutory requirements, the NSA's minimization procedures now also impose additional restrictions on the use of MCTs. Specifically, before a discrete communication contained within an MCT can be used in an intelligence report, FISA application, or to engage in further Section 702 targeting, the NSA analyst must determine if the discrete communication contains a tasked selector.[286] If not, and the communication is to or from an identifiable U.S. person or person located in the United States, that discrete communication may only be used to protect against an immediate threat to life, such as a hostage situation.[287]

The CIA's minimization procedures permit the CIA to disseminate U.S. person information if any information that identifies the U.S. person is masked in the dissemination. The CIA may also disseminate U.S. person information in a manner that identifies the U.S. person if that person's identity is necessary to understand foreign

---

281 NSA DCLPO REPORT, *supra*, at 7.

282 NSA DCLPO REPORT, *supra,* at 7-8; NSA October 2011 Minimization Procedures, *supra*, §§ 6(b) and 7.

283 NSA October 2011 Minimization Procedures, *supra*, § 7.

284 NSA DCLPO REPORT, *supra*, at 7.

285 *See generally* Exec. Order No. 12333 §§ 1.3(b)(4) and 1.6(f).

286 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(b)(2).

287 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(b)(2)(c).

intelligence information or (if concerning an attack by a foreign power, sabotage by a foreign power, international terrorism or the international proliferation of weapon of mass destruction by a foreign power, or clandestine intelligence activities by a foreign power) may become necessary to understand the foreign intelligence information. The CIA may further disseminate evidence of a crime to federal law enforcement authorities.

The FBI's minimization procedures permit the FBI to disseminate Section 702–acquired U.S. person information that reasonably appears to be foreign intelligence information or is necessary to understand foreign intelligence information. Disseminations concerning the national defense or security of the United States or the conduct of foreign affairs of the United States are permitted to identify U.S. persons only if necessary to understand the foreign intelligence information or to assess its importance. The FBI is also permitted to disseminate U.S. person information that reasonably appears to be evidence of a crime to law enforcement authorities. The FBI's minimization procedures incorporate certain guidelines, already otherwise applicable to the FBI, regarding the dissemination of information to foreign governments.[288]

VII. Internal Agency Oversight and Management of the Section 702 Program

In addition to the training programs previously described, each of the agencies subject to targeting or minimization procedures has developed a corresponding compliance program to evaluate and oversee compliance with these procedures, as well as facilitate the reviews by external overseers.[289] Any incidents of noncompliance that have been identified either by these compliance programs or that are otherwise discovered by the agencies must be reported to the DOJ and ODNI, who in turn must report these incidents to Congress and the FISC,[290] as discussed in the next section.

The NSA's use of the Section 702 authorities are internally overseen by various NSA entities, including the NSA's Office of the Director of Compliance ("ODOC"), NSA's Office of General Counsel ("OGC"), embedded compliance elements within NSA's directorates (in

---

288 NSA October 2011 Minimization Procedures, *supra*, § 3(b)(5)(b)(2)(c).

289 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-6 to A-8 (discussing NSA oversight program); *id*. at A-9 (discussing CIA oversight program); *id*. at A-11 to A-12 (discussing FBI oversight program). *See generally id.* at 4-5 n.2 (noting that no incidents of noncompliance have been reported by the NCTC and that the NSD and ODNI would be conducting a review of the NCTC's compliance in the following reporting period).

290 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 28 (noting that the semiannual report required by Section 707 is given to both Congress and the FISC and describes all incidents of noncompliance); 50 U.S.C. § 1881f(b)(1(G) (requiring all incidents of noncompliance with the targeting procedures, minimization procedures, and Attorney General Guidelines, as well as any incidents of noncompliance by a provider, to be reported in the Section 707 Report); FISC Rule of Procedure 13(b) (requiring incidents of noncompliance to be reported to the FISC).

particular, the Signals Intelligence Directorate's Oversight and Compliance ("O&C") section), and — as of early 2014 — the NSA's new Director of Civil Liberties and Privacy Office ("DCLPO").[291] Each of these organizations has different, but related, roles. The NSA's ODOC is responsible for NSA-wide compliance efforts and conducts periodic risk assessments to identify potential systemic incidents of noncompliance with the NSA targeting or minimization procedures.[292] For example, the ODOC conducted a risk assessment regarding how effective the NSA's purge practices had been in removing data required to be purged from the NSA's systems. Particularly important in light of errors and misunderstandings that have led to compliance issues in Section 702 and other programs, such as the MCT issue discussed above, ODOC also coordinates programs intended to ensure that factual representations made to the FISC are accurate and that interpretations of how the targeting and minimization procedures are to be applied in practice are consistent both within the NSA and between the NSA and its overseers.[293]

The NSA's O&C section and OGC conduct more granular oversight of the Section 702 program. The O&C section conducts spot checks of individual targeting decisions, queries of acquired data, and disseminations for compliance with the NSA's targeting and minimization procedures.[294] The O&C section and OGC also offer compliance-related guidance regarding targeting decisions, investigate and report potential incidents of noncompliance with the procedures and other legal requirements, and provide remedial training when an incident investigation reveals that the incident was caused by an avoidable error.[295] The O&C section and OGC also facilitate the reviews conducted by the DOJ and ODNI that are described below.[296]

The NSA appointed its first Director of Civil Liberties and Privacy while the Board was conducting its review of the Section 702 program. The Director's office is not, as of yet, involved in periodic Section 702 programmatic reviews. The Director's first public report, however, was issued in April 2014 and described in an unclassified manner aspects of the NSA's implementation of the Section 702 program.

The CIA's internal compliance program is managed by the CIA's FISA Program Office and the CIA's OGC.[297] These entities conduct oversight of the CIA's day-to-day use of the Section 702 authorities by, for example, conducting pre-tasking reviews of the CIA

---

291 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-6 to A-8; NSA DCLPO REPORT, *supra*, at 9.

292 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-7 to A-8.

293 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-7.

294 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-7; NSA DCLPO REPORT, *supra*, at 7.

295 *See generally* NSA DCLPO REPORT, *supra*, at 9.

296 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

297 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

nominations to the NSA regarding proposed new selectors to be tasked for Section 702 acquisition.[298] The FISA Program Office also oversees whether current and proposed systems handle Section 702–acquired data in compliance with the minimization procedures.[299] The FISA Program Office additionally conducts reviews regarding whether Section 702 selectors remain properly tasked.[300] The CIA's OGC has attorneys embedded with CIA personnel to answer specific targeting, querying, retention, and dissemination questions.[301] Finally, the CIA FISA program office and the CIA OGC facilitate the reviews conducted by the DOJ and ODNI that are described below.

Several sub-organizations within the FBI are responsible for conducting internal oversight over the Bureau's Section 702 activities. The FBI's OGC, in particular its National Security Law Branch, is responsible for providing legal advice regarding the application of the FBI targeting and minimization procedures. The FBI's Exploitation Threat Section ("XTS") takes the lead in reviewing the FBI's nominations to the NSA for proposed Section 702 tasking.[302] Various sub-organizations within the Bureau are responsible for reviewing and monitoring compliance with the FBI targeting and minimization procedures.

As described above, the NCTC's role in the Section 702 program is minimal. The NCTC has assigned legal and program personnel to oversee the implementation of its minimization procedures.

Incidents of noncompliance with the targeting or minimization procedures that are identified by any of these internal compliance efforts, or that are otherwise self-identified by the agencies, must be reported to the DOJ and ODNI.[303] Historically, most identified compliance incidents have been discovered as a result of self-reporting or via the internal compliance programs.[304] Once an incident has been identified and reported, the internal

---

298 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-8 to A-9.

299 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

300 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

301 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-9.

302 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-12.

303 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7 (regarding the NSA's reporting of incidents), 10 (regarding reporting of incidents by the FBI Office of General Counsel), A-7 (regarding the NSA's reporting via the NSA Office of General Counsel), and A-9 (regarding reporting of incidents by the CIA Office of General Counsel).

304 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7 (stating that most incidents "are identified by NSA analysts or by NSA's internal compliance program"); *id*. at 25 (noting that most compliance incidents involve the NSA targeting or minimization procedures); *id*. at 28 (advising that the "volume" of NSA incidents is robust enough such that pattern and trend analysis is more fruitful than is the case with other compliance matters).

compliance programs are also involved in implementing remedial actions, such as purging and retraining as required.[305]

In addition to reporting incidents of noncompliance, as an additional prophylactic measure the NSA is required under its targeting procedures to report any instance in which a user of a Section 702–tasked selector is determined to have been in the United States while the selector was tasked.[306] Should the CIA or FBI determine that a user of a Section 702 selector is a U.S. person or located in the United States, the CIA and FBI report this to the NSA, which in addition to promptly detasking the selector, sends a report to the DOJ and ODNI. This reporting requirement applies whether or not the NSA assesses that this acquisition occurred as the result of a compliance incident. For example, if the NSA correctly assessed that a target was a non-U.S. person located abroad, but unbeknownst to the NSA (and not reasonably predictable based on information available to the NSA), the target subsequently entered the United States, no compliance incident would have occurred. The NSA would be required to promptly detask the target's selectors from Section 702 acquisition upon recognition and purge data acquired while the user was in the United States, but no incident of noncompliance with the targeting or minimization procedures would have occurred. This is because the NSA assessed that the target was a non-U.S. person reasonably believed to be located outside the United States up until the time that the NSA detasked the selector from Section 702 acquisition. Nonetheless, the NSA would be required to report such an incident to the DOJ and ODNI. As described below, the DOJ and ODNI investigate such incidents and will request additional information in order to make their own determination regarding whether a compliance incident did or did not occur.[307]

Additionally, but separately, the statute also requires each agency that conducts Section 702 acquisition to conduct an annual review of the Section 702 program.[308] These annual reviews must be sent to the Senate Select Committee on Intelligence, Senate Committee on the Judiciary, House Permanent Select Committee on Intelligence, and House Judiciary Committee (hereinafter, "the Congressional Committees"), the FISC, Attorney General, and Director of National Intelligence.[309] The annual reviews must report the number of disseminations of U.S. person identities made, the number of U.S. person identities that were subsequently unmasked, and the number of Section 702 targets that

---

305 *See, e.g.*, NSA DCLPO REPORT, *supra*, at 9 (regarding various remedies implemented by NSA after an incident is discovered); AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-13 (describing elements of the purge process).

306 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

307 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

308 50 U.S.C. § 1881a(l)(3).

309 50 U.S.C. § 1881a(l)(3).

were subsequently determined to be located in the United States.[310] The agency reviews must also evaluate whether foreign intelligence information is being acquired under the Section 702 program and whether the minimization procedures adequately minimize the acquisition, retention, and dissemination of U.S. person information consistent with the United States' foreign intelligence needs.[311] The CIA receives Section 702 acquisition but does not actually conduct any acquisition. As such, the CIA does not conduct an annual review; some information regarding the CIA's use of the program, however, is included in the NSA's annual report.

VIII. External Oversight of the Section 702 Program

In enacting Section 702, Congress mandated additional external layers of oversight, each resulting in reports made to Congress and the FISC. This Section describes the targeting and minimization reviews conducted by the DOJ's National Security Division ("NSD") and the ODNI, the reports issued by the inspectors general, and additional oversight activities conducted by the FISC and the Congressional Committees.

A. NSD/ODNI Targeting Reviews

As is discussed above, the NSA is required under its targeting procedures to document every targeting decision made under its targeting procedures. The record of each targeting decision, known as a tasking sheet, includes (1) the specific selector to be tasked,[312] (2) citations to the specific documents and communications that led the NSA to determine that the target is reasonably believed to be located outside the United States,[313] (3) a narrative describing the contents of these specific documents and communications, (4) a statement regarding the assessed U.S. person status of the target, and (5) a statement identifying the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired.[314]

The NSD conducts a post-tasking review of every tasking sheet provided by the NSA;[315] the ODNI reviews a sample of these sheets. In addition to evaluating whether the tasking complied with the targeting procedures, the NSD and ODNI review the targeting for

---

310 50 U.S.C. § 1881a(l)(3)(A)(i)-(iii).

311 50 U.S.C. § 1881a(l)(3)(A), (B).

312 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

313 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-5; *see also* NSA DCLPO REPORT, *supra*, at 4-5.

314 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-5.

315 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 61 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) (stating that tasking sheets "are all reviewed . . . by the Department of Justice on a regular basis").

overall compliance with the statutory limitations, such as the prohibition against reverse targeting. If the NSD or ODNI is unable to determine whether the tasking sheet is sufficient, the NSD and ODNI will require the NSA to provide the cited documents and communications that underlie the NSA's foreignness determination at a bimonthly onsite review.[316] The NSD and ODNI also engage with the NSA compliance and legal personnel to ask follow-up questions regarding the foreignness and foreign intelligence purpose determinations.[317] As needed, the NSD and ODNI also seek additional information from the CIA and FBI regarding selectors that they have nominated.[318] The NSD and ODNI's review of foreign intelligence purpose determinations is more limited than its review of foreignness determinations insofar as the NSA analysts are required to document the basis for their foreignness determination (i.e., they must show their work), whereas the analyst need only identify a foreign intelligence purpose. The results of each NSD/ODNI bimonthly review are required by statute to be provided to the Congressional Committees.[319] Historically, the NSD and ODNI's bimonthly reviews have determined that approximately 0.1% of all the NSA taskings did not meet the requirements of the NSA targeting procedures.[320]

Additionally but separately, the NSD and ODNI also conduct approximately monthly reviews of the FBI's application of its own targeting procedures.[321] The NSD currently reviews every instance in which the FBI's evaluation of foreignness revealed any information regarding the target, regardless of whether the information confirms or rebuts the NSA's foreignness determination. Follow-up questions regarding the FBI's evaluation of this information are discussed with FBI analysts and supervisory personnel.[322] Like the NSA reviews, the results of the NSD/ODNI monthly reviews regarding FBI targeting are documented in a report that must be sent to the Congressional Committees.[323] The NSD and ODNI have not reported the historical percentage of tasking incidents that have been discovered as a result of these reviews. For the period of June through November 2012, the

316 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

317 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

318 *See, e.g.*, AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8 (noting that with respect to CIA nominations "the joint oversight review team conducts onsite visits at CIA" and "the results of these visits are included in the bimonthly NSA review reports discussed above")*; see also* AUGUST 2013 SEMIANNUAL ASSESSMENT, at 6-7 (describing these content of the bimonthly review reports, including the NSA tasking review).

319 50 U.S.C. § 1881f(b)(1)(F).

320 PCLOB March 2014 Hearing Transcript, *supra*, at 43 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

321 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 9-10.

322 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 10.

323 50 U.S.C. § 1881f(b)(1)(F).

overall FBI tasking incident error rate, which would include incidents discovered by the NSD/ODNI reviews, was 0.04%.

B. NSD/ODNI Minimization Reviews

The NSD and ODNI also conduct at least bimonthly reviews of the NSA, CIA, and FBI's application of their respective minimization procedures.[324] These reviews vary based on the differences in each agency's minimization procedures and the manner in which each agency uses the Section 702–acquired data.[325] In addition to reviewing agency activities for compliance with the minimization procedures, the NSD and ODNI also look for any other potential violations of statutory prohibitions, such as the prohibition against reverse targeting. For example, if a Section 702 tasking resulted in substantial reporting by the Intelligence Community regarding a U.S. person, but little about the Section 702 target, this would be a strong indication to the oversight team that reverse targeting may have occurred. The results of the NSD/ODNI reviews are documented in reports that are, as required by FISA, sent to the Congressional Committees.[326]

The NSD and ODNI bimonthly minimization reviews at the NSA focus on dissemination and queries using U.S. person identifiers.[327] With respect to dissemination, the NSA identifies to the NSD/ODNI review team all NSA-issued reports that contain U.S. person information derived from Section 702 acquisition.[328] The NSD/ODNI team has reviewed a substantial majority of these reports.[329] The NSD/ODNI team also reviews other disseminations of foreign intelligence information to foreign governments, which may or may not contain U.S. person information.[330] With respect to queries of Section 702–acquired metadata using U.S. person identifiers, the NSD/ODNI team reviews all such queries and analysts' justifications for the queries. With respect to Section 702–acquired content queries, the NSD/ODNI review team reviews the documentation for all U.S. person identifiers that are approved as query terms.[331]

---

324 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 5-10 (regarding frequency of reviews and fact that they include minimization reviews).

325 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 5-6.

326 50 U.S.C. § 1881f(b)(1)(F).

327 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7, 13.

328 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

329 The NSD/ODNI previously reviewed a substantial majority of these reports. *See* NSA DCLPO REPORT, *supra*, at 8. NSD has advised that it has recently revised its reviews and is now reviewing all reports provided by NSA that that contain U.S. person information.

330 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 7.

331 *See* NSA October 2011 Minimization Procedures, *supra*, § 3(b)(6) (regarding documentation requirements for such query terms); NSA DCLPO REPORT, *supra*, at 7 (regarding fact that this documentation is made available to NSD and ODNI for review).

At the CIA, the NSD/ODNI team reviews the CIA's querying, retention, and dissemination of Section 702–acquired data.[332] The NSD/ODNI team evaluates all of the required written justifications for use of a U.S. person identifier (or any other query term intended to return information about a particular U.S. person) to query Section 702–acquired content.[333] Metadata queries are not reviewed. The NSD/ODNI review team samples decisions made by CIA personnel to permanently retain data.[334] The CIA is required to provide, and the NSD/ODNI team reviews, all disseminations of Section 702–acquired U.S. person information.[335]

With respect to the FBI, the NSD/ODNI team also evaluates the FBI's querying, retention, and dissemination determinations.[336] The NSD and ODNI review a sample of communications that FBI assesses meets the retention standards, a sample of disseminations containing Section 702–derived U.S. person information, and a sample of queries conducted by FBI personnel.

The NSD and ODNI also conduct annual process reviews at the NCTC and FBI. The NCTC process review examines the processes that the NCTC has put in place to control access and train personnel with regard to its limited Section 702 minimization procedures. The FBI annual process review surveys the systems FBI uses to receive, verify, and route PRISM collection.

The NSD and ODNI also conduct ad hoc reviews related to newly developed or modified systems that the agencies plan to use to target non-U.S. persons under Section 702 or acquire, retain, or disseminate Section 702–acquired information.[337] These ad hoc system reviews are intended to identify existing compliance issues, prevent future compliance incidents from occurring, and ensure that systems are designed in a manner that facilitates subsequent oversight of their use.

C. NSD/ODNI Incident Investigation, Reporting, and Related Activities

Whether initially discovered via an NSD/ODNI review, an internal agency compliance review, or by self-reporting, Section 702 and the FISC's own rules of procedure require the NSD to report compliance incidents by the Intelligence Community or electronic communication service providers to the Congressional Committees and to the

---

332 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8.

333 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8.

334 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8.

335 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 8.

336 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 10 & n.6.

337 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 11.

FISC.[338] Specifically, the FISA Amendments Act requires the Attorney General to report every incident of noncompliance to the Congressional Committees in a semiannual report.[339] Pursuant to FISC Rule of Procedure 13(b), all compliance incidents must be reported to the FISC in either an immediate notice or (for less significant incidents) in a quarterly report.[340] Rule 13(b) states that such reports must include a description of the incident of noncompliance, the facts and circumstances related to the incident, any modifications that will be made in how the government is using the authority in light of the incident, and a description of how the government will handle any information obtained as a result of the incident.[341] In addition, but separately, the Attorney General and Director of National Intelligence must semiannually jointly conduct an assessment regarding the agencies' compliance with their targeting procedures, minimization procedures, and the Attorney General Guidelines.[342] This semiannual assessment must be provided to the Congressional Committees and to the FISC.[343] To date, four of the semiannual assessments have been partially declassified and are publicly available.[344]

To meet these various reporting obligations, a team of NSD and ODNI personnel review incident reports, request additional information, and (when necessary) further investigate potential incidents of noncompliance.[345] These inquiries and investigations entail frequent interaction with counterparts in the internal agency compliance programs discussed above. In addition to resolving individual compliance matters, the NSD and ODNI team lead weekly calls and bimonthly meetings with representatives from the NSA, CIA, and FBI to discuss, among other things, compliance trends and incidents that affect multiple agencies.[346]

---

338 *See* 50 U.S.C. § 1881f(b)(1)(G); FISC Rule of Procedure 13(b).

339 50 U.S.C. § 1881f(b)(1)(G).

340 *See* MAY 2010 SEMIANNUAL ASSESSMENT, *supra* at 22 (discussing requirements under Rule 10(c), the predecessor to Rule 13(b) in the prior set of FISC Rules of Procedure); NSA DCLPO REPORT, *supra*, at 3 (discussing individual notices and quarterly reports).

341 FISC Rule of Procedure 13(b).

342 50 U.S.C. § 1881a(l)(1).

343 50 U.S.C. § 1881a(l)(1).

344 *See* SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, MARCH 2009, *available at* http://www.dni.gov/files/documents/FAA/SAR%20March%202009%20Final%20Release%20with%20Exemptions.pdf; SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, DECEMBER 2009, *available at* http://www.dni.gov/files/documents/FAA/SAR%20December%202009%20Final%20Release%20with%20Exemptions.pdf; May 2010 Semiannual Assessment, *supra*; August 2013 Semiannual Assessment, *supra*.

345 MAY 2010 SEMIANNUAL ASSESSMENT, *supra*, at 22.

346 *See generally* AUGUST 2013 SEMIANNUAL REPORT, *supra*, at 11 (discussing bimonthly meetings).

Some of the results of the NSD and ODNI's compliance investigations and reports are discussed below.

D. Inspector General Reports

Section 702 also authorizes inspectors general of agencies that acquire data pursuant to Section 702 to conduct reviews of the Section 702 program.[347] The inspectors general are authorized to evaluate the agencies compliance with the targeting procedures, minimization procedures, and Attorney General Guidelines.[348] Any such reviews are required to contain an accounting of the number of disseminated reports containing U.S. person identities, the number of instances those identities were unmasked, and the number of targets that were subsequently determined to be located in the United States.[349] The results of these reviews must be provided to the Attorney General, Director of National Intelligence, FISC, and the Congressional Committees.[350] The NSA and DOJ[351] Inspectors General have conducted reviews under this provision. The reports of these reviews have not been declassified.

E. FISC Oversight

The FISC's primary role in Section 702 is to review the Section 702 certifications and corresponding targeting and minimization procedures for compliance with the statute and the Fourth Amendment. As is described in detail above, the FISC has held that this review of the Section 702 certifications and related documents cannot be made in a vacuum, but instead must be made in light of the actual manner in which the government has implemented (or plans to implement) the Section 702 authorities. In addition to filings made by the government to the FISC in support of the certifications, the FISC's determinations are informed by the information provided in the NSD's reports of all incidents of noncompliance with the procedures,[352] the Attorney General and Director of National Intelligence's semiannual assessment regarding compliance with the procedures,[353] the annual reports of agency heads that conduct Section 702 acquisition,[354]

---

347 50 U.S.C. § 1881a(l)(2).

348 50 U.S.C. § 1881a(l)(2)(A).

349 50 U.S.C. § 1881a(l)(2)(B), (C).

350 50 U.S.C. § 1881a(l)(2)(D).

351 *See* Press Release, Dept. of Justice, Office of the Inspector General, DOJ OIG Issues Report on Activities Under Section 702 of the FISA Amendments Act (Sept. 25, 2012), *available at* http://www.justice.gov/oig/press/2012/2012_09_25.pdf.

352 FISC Rule of Procedure 13(b).

353 50 U.S.C. § 1881a(l)(1).

354 50 U.S.C. § 1881a(l)(3).

and any reports by the inspectors general.[355] In reviewing the certifications, the FISC also will order the government to respond in writing to questions regarding the conduct of the Section 702 collection program and holds hearings in order to take sworn testimony from government witnesses.[356]

The FISC's oversight role is not limited to the renewal of Section 702 certifications. The government's obligation to report incidents of noncompliance under the FISC's rules is independent of whether any Section 702 certification is currently pending before the court.[357] In a letter to Senate Judiciary Committee Chairman Patrick Leahy, former FISC Presiding Judge Reggie Walton stated that with respect to all FISA compliance matters, to include incidents of noncompliance with the Section 702 program, the court may seek additional information, issue orders to the government to take specific action to address an incident of noncompliance, or (if deemed necessary) issues orders to the government to cease an action that the court assesses to be non-compliant.[358]

F. Congressional Oversight

The Senate Select Committee on Intelligence, Senate Committee on the Judiciary, House Permanent Select Committee on Intelligence, and House Judiciary Committee are the committees that oversee the government's use of FISA information, including Section 702 information. In passing the FISA Amendments Act, Congress mandated that the Attorney General provide these four committees with a semiannual report describing several aspects of the Section 702 program and further provide the committees with the underlying documents that govern the program.[359] Among other things, this semiannual report must include copies of the reports from any compliance reviews conducted by the DOJ or ODNI, a description of any and all incidents of noncompliance by the Intelligence Community or an electronic communications service provider, any certifications (including targeting and minimization procedures), and the directives sent to the electronic communication service providers.[360] The semiannual report must also include a description of the FISC's review of the certifications and copies of any order by the FISC or

---

355 50 U.S.C. § 1881a(l)(2).

356 FISC Rules of Procedure 5(c) and 17; Bates October 2011 Opinion, *supra*, at 7-10, 2011 WL 10945618 at *2-4 (examples of filings and hearing described); Letter from Presiding Judge Reggie B. Walton, Foreign Intelligence Surveillance Court to Senator Patrick Leahy, Chairman, Senate Comm. on the Judiciary, at 4-6 (July 29, 2013) ("Judge Walton Letter") (describing government submissions related to Section 702 certifications and the types of additional information sought from the government by the FISA court), *available at* http://www.fisc.uscourts.gov/sites/default/files/Correspondence%20Leahy-1.pdf.

357 FISC Rule of Procedure 13(b).

358 Judge Walton Letter, *supra*, at 10-11.

359 50 U.S.C. § 1881f.

360 50 U.S.C. § 1881f(b)(1).

pleading by the government that contains a significant legal interpretation of Section 702.[361]

In practice, the government provides the four committees all government filings, hearing transcripts, and FISC orders and opinions related to the court's consideration of the Section 702 certifications. In addition, the Congressional Committees receive the classified Attorney General and Director of National Intelligence's semiannual assessment regarding compliance with the procedures,[362] the annual reports of agency heads that conduct Section 702 acquisition,[363] and any reports by the inspectors general.[364]

In addition to these statutory requirements, the agencies may separately (and more promptly) inform the Congressional Committees of substantial compliance incidents.[365] The committees also hold hearings, and committee members and staff receive briefings, regarding the implementation of the Section 702 program.[366]

IX. Compliance Issues

The Section 702 program is a technically complex collection program with detailed rules embodied in the targeting procedures, minimization procedures, and Attorney General Guidelines regarding targeting, acquisition, querying, retention, and dissemination. Incidents of noncompliance with these rules have been identified in the course of the oversight conducted by the agencies themselves, by the NSD, and by the ODNI. These internal and external compliance programs have not to date identified any intentional attempts to circumvent or violate the procedures or the statutory requirements,[367] but both unintentional incidents of noncompliance and instances where Intelligence Community personnel did not fully understand the requirements of the statute and the procedures have been identified.

The government calculates a compliance incident rate for the Section 702 program by dividing the number of identified compliance incidents by the average number of selectors on task. This incident rate has been substantially below one percent since the

361 50 U.S.C. § 1881f(b)(1)(D). Copies of documents related to significant legal interpretations are also produced to Congress pursuant to 50 U.S.C. § 1871.

362 50 U.S.C. § 1881a(l)(1).

363 50 U.S.C. § 1881a(l)(3).

364 50 U.S.C. § 1881a(l)(2).

365 *See, e.g.,* NSA DCLPO REPORT, *supra*, at 3.

366 *See, e.g.,* S. Rep. No. 112-174, at 2 (2012).

367 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 23.

Section 702 program was initiated. The most common type of compliance incident that has occurred has involved instances in which the NSA otherwise complied with the targeting and minimization procedures in tasking and detasking a selector, but failed to make a report to the NSD and ODNI in the time frame required by the NSA targeting procedures.[368] Such notification delays made up over half of the reported incidents in the most recently declassified Attorney General/Director of National Intelligence semiannual assessment.[369] Two other common reasons compliance incidents occurred have been that (1) the wrong selector was tasked due to a typographical error,[370] or (2) a delay in detasking resulted when an analyst detasked some, but not all, of the Section 702–tasked selectors used by a non-U.S. person target known to be traveling to the United States.[371] Taken together, these three errors accounted for almost 75% of the compliance incidents that occurred during the reporting period of the most recently declassified Attorney General/Director of National Intelligence semiannual assessment.

Less common incidents, however, can have greater privacy implications. For example, the NSA has reported instances in which the NSA analysts conducted queries of Section 702–acquired data using U.S. person identifiers without receiving the proper approvals because the analyst either did not realize that the NSA knew the identifier to be used by a U.S. person or the analyst mistakenly queried Section 702–acquired data after receiving approvals to use a U.S. person identifier to query other non-Section 702–acquired data.[372]

In addition to such human errors, technical issues can lead to overcollection incidents. For example, the government has disclosed that technical errors have resulted in delays in detasking selectors found to be used by persons located in the United States.[373] The government has also disclosed that both changes in how communications transit the telecommunications system and design flaws in the systems the government uses to acquire such communications can, and have, resulted in the acquisition of data beyond what was authorized by Section 702 program.[374] Such unauthorized collection is required to be purged upon recognition.

---

368 *See, e.g.,* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 23-24.

369 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 26.

370 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 33 n.21.

371 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 33.

372 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 30.

373 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 32.

374 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 31-32 (stating that an undisclosed number of "incidents" involving overcollection as a result of changes in the global telecommunications environment, unforeseen consequences of software modifications, or system design issues occurred during the reporting period).

Several systemic incidents have also occurred in the government's operation of the Section 702 program. As is described above, the government's upstream acquisition of multi-communication transactions led to substantial modifications of the NSA minimization procedures and the purging of several years of prior collection. In an earlier incident, the NSA discovered that its practices for executing purges were substantially incomplete. Modifications to better tag, track, and purge data from the NSA's systems when required were implemented.

More recently, questions raised by the NSD/ODNI oversight team led to the discovery that post-tasking checks used to identify indications that a target is located in the United States were incomplete or, for some selectors, non-existent for over a year. After this issue was discovered, the relevant systems were modified to correct several errors, efforts were made to identify travel to the United States that had been previously missed (and corresponding purges were conducted), and additional modifications to the agencies' minimization procedures were made to ensure that data acquired while a Section 702 target had traveled to the United States will not be used.

Since the Section 702 program's inception, the compliance programs have also identified two instances of reverse targeting. The first instance, which was discovered by the NSD/ODNI targeting review, involved the reverse targeting of a non-U.S. person located inside the United States in order to acquire foreign intelligence information. The second, which involved reverse targeting to acquire information about a U.S. person located outside the United States, was identified by NSA oversight personnel. The targeting in the first incident resulted in the acquisition of communications that were subsequently purged; the targeting in the second incident did not result in any communications being acquired. In both incidents, the analysts who engaged in the reverse targeting substantially misunderstood the prohibition against reverse targeting. Given the centrality of this prohibition to Section 702 targeting, these analysts were retrained not only on the reverse targeting prohibition, but on other fundamental targeting requirements.

Part 4:

LEGAL ANALYSIS

I. Overview

Part Four is divided into three sections: Statutory Analysis, Constitutional Analysis, and Analysis of Treatment of Non-U.S. Persons. The Statutory Analysis section explains the statutory framework for collection under Section 702 of the Foreign Intelligence Surveillance Act ("FISA") and provides the Board's evaluation of whether PRISM and upstream collection comply with the statute. The Constitutional Analysis section details the Board's evaluation of the constitutionality of the program — examining the warrant requirement and its exceptions, and assessing the program's reasonableness under the Fourth Amendment. Part Four concludes with a discussion of the treatment of non-U.S. persons under the program.

II. Statutory Analysis

A. Establishment of Section 702

As noted in the Board's Report on the Section 215 program, FISA was enacted in 1978 to establish a procedure under which the Attorney General could obtain a judicial order authorizing the use of electronic surveillance in the United States for foreign intelligence purposes. Its original provisions — now referred to as "traditional FISA" — authorized, among other things, individualized FISA orders for electronic surveillance relating to a specific person, place, or communications account or device.

Over time, Congress has enacted legislation bringing additional categories of foreign intelligence gathering within FISA's ambit. One of the latest examples of this is the enactment of the FISA Amendments Act of 2008.[375] As outlined in Part 3 of this Report, the FISA Amendments Act, which includes the new Section 702 of FISA, replaced the temporary authority of the Protect America Act, which in turn, was designed to codify part of the President's Surveillance Program. The statute was enacted in response to Congress' conclusion that FISA should be amended to provide a separate procedure to facilitate the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information.[376] This statute was developed during a time of public debate and

375 Pub. L. No. 110-261, 122 Stat. 2436 (2008).

376 S. Rep. No. 110-209, at 2 (2007).

concern regarding the intelligence activities undertaken by the government, and it was an attempt to put a statutory framework around activities that were currently ongoing.[377]

As discussed below, the government utilizes two collection methods under Section 702 — PRISM collection and upstream collection (which includes acquiring "about" communications). The manner in which collection is effectuated via PRISM and upstream varies; therefore, the Board has analyzed the statutory compliance of each collection method separately. After reviewing the operation of the Section 702 program as a whole, and each collection method implemented under Section 702 individually, the Board has concluded that PRISM collection is expressly authorized by the statute and that the statute, while silent on "about" upstream collection, can permissibly be interpreted as allowing such collection as currently implemented.

B. Collection Under Section 702

1. Statutory Framework for Collection

Congress created Section 702 to authorize Foreign Intelligence Surveillance Court ("FISC" or "FISA court") approval of certifications which authorize the acquisition of broad *categories* of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States.[378] A non-U.S. person is an individual who is neither a citizen nor a lawful permanent resident of the United States. As described in detail in Part 3 of this Report, the Attorney General and the Director of National Intelligence must submit a certification to and receive an order from the FISA court that permits them to authorize the targeting.[379]

Under Section 702, the FISC has the authority to review the government's certifications, targeting procedures, and minimization procedures, and the court must approve these certifications and procedures under criteria set forth in the statute. The FISC does not review specific selectors[380] tasked for collection nor does it review the *individual* factual basis for expecting that the tasking of a particular selector will result in the acquisition of foreign intelligence information. In its review and approval process, however, the FISC has the authority to do more than a rote check to ensure that the government meets its statutory requirements. The FISC's mandate to ensure compliance with the Fourth Amendment is expressly enumerated in the statute, and the court has required the government to make changes to its collection under Section 702 in the past on

---

377 *See* S. Rep. No. 110-209, at 5 (2007).

378 *See* 50 U.S.C. § 1881a(a), (g).

379 50 U.S.C. § 1881a(a), (g), (i).

380 A selector is a unique identifier associated with a *particular* individual or entity. See pages 32-33 of this Report.

this basis.[381] Additionally, the FISA court has an oversight role: the FISC Rules of Procedure impose an ongoing duty on the government to immediately correct any misstatement or omission of material facts that it has provided to the court, as well as to disclose any instance in which the government's conduct did not comply with the FISC's authorization or with applicable law.[382]

On the whole, Section 702 provides the public with transparency into the legal framework for collection and publicly outlines the basic structure of the program. Use of the words "target" and "targeting" allowed Congress to signal the type of collection activity undertaken by the government without detailing operational methods and tactics. In addition, it is clear from the face of the statute that the government must submit certifications to the FISC as well as implement targeting and minimization procedures that have been approved by the court.

2. PRISM Collection

The Board concludes that as currently implemented, the operation of PRISM collection falls within the framework of the statute. Section 702 expressly authorizes the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." As described in Part 3 above, under PRISM collection the government acquires communications to and from approved targets using communications "selectors" that are associated with particular persons. Examples of communications selectors include email addresses, but not key words.[383] The collection of communications to and from a target inevitably returns communications in which non-targets are on the other end, some of whom will be U.S. persons.[384] Such "incidental" collection of communications is not accidental, nor is it inadvertent.[385]

The incidental collection of communications between a U.S. person and a non-U.S. person located outside the United States, as well as communications of non-U.S. persons outside the United States that may contain information about U.S. persons, was clearly

---

381 *See* Memorandum Opinion, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618 (FISA Ct. Oct. 3, 2011) ("Bates October 2011 Opinion"), *available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

382 United States Foreign Intelligence Surveillance Court Rules of Procedure, Rule 13, *available at* http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.

383 Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 26 (Mar. 19, 2014) ("PCLOB March 2014 Hearing Transcript") (statement of Rajesh De, General Counsel, NSA), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

384 PCLOB March 2014 Hearing Transcript, *supra*, at 96-97 (statement of Robert Litt, General Counsel, ODNI).

385 PCLOB March 2014 Hearing Transcript, *supra*, at 96-97.

contemplated by Congress at the time of drafting. The statute prohibits the targeting of U.S. persons, but not the incidental acquisition of communications involving U.S. persons. Further, the statute requires the government to adopt procedures that, among other things, are reasonably designed to minimize (not eliminate) the acquisition and retention of private information about U.S. persons, consistent with the government's foreign intelligence needs.[386] The statute also calls for the Department of Justice and the Intelligence Community to review and report on disseminations of U.S. person information, including cases in which the U.S. person is not referred to by name.[387] The Senate Select Committee on Intelligence has explained the inevitability of such incidental collection and how Congress responded to that inevitability:

> Congress recognized at the time the FISA Amendments Act was enacted that it is simply not possible to collect intelligence on the communications of a party of interest without also collecting information about the people with whom, and about whom, that party communicates, including in some cases non-targeted U.S. persons . . .
>
> Specifically, in order to protect the privacy and civil liberties of U.S. persons, Congress mandated that, for collection conducted under Section 702, the Attorney General adopt, and the FISA Court review and approve, procedures that minimize the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting U.S. persons.[388]

Based on the information that the Board has reviewed, the government's PRISM collection complies with the structural requirements of the statute. As outlined above, the government has filed certifications authorizing the acquisition of certain categories of targets with the FISA court and has developed and submitted for FISA court approval targeting and minimization procedures as required by the statute. Incidentally collected U.S. person information is subject to these minimization procedures that set standards for acquisition and retention of information and permit disseminations of U.S. person information only for a foreign intelligence purpose or when the information is evidence of a crime.[389] After a thorough review, the Board has concluded that the government generally is complying with the targeting limitations set forth in subsections (b)(1) through (b)(4) and has adopted Attorney General guidelines that, among other things, prohibit reverse

386 *See* 50 U.S.C. §§ 1801(h), 1881a(e).

387 *See* 50 U.S.C. § 1881a(l)(2), (3).

388 S. Rep. No. 112-174, at 8 (2012).

389 *See* 50 U.S.C. §§ 1801(h), 1881a(e).

targeting. Although there have been documented compliance incidents,[390] we conclude that overall PRISM collection falls within the framework of the statute.

3. Upstream Collection

As described above, upstream collection constitutes a small percentage of collection under Section 702. To the extent that upstream collection involves acquiring communications to and from targeted persons, it fits within the statutory framework in the same way that PRISM collection does. Targeting under PRISM and upstream collection work in the same way; the mode of collection is different.

Upstream collection under Section 702 poses an additional question for statutory analysis because, as described above in Part 3, the upstream process captures not only communications to and from targeted persons, but also other communications that contain reference to the selector of a targeted person — which are referred to as "about" communications.[391]

The statutory language of Section 702 does not expressly permit or prohibit collection of communications "about" a target. The fact that the government engages in such collection is not readily apparent from the face of the statute, nor was collection of information "about" a target addressed in the public debate preceding the enactment of FISA or the subsequent enactment of the FISA Amendments Act. Indeed, the words "target" and "targeting" are not defined in either the original version of FISA or the FISA Amendments Act despite being used throughout the statute. Some commenters have questioned whether the collection of such "about" communications complies with the statute. We conclude that Section 702 may permissibly be interpreted to allow "about" collection as it is currently conducted.

Collection of "about" communications occurs only in upstream collection, not in PRISM.[392] Unlike PRISM collection, upstream collection acquires "Internet transactions," meaning packets of data that traverse the Internet, directly from the Internet "backbone."[393] Utilizing this method, the government is able to capture communications that contain an approved selector, no matter where it appears in the communication — whether in the "to" or "from" lines of an email, for instance, or in the body of the email.

As discussed in Part 3 above, there are technical reasons why "about" collection is needed to acquire even some communications that are "to" and "from" a target. Some other

---

390 See pages 77-79 of this Report.

391 PCLOB March 2014 Hearing Transcript, *supra*, at 26.

392 PCLOB March 2014 Hearing Transcript, *supra*, at 63.

393 PCLOB March 2014 Hearing Transcript, *supra*, at 26; Bates October 2011 Opinion, *supra*, at 27-28 & n.23, 2011 WL 10945618, at *9 & n.23.

types of "about" communications also involve Internet activity of the actual target. For some communications, the NSA's collection devices are not able to distinguish between communications that are actually "to" or "from" a target and those in which the selector is found in the body or a communication, nor can they distinguish among the different types of "about" communications. Thus, under current technology and program design, in order to avoid significant gaps in upstream collection coverage, "about" collection is largely a technical inevitability.[394]

As a result, if the selector is contained within the body of a communication, "about" collection may result in the acquisition of communications between two non-targets. In some such instances, both of the individuals who are parties to the communication could be U.S. persons or persons located within the United States. This occurs because the current state of technology renders the government unable to determine with certainty the location of all communicants at the time of acquisition.

In addition, upstream collection leads to the acquisition of multi-communication transactions ("MCTs").[395] As explained in Part 3 above, MCTs that contain a communication to, from, or about a target may be embedded within communications that are between U.S. persons or persons located within the United States, and the government has not been able to design a filter that would acquire only the single discrete communications within transactions that contain a selector.

Thus, due to the inclusion of "about" collection and the collection of MCTs, there is a greater risk that the NSA will acquire purely domestic communications through upstream collection than through PRISM. This risk is mitigated to some extent by the fact that through the upstream process, Internet transactions are first filtered to help eliminate potential domestic transactions before they are screened to determine whether a transaction contains a tasked selector. Further, NSA's minimization procedures include more stringent safeguards for upstream data than they do for PRISM data. In particular, the NSA, the only agency that conducts upstream collection and the only agency that has access to unminimized results of upstream collection, is not permitted to use U.S. person identifiers in conducting queries of the upstream data. In addition, the retention period for

394 As a general rule, in conducting traditional wiretaps, the government has been permitted to access a trunk line if it has no reasonable physical access to a particular line or device, subject to strict limits on retention and use of non-targeted communications.

395 The acquisition of MCTs through the upstream collection process, and the minimization procedures adopted to address the specific challenges posed by acquisition of MCTs, are described in detail in Part 3 of this Report. The constitutional and policy questions raised by the collection of MCTs are addressed in those respective sections of this Report.

Internet communications collected through upstream is two years, as opposed to the NSA's five-year retention period for data collected in PRISM.[396]

Given the lack of any textual prohibition, as well as the present technical necessity of capturing "about" communications in certain circumstances as part of the upstream collection process, we conclude that the inclusion of "about" collection under the current operation of the program is a permissible reading of the statute.

III. Constitutional Analysis

Evaluating the constitutionality of the Section 702 program poses unique challenges. Unlike the typical Fourth Amendment inquiry, where the legitimacy of "a particular search or seizure" is judged "in light of the particular circumstances" of that case,[397] evaluating the government's implementation of Section 702 requires assessing a complex surveillance *program* — one that entails many separate decisions to monitor large numbers of individuals, resulting in the annual collection of hundreds of millions of communications of different types, obtained through a variety of methods, pursuant to multiple foreign intelligence imperatives, and involving four intelligence agencies that each have their own rules governing how they may handle and use the communications that are acquired.[398]

Further complicating the analysis, the constitutional interests at stake are not those of the persons targeted for surveillance under Section 702, all of whom lack Fourth Amendment rights because they are foreigners located outside of the United States.[399]

---

396 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, § 3(c) (Oct. 31, 2011) ("NSA 2011 Minimization Procedures").

397 *Scott v. United States*, 436 U.S. 128, 137 (1978).

398 Most *programs* of searches or seizures that have been evaluated under the Fourth Amendment have involved uniform practices that advanced a single government interest through standardized means that intruded upon the privacy interests of each person affected in the same manner. *See, e.g.*, *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995) (drug testing of student athletes); *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990) (highway sobriety checkpoints). Courts also sometimes undertake programmatic assessments in response to statutory facial challenges, where they evaluate "the constitutionality of a statute without factual development centered around a particular application." *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1009 (FISA Ct. Rev. 2008) (citing *Wash. State Grange v. Wash. State Repub. Party*, 128 S. Ct. 1184, 1190 (2008)). Here, however, the Board has not asked whether Section 702 "is valid on its face — a question that would be answered by deciding whether *any* application of the statute passed constitutional muster." *Id.* at 1009-10. Instead, it has asked whether "this specific application" of the statute — the program as it is conducted today — is consistent with the Constitution. *Id*. at 1010.

399 *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990) (holding that the Fourth Amendment has no application to a physical search in a foreign country of the residence of a citizen of that country who has no voluntary attachment to the United States).

Instead, the relevant Fourth Amendment interests are those of the U.S. persons whose communications may be acquired despite not themselves having been targeted for surveillance.[400]

Although U.S. persons and other persons in the United States may not be targeted under Section 702, operation of the program nevertheless results in the government acquiring some telephone and Internet communications involving U.S. persons, potentially in large numbers. As explained above, this acquisition can occur in four main situations:

(1) A U.S. person communicates by telephone or Internet with a foreigner located abroad who has been targeted. The government refers to this as "incidental" collection.

(2) A U.S. person sends or receives an Internet communication that is routed internationally and that includes a reference to a selector such as an email address used by a foreigner who has been targeted. The government refers to this as "about" collection.[401]

(3) A U.S. person sends or receives an Internet communication that is embedded within the same "transaction" as a different communication that meets the requirements for acquisition (because it is to or from a targeted foreigner or includes a reference to the communications identifier of a targeted foreigner). The government refers to these transactions containing more than one separate communication as "multiple-communication transactions" or "MCTs."[402]

(4) A U.S. person's communications are acquired by mistake due to a targeting error, an implementation error, or a technological malfunction. The government refers to this as "inadvertent" collection.

Any Fourth Amendment assessment of the Section 702 program must take into account the cumulative privacy intrusions and risks of all four categories above, together with the limits and protections built into the program that mitigate them.[403]

---

400 In addition to U.S. persons, foreign citizens temporarily and voluntarily present within the United States likely possess Fourth Amendment rights. *See Verdugo-Urquidez*, 494 U.S. at 278 (Kennedy, J., concurring).

401 See pages 37-39 of this Report for an explanation of "about" collection.

402 See pages 39-41 of this Report for a discussion of "MCTs."

403 Apart from these four categories, there is of course a risk that government personnel could deliberately misuse the Section 702 program to target a U.S. person for surveillance. Doing so would be grounds for professional sanction and possibly criminal prosecution, however, and auditing procedures are in place to deter such wrongdoing. Every targeting decision made by an analyst is recorded and reviewed both by supervisors within the NSA and also by a joint oversight team from the Department of Justice and Office of

After analyzing these factors, the Board finds that the core of this program — acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court–approved targeting rules that have proven to be accurate in targeting persons outside the United States, and subject to multiple layers of rigorous oversight — fits within the totality of the circumstances test for reasonableness as it has been defined by the courts to date. Outside of this fundamental core, certain aspects of the Section 702 program push the entire program close to the line of constitutional reasonableness. Such aspects include the scope of the incidental collection of U.S. persons' communications, the use of "about" collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search the information collected under the program for the communications of specific U.S. persons. With these concerns in mind, this Report offers a set of policy proposals designed to push the program more comfortably into the sphere of reasonableness, ensuring that the program remains tied to its constitutionally legitimate core.

A. Privacy in Telephone and Internet Communications

The Fourth Amendment protects the right of the people "to be secure in their persons, houses, papers, and effects." It thus prohibits "unreasonable searches and seizures" by the government, and it specifies that a warrant authorizing a search or seizure may issue only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[404] A search occurs not only where the government intrudes on a person's tangible private property to obtain information, but also where "the government violates a subjective expectation of privacy that society recognizes as reasonable."[405]

Because individuals who are protected by the Constitution have a reasonable expectation of privacy in their telephone conversations, it has long been the rule that wiretapping conducted within the United States for criminal or other domestic purposes is presumptively unreasonable under the Fourth Amendment unless the government has obtained a warrant based on probable cause.[406] While the Supreme Court has not expressly

---

the Director of National Intelligence. To date, there are no known instances in which government personnel deliberately violated the statute, targeting procedures, or minimization procedures. There have, however, been instances in which analysts have made mistakes of law, including two instances of reverse targeting. See page 79 of this Report.

404 U.S. Const. amend. IV.

405 *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)); *see United States v. Jones*, 132 S. Ct. 945, 949-50 (2012).

406 *Katz*, 389 U.S. at 352-59; *see Arizona v. Gant*, 556 U.S. 332, 338 (2009).

ruled on the extent of Fourth Amendment protection for Internet communications, lower courts have concluded that emails are functionally analogous to mailed letters and that therefore their contents cannot be examined by the government without a warrant.[407] The same may be true for other, similarly private forms of Internet communication, although this question awaits further development by the courts.

B. Foreign Intelligence Exception to the Warrant Requirement

Under the authority of Section 702, the government collects telephone and Internet communications without obtaining individual judicial warrants for the specific people it targets. Decisions about which telephone and Internet communications to collect are made by executive branch personnel without court review. While the FISC plays a role in overseeing the categories of foreign intelligence the government seeks, the procedures it employs, and its adherence to statutory and constitutional limits, the court has no part in approving individual targeting decisions.

"Although as a general matter, warrantless searches are *per se* unreasonable under the Fourth Amendment, there are a few specifically established and well-delineated exceptions to that general rule."[408] And while wiretapping and other forms of domestic electronic surveillance generally require a warrant, the Supreme Court has left open the question of whether "safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security" and "the activities of foreign powers."[409]

In other words, there may be a "foreign intelligence exception" to the warrant requirement permitting the executive branch to conduct wiretapping and other forms of electronic surveillance without judicial approval. The Supreme Court has not decided whether such an exception exists, in part because the 1978 enactment of the Foreign Intelligence Surveillance Act ("FISA") forestalled the question: the Act established a framework for foreign intelligence surveillance under which the executive branch obtains

---

407 *See United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010) (stating that "[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection," and holding that government agents must obtain a warrant based on probable cause before compelling an Internet service provider to turn over the contents of a subscriber's emails); *United States v. Maxwell*, 45 M.J. 406, 418 (C.A.A.F. 1996) (holding that "the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant."); Bates October 2011 Opinion, *supra*, at 73-74, 2011 WL 10945618, at *26 ("A person's 'papers' are among the four items that are specifically listed in the Fourth Amendment as subject to protection against unreasonable search and seizure. Whether they are transmitted by letter, telephone or e-mail, a person's private communications are akin to personal papers.").

408 *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010) (quoting *Katz*, 389 U.S. at 357) (internal quotation marks omitted).

409 *Katz*, 389 U.S. at 358 n.23; *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 308 (1972) ("*Keith*").

warrant-like orders from the FISA court before engaging in surveillance that falls within the ambit of the statute.[410]

While the Supreme Court has not spoken, lower courts evaluating surveillance conducted before the enactment of FISA addressed the existence of a foreign intelligence exception, and every court to decide the question recognized such an exception.[411] More recently the Foreign Intelligence Surveillance Court of Review concluded that a foreign intelligence exception permitted warrantless surveillance "directed at a foreign power or an agent of a foreign power" — which could include U.S. citizens — under the Protect America Act, a predecessor to Section 702.[412]

This precedent does not neatly resolve all questions about the existence and scope of a foreign intelligence exception to the warrant requirement.[413] The Board takes no position here on the existence or scope of that exception. We note that the program's intrusion on U.S. persons' privacy is reduced by its focus on targeting individually selected foreigners located outside the United States from whom the government reasonably

---

410 *See* 50 U.S.C. §§ 1801-1812; *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 161 (2d Cir. 2008).

411 *See United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973); *but see Zweibon v. Mitchell*, 516 F.2d 594, 618-20 (D.C. Cir. 1975).

It is not necessarily clear that the Section 702 program would fall within the *scope* of the foreign intelligence exception recognized by these decisions, which were limited to surveillance directly authorized by the Attorney General, targeting foreign powers or their agents, and/or pursuing foreign intelligence as the primary or sole purpose of the surveillance. *See Truong Dinh Hung*, 629 F.2d at 912-16 (approving surveillance authorized by Attorney General "only if [the executive] is attempting primarily to obtain foreign intelligence from foreign powers or their assistants"); *Buck*, 548 F.2d at 875 (approving surveillance "expressly authorized by the Attorney General"); *Butenko*, 494 F.2d at 596, 606 (approving surveillance "concerning activities within the United States of foreign powers" where "the primary purpose of these searches is to secure foreign intelligence information"); *Brown*, 484 F.2d at 421 (approving "electronic surveillance authorized by the Attorney General and made solely for the purpose of gathering foreign intelligence"). Under Section 702, targets are selected by NSA personnel without Attorney General approval, and they need not be foreign powers or their agents; foreign intelligence need only be "a significant purpose" of the surveillance. *See* 50 U.S.C. § 1881a(a), (g)(2)(A)(v).

Critically, however, Section 702 targets cannot be U.S. persons or anyone located in the United States. Moreover, limits expressed in pre-FISA opinions addressing the president's *inherent* and unilateral constitutional power to conduct foreign intelligence surveillance do not necessarily apply to executive implementation of a congressionally enacted statute that involves oversight by all three branches of government. *See United States v. Abu-Jihaad*, 630 F.3d 102, 121 (2d Cir. 2010).

412 *See In re Directives*, 551 F.3d at 1010-12.

413 Apart from the distinctions noted above, nearly all of the relevant decisions predated the implementation of FISA's surveillance framework beginning in 1978, and experience with FISA and the FISA court since then arguably undermines some of the rationales underlying the foreign intelligence exception, such as the fear that a warrant requirement will unduly "reduce the flexibility of executive foreign intelligence initiatives" and that the judiciary is ill-suited to address "the delicate and complex decisions that lie behind foreign intelligence surveillance." *Truong Dinh Hung*, 629 F.2d at 913.

expects to obtain foreign intelligence — and by the government's employment of oversight mechanisms to help ensure adherence to those limitations. Unlike the warrantless surveillance of the pre-FISA era, U.S. persons and others in the United States cannot be targeted under this program, and therefore the government never will be permitted to collect and retain their entire communications history.[414] Instead, the government will have access only to those scattered communications that occur between a U.S. person and a targeted overseas foreigner, or that are acquired through "about" collection or as part of an MCT (which are subject to special limitations on retention and use). Moreover, the fact that the people targeted under Section 702 are situated in foreign countries may often make it difficult and time-consuming for the government to assemble documentation about them sufficient to obtain independent judicial approval for surveillance — while those targets' lack of Fourth Amendment rights militates against any legal obligation to obtain such approval or to strictly limit targeting to foreign powers and their agents.

C. The "Reasonableness" Framework

"Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution."[415] Thus, "even though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement."[416] The absence of a warrant requirement simply means that, "rather than employing a *per se* rule of unreasonableness," privacy concerns and governmental interests must be balanced to determine if the intrusion is reasonable.[417]

"Whether a search is reasonable," therefore, "is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[418] Making this determination requires considering the "totality of the circumstances."[419]

Applying this test to a program of intelligence gathering demands "sensitivity both to the government's right to protect itself from unlawful subversion and attack and to the

---

414 If a U.S. person or someone located in the United States is inadvertently targeted based on an erroneous belief about that person's nationality or location, all of the communications acquired through that targeting must be destroyed, unless, for example, the Director or Acting Director of the NSA specifically determines in writing that an individual communication should be retained because it satisfies one of four criteria. See pages 49-50 of this Report.

415 *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).

416 *In re Directives*, 551 F.3d at 1012 (citing *United States v. Place*, 462 U.S. 696, 703 (1983)).

417 *King*, 133 S. Ct. at 1970 (quoting *Illinois v. McArthur*, 531 U.S. 326, 331 (2001)).

418 *Samson v. California*, 547 U.S. 843, 848 (2006) (internal quotation marks omitted).

419 *Samson*, 547 U.S. at 848.

citizen's right to be secure in his privacy against unreasonable government intrusion."[420] When considering surveillance directed at national security threats, particularly those of a foreign nature, it is appropriate to "begin the inquiry by noting that the President of the United States has the fundamental duty, under Art. II, s 1, of the Constitution, to 'preserve, protect and defend the Constitution of the United States,'" and that "[i]mplicit in that duty is the power to protect our government against those who would subvert or overthrow it by unlawful means."[421] More broadly, the government's interest in protecting national security "is of the highest order of magnitude."[422]

Additional consideration is due to the fact that the executive branch, acting under Section 702, is not exercising its Article II power unilaterally, but rather is implementing a statutory scheme enacted by Congress after public deliberation regarding the proper balance between the imperatives of privacy and national security. By establishing a statutory framework for surveillance conducted within the United States but exclusively targeting overseas foreigners, subject to certain limits and oversight mechanisms, "Congress sought to accommodate and advance both the government's interest in pursuing legitimate intelligence activity and the individual's interest in freedom from improper government intrusion."[423] The framework of Section 702, moreover, includes a role for the judiciary in ensuring compliance with statutory and constitutional limits, albeit a more circumscribed role than the approval of individual surveillance requests. Where, as here, "the powers of all three branches of government — in short, the whole of federal authority" — are involved in establishing and monitoring the parameters of an intelligence-gathering activity, the Fourth Amendment calls for a different calculus than when the executive branch acts alone.[424]

Furthermore, the hostile activities of terrorist organizations and other foreign entities are prone to being geographically dispersed, long-term in their planning, conducted in foreign languages or in code, and coordinated in large part from locations outside the reach of the United States. Accordingly, "complex, wide-ranging, and

---

420 *Keith*, 407 U.S. at 299 (addressing intelligence gathering aimed at domestic national security threats).

421 *Keith*, 407 U.S. at 310.

422 *In re Directives*, 551 F.3d at 1012 (citing *Haig v. Agee*, 453 U.S. 280, 307 (1981)); *see Keith*, 407 U.S. at 312 ("It has been said that '(t)he most basic function of any government is to provide for the security of the individual and of his property.'" (citation omitted)).

423 *United States v. Cavanagh*, 807 F.2d 787, 789 (9th Cir. 1987) (addressing traditional FISA).

424 *Abu-Jihaad*, 630 F.3d at 121 (addressing traditional FISA); *cf. Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring).

decentralized organizations, such as al Qaeda, warrant sustained and intense monitoring in order to understand their features and identify their members."[425]

On the other side of the coin, the acquisition of private communications intrudes on Fourth Amendment interests. Even though U.S. persons and persons located in the United States are subject to having their telephone conversations collected only when they communicate with a targeted foreigner located abroad, the program nevertheless gains access to numerous personal conversations of U.S. persons that were carried on under an expectation of privacy. Email communications to and from U.S. persons, which the FISA court has said are akin to "papers" protected under the Fourth Amendment,[426] are also subject to collection in a variety of circumstances. Digital tools enable the government to query the repository of collected communications to locate communications involving a given person in search of foreign intelligence or evidence of a crime.[427]

D. Holistic Assessment of Reasonableness

As discussed elsewhere in this Report, the Board believes that the Section 702 program significantly aids the government's efforts to prevent terrorism, as well as to combat weapons proliferation and gather foreign intelligence for other purposes. The question, then, is how the program's intrusion on the privacy of U.S. persons weighs against its substantial contribution to these governmental interests.[428]

This evaluation must consider *the program as a whole* — taking into account how and why the communications of U.S. persons are acquired and what is done with them afterward. Thus, the privacy risks posed by the comparatively broad scope of targeting under this program and the absence of individual warrants must be offset by the applicable rules restricting the acquisition, use, dissemination, and retention of the communications that are acquired. In this regard, we must consider whether practices that permit use of U.S.

---

425 *In re Terrorist Bombings*, 552 F.3d at 175 (citing *In re Sealed Case*, 310 F.3d 717, 740-41 (FISA Ct. Rev. 2002)).

426 *See* Bates October 2011 Opinion, *supra*, at 74, 2011 WL 10945618, at *26 ("[T]he Supreme Court has held that the parties to telephone communications and the senders and recipients of written communications generally have a reasonable expectation of privacy in the contents of those communications . . . . The intrusion resulting from the interception of the contents of electronic communications is, generally speaking, no less substantial."). Since the nineteenth century, in order to protect the security of personal papers and effects, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail. *Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("Letters . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."). The Sixth Circuit Court of Appeals has held that email enjoys constitutional protection no less than physical letters. *Warshak*, 631 F.3d at 284-86.

427 See pages 55-60 of this Report for a description of the rules and procedures governing queries.

428 *See Samson*, 547 U.S. at 848.

persons' communications after their collection are appropriate given the less rigorous rules on targeting that permitted their acquisition.

This holistic approach is consistent with available precedent. When evaluating governmental policies authorizing warrantless searches or seizures, the Supreme Court has indicated that limits on the uses to which the collected information may be put, and on access to that information, bear on the policy's reasonableness under the Fourth Amendment.[429] Lower courts addressing the traditional FISA process have similarly noted that, despite its somewhat more lenient requirements compared with traditional criminal wiretaps, it safeguards privacy rights through "an expanded conception of minimization that differs from that which governs law-enforcement surveillance."[430] The Foreign Intelligence Surveillance Court of Review, addressing a surveillance program with similarities to Section 702, emphasized the "matrix of safeguards" governing the program, including "effective minimization procedures" that "serve[d] as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons."[431] The FISA court has applied this approach to Section 702, having "recognized that the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."[432]

The government has acknowledged that the Fourth Amendment rights of U.S. persons are affected when their communications are acquired under Section 702 incidentally or otherwise, and it has echoed the FISA court's observation that the implementation of adequate minimization procedures is part of what makes the collection reasonable.[433]

---

429 *See, e.g.*, *King*, 133 S. Ct. at 1967 (in approving collection of DNA information from arrestees, ascribing significance to restrictions on the information that may be added to databases and for what purposes it may be used); *Vernonia*, 515 U.S. at 658 (emphasizing that "the results of the [drug] tests [for student athletes] are disclosed only to a limited class of school personnel who have a need to know; and they are not turned over to law enforcement authorities or used for any internal disciplinary function").

430 *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982) (citation omitted).

431 *In re Directives*, 551 F.3d at 1013, 1015.

432 *See* Bates October 2011 Opinion, *supra*, at 77, 2011 WL 10945618, at *27. Exemplifying this approach, when the FISA court concluded that the upstream portion of the program was unreasonably acquiring too many domestic and irrelevant communications through the collection of MCTs, it declared that portion of the program to violate the Fourth Amendment, but it later concluded that the program had returned within constitutional bounds after new procedures were adopted to specially handle those communications. *See id*. at 68-79, 2011 WL 10945618, at *24-28; *see also* Memorandum Opinion, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10947772 (FISA Ct. Nov. 30, 2011), *available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

433 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 15 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ) ("That's not to say that U.S. persons whose . . . communications are collected incidentally doesn't trigger a Fourth Amendment review. It does. Those people

An important ramification of this holistic approach is that concerns about post-collection practices such as the use of queries to search for the communications of specific U.S. persons cannot be dismissed on the basis that the communications were "lawfully collected." Rather, whether Section 702 collection is constitutionally reasonable in the first place, and hence "lawful," depends on the reasonableness of the surveillance regime as a whole, including whether its rules affecting the acquisition, use, dissemination, and retention of the communications of U.S. persons appropriately balance the government's valid interests with the privacy of U.S. persons.

This totality of the circumstances test is applicable when examining the implications of "incidental" collection. Where a wiretap is conducted in a criminal investigation pursuant to a warrant, satisfaction of the three requirements of the warrant clause (probable cause, particularity, and prior judicial review)[434] renders the wiretap constitutionally reasonable — both as to the intended subjects of the surveillance *and* as to any persons who end up being incidentally overheard, the full range of whom the government can never predict.[435] Likewise, under Title I of FISA, the government obtains warrant-like orders from the FISA court that require a modified form of particularity and probable cause.[436] Just as the requirements of judicial review, probable cause, and particularity render a wiretap constitutionally reasonable in the criminal context, even as to individuals about whom the government had no prior evidence, so the corresponding protections of Title I of FISA render it reasonable under the Fourth Amendment, courts have held.[437]

However, where surveillance is undertaken without individual warrants or judicial orders, as under Section 702, and where the warrant requirements therefore are not satisfied, the legitimacy of the surveillance must be assessed under the reasonableness standard of the Fourth Amendment as described above, weighing the competing privacy

---

still have Fourth Amendment rights, but . . . what the FISA court has said is that the minimization procedures that are in place render that collection reasonable from a Fourth Amendment perspective."); *see also* Government's Unclassified Memorandum in Opposition to Defendants' Motion to Suppress, at 62, *United States v. Muhtorov*, No. 12-0033 (D. Colo. May 9, 2014) (arguing that the Section 702 program's targeting and minimization rules contribute to its reasonableness under the Fourth Amendment).

434 *Dalia v. United States*, 441 U.S. 238, 255 (1979) (listing the requirements of a search warrant).

435 *See United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977); *United States v. Kahn*, 415 U.S. 143, 155 n.15 (1974); *United States v. Gaines*, 639 F.3d 423, 429-33 (8th Cir. 2011); *United States v. Urban*, 404 F.3d 754, 773-74 (3d Cir. 2005); *United States v. Tehfe*, 722 F.2d 1114, 1118 (3d Cir. 1983); *United States v. Ramsey*, 503 F.2d 524, 526 n.7 (7th Cir. 1974). Of course, even a validly authorized wiretap or other search can be executed in a constitutionally unreasonable manner.

436 *See In re Sealed Case*, 310 F.3d at 739-40.

437 *See, e.g.*, *United States v. Stewart*, 590 F.3d 93, 129 (2d Cir. 2009); In *re Sealed Case*, 310 F.3d at 741; *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *Cavanagh*, 807 F.2d at 789-91; *United States v. Duggan*, 743 F.2d 59, 79-80 & n.7 (2d Cir. 1984).

and governmental interests while taking into account the totality of circumstances. Thus, even where only foreigners outside the United States are targeted, the nature of the collection and use of some communications involving a U.S. person bears on the constitutional reasonableness of the program. Simply put, the "totality of the circumstances" that must be considered under the Fourth Amendment in this context may include factors such as why U.S. persons' communications are acquired, the frequency with which they are acquired, how long they may be retained, who is given access to them, whether and how the government may query them for information about specific U.S. persons, under what circumstances they may be disseminated, and what degree of oversight attends to these matters. For instance, given the comparatively low standards for *collection* of information under Section 702, standards for querying the collected data to find the communications of specific U.S. persons may need to be more rigorous than where higher standards are required at the collection stage.

Applying this holistic inquiry to the Section 702 program therefore requires examining a web of factors bearing on the collection, use, dissemination, and retention of the communications of U.S. persons under the program. Pulling one of the threads of this web, in a more or less privacy-protective direction, alters the total picture. The ultimate Fourth Amendment assessment rests on an appraisal of the point at which any particular feature of the program, or any particular combination of features, goes too far and pushes the program across the threshold of unreasonableness.

In the Board's view, the core of this program — acquiring the communications of specifically targeted foreign persons who are located outside the United States, upon a belief that those persons are likely to communicate foreign intelligence, using specific communications identifiers, subject to FISA court–approved targeting rules that have proven to be accurate in targeting persons outside the United States, and subject to multiple layers of rigorous oversight — fits within the totality of the circumstances test for reasonableness as it has been defined by the courts to date.

Outside of this fundamental core, certain aspects of the Section 702 program raise questions about whether its impact on U.S. persons pushes the program over the edge into constitutional unreasonableness. Such aspects include the scope of the incidental collection of U.S. persons' communications, the use of "about" collection to acquire Internet communications that are neither to nor from the target of surveillance, the collection of MCTs that predictably will include U.S. persons' Internet communications unrelated to the purpose of the surveillance, the use of database queries to search the information collected under the program for the communications of specific U.S. persons, and the possible use of

communications acquired under the program for criminal assessments, investigations, or proceedings that have no relationship to foreign intelligence.[438]

These features of the Section 702 program, and their cumulative potential effects on the privacy of U.S. persons, push the entire program close to the line of constitutional reasonableness. At the very least, too much expansion in the collection of U.S. persons' communications or the uses to which those communications are put may push the program over the line. The response if any feature tips the program over the line is not to discard the entire program; instead, it is to address that specific feature.

With these concerns in mind, the next section of this Report offers a set of proposals designed to push the program more comfortably into the sphere of reasonableness, ensuring that the program remains tied to its constitutionally legitimate core. Because the same factors that bear on Fourth Amendment reasonableness under a "totality of the circumstances" test are equally relevant to an assessment based purely on policy, the Board opts to present its proposals for changes to the Section 702 program as policy recommendations, without rendering a judgment about which, if any, of those proposals might be necessary from a constitutional perspective. This approach is fitting because some of the facts that may bear on the reasonableness of the Section 702 program under the Fourth Amendment, such as how many U.S. persons' communications and domestic communications are acquired, simply are not known. It also permits us to offer the recommendations that we believe are merited on privacy grounds without making fine-tuned determinations about whether any aspect of the status quo is constitutionally fatal, and without limiting our recommendations to changes that we may deem constitutionally required.

In sum, the Board has carefully considered the totality of the circumstances surrounding the Section 702 program that must be considered in assessing the program's reasonableness under the Fourth Amendment, but rather than render a judgment about the constitutionality of the program as a whole, the Board instead has addressed the areas of concern it has identified by formulating recommendations for changes to those aspects of the program.

---

438 Anecdotally, the FBI has advised the Board that it is extremely unlikely that an agent or analyst who is conducting an assessment of a non–national security crime would get a responsive result from the query against the Section 702–acquired data.

IV. Analysis of Treatment of Non-U.S. Persons

The treatment of non-U.S. persons under U.S. surveillance programs raises important but difficult legal and policy questions. Privacy is a human right that has been recognized most prominently in the International Covenant on Civil and Political Rights ("ICCPR"), an international treaty ratified by the U.S. Senate. Many of the generally applicable protections that already exist under U.S. surveillance laws apply to U.S. and non-U.S. persons alike. The President's recent initiative under Presidential Policy Directive 28 on Signals Intelligence ("PPD-28")[439] will further address the extent to which non-U.S. persons should be afforded the same protections as U.S. persons under U.S. surveillance laws. Because PPD-28 invites the PCLOB to be involved in its implementation, the Board has concluded that it can make its most productive contribution in assessing these issues in the context of the PPD-28 review process.

A. Existing Legal Protections for Non-U.S. Persons' Privacy

A number of provisions of Section 702, as well as provisions in other U.S. surveillance laws, protect the privacy of U.S. and non-U.S. persons alike. These protections can be found, for example, in (1) limitations on the scope of authorized surveillance under Section 702; (2) damages and other civil remedies that are available to subjects of unauthorized surveillance as well as sanctions that can be imposed on government employees who engage in such conduct; and (3) prohibitions on unauthorized secondary use and disclosure of information acquired pursuant to the Section 702 program. These sources of statutory privacy protections are discussed briefly.

The first important privacy protection provided to non-U.S. persons is the statutory limitation on the scope of Section 702 surveillance, which requires that targeting be conducted only for purposes of collecting foreign intelligence information.[440] The definition of foreign intelligence information purposes is limited to protecting against actual or potential attacks; protecting against international terrorism, and proliferation of weapons of mass destruction; conducting counter-intelligence; and collecting information with respect to a foreign power or foreign territory that concerns U.S. national defense or foreign affairs.[441] Further limitations are imposed by the required certifications identifying the specific categories of foreign intelligence information, which are reviewed and

---

439 Presidential Policy Directive — Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435 (Jan. 17, 2014) ("PPD-28"), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

440 50 U.S.C. § 1881a(a).

441 50 U.S.C. § 1801(e).

approved by the FISC.[442] These limitations do *not* permit unrestricted collection of information about foreigners.

The second group of statutory privacy protections for non-U.S. persons are the penalties that apply to government employees who engage in improper information collection practices — penalties that apply whether the victim is a U.S. person or a non-U.S. person. Thus, if an intelligence analyst were to use the Section 702 program improperly to acquire information about a non-U.S. person (for example, someone with whom he or she may have had a personal relationship), he or she could be subject not only to the loss of his or her employment, but to criminal prosecution.[443] Finally, a non-U.S. person who was a victim of a criminal violation of either FISA or the Wiretap Act could be entitled to civil damages and other remedies.[444] In sum, if a U.S. intelligence analyst were to use the Section 702 program to collect information about a non-U.S. person where it did not both meet the definition of foreign intelligence and relate to one of the certifications approved by the FISA court, he or she could face not only the loss of a job, but the prospect of a term of imprisonment and civil damage suits.

The third privacy protection covering non-U.S. persons is the statutory restriction on improper secondary use found at 50 U.S.C. § 1806, under which information acquired from FISA-related electronic surveillance may not "be used or disclosed by Federal officers or employees except for lawful purposes."[445] Congress included this language "to insure that information concerning foreign visitors and other non-U.S. persons . . . is not used for illegal purposes."[446] Thus, use of Section 702 collection for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion, would violate Section 1806.

Further, FISA provides special protections in connection with legal proceedings, under which an aggrieved person — a term that includes non-U.S. persons — is required to be notified prior to the disclosure or use of any Section 702–related information in any

---

442 50 U.S.C. § 1881a(g)(2)(A)(v).

443 *See* Bates October 2011 Opinion, *supra*, at 17 n.15, 2011 WL 10945618, at *6 n.15 (criminal penalties of 50 U.S.C. § 1809 of the FISA are implicated by Section 702 surveillance that strays beyond the scope of the court's order approving such activities). In addition, to the extent that Section 702 program surveillance strayed from the certifications approved by the FISA court, it would potentially implicate the criminal provisions of the Wiretap Act, 18 U.S.C. § 2511(1), because the Section 702 surveillance would then lose its safe harbor for authorized FISA activities under Section 2511(2)(e) of the Wiretap Act.

444 *See* 50 U.S.C. § 1810 ("aggrieved person" not limited to U.S. persons); 18 U.S.C. § 2520 ("any person" not limited to U.S. persons); *see also Suzlon Energy Ltd. v. Microsoft Corp*., 671 F.3d 726, 728-29 (9th Cir. 2011) (construing the statutory term "any person" to include non-U.S. persons).

445 50 U.S.C. § 1806(a) (incorporated into Section 702 by 50 U.S.C. § 1881e(a)).

446 H.R. Rep. No. 95-1283(I), at 88-90 (1978) (discussing Section 106 of H.R. 7308, which became Section 106 of the FISA).

federal or state court.[447] The aggrieved person may then move to suppress the evidence on the grounds that it was unlawfully acquired and/or was not in conformity with the authorizing Section 702 certification.[448] Determinations regarding whether the Section 702 acquisition was lawful and authorized are made by a United States District Court, which has the authority to suppress any evidence that was unlawfully obtained or derived.[449]

Finally, as a practical matter, non-U.S. persons also benefit from the access and retention restrictions required by the different agencies' minimization and/or targeting procedures. While these procedures are legally required only for U.S. persons, the cost and difficulty of identifying and removing U.S. person information from a large body of data means that typically the entire dataset is handled in compliance with the higher U.S. person standards.

B. President's Initiative to Protect the Privacy of Non-U.S. Persons

As a matter of international law, privacy is a human right that has been recognized most prominently in the ICCPR, an international treaty ratified by the U.S. Senate. The question of how to apply the ICCPR right of privacy to national security surveillance, however, especially surveillance conducted in one country that may affect residents of another country, has to this point not been settled among the signatories to the treaty and is the subject of ongoing spirited debate.[450]

The executive branch is currently engaged in an extensive review of the extent to which, as a policy matter, the United States should afford all persons, regardless of nationality, a common baseline level of privacy protections in connection with foreign intelligence surveillance. This review began on January 17 of this year, when President Obama issued PPD-28,[451] in which he directed the review of the treatment of information regarding non-U.S. persons in connection with its surveillance programs.

Issues relating to the treatment of non-U.S. persons in government surveillance programs are by no means limited to the Section 702 program. Questions arise in

---

447 *See* 50 U.S.C. § 1806(c), (d).

448 50 U.S.C. § 1806(e).

449 50 U.S.C. § 1806(f), (g).

450 The United States currently interprets the ICCPR as not applying extra-territorially. Nonetheless the Board has received thoughtful comments and testimony arguing to the contrary. The Board also notes that in November 2013, the United Nations adopted, with United States support, a Resolution on "The right to privacy in the digital age." This resolution includes a provision requesting that the United Nations High Commissioner for Human Rights develop and present a report examining "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale." This report is expected to be presented in August 2014.

451 PPD-28, *supra*.

connection with signals intelligence conducted under other statutes and programs, including Executive Order 12333. Under PPD-28, the government has begun to address, as a matter of policy, the privacy and civil liberties of non-U.S. persons in connection with the full spectrum of signals intelligence programs conducted by the United States. The introduction to that directive notes 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."[452] The government is presently in the process of implementing the principles set forth in that directive, including the requirement that "signals intelligence activities shall be as tailored as feasible."[453] PPD-28 sets forth a number of principles that have historically been, or will be, implemented, among them:

> Privacy and civil liberties shall be integral considerations in the planning of U.S. signals intelligence activities. The United States shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion. Signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not for any other purposes.[454]

Further, PPD-28 provides that:

> U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.[455]

The Intelligence Community has already begun reviewing various options for implementing PPD-28, and the Board will engage in this process. PPD-28 specifically provides for direct PCLOB participation:

> The Privacy and Civil Liberties Oversight Board is encouraged to provide [the President] with a report that assesses the implementation of any matters contained within this directive that fall within its mandate.[456]

---

452 PPD-28, *supra*.

453 PPD-28, *supra*, § 3(d).

454 PPD-28, *supra*, § 3(b).

455 PPD-28, *supra*, § 4.

456 PPD-28, *supra*, § 5(b).

The Board has thus concluded that the optimal way for it to assess the treatment of information of non-U.S. persons is in the broader context of the PPD-28 review where it can evaluate other surveillance programs, along with Section 702, with a view to an integrated approach to foreign subjects of surveillance and the collection of signals intelligence. The implementation of PPD-28 may change the way Section 702 is operated and in so doing alleviate some of the concerns that have been voiced about its treatment of non-U.S. persons.

Part 5:

POLICY ANALYSIS

I. Introduction

In the Board's assessment, the Section 702 program has proven valuable in enabling the government to prevent acts of terrorism within the United States and abroad, and to pursue other foreign intelligence goals. The program has helped the government to learn about the membership and activities of terrorist organizations, as well as to discover previously unknown terrorist operatives and disrupt specific terrorist plots. Although the program is large in scope and involves collecting a great number of communications, it consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence. The program does not operate by collecting communications in bulk.

At the same time, the communications of U.S. persons or people located in the United States may be acquired by the government under Section 702 in the course of targeting non-U.S. persons located abroad. The breadth of collection under the program and its technical complexity enhance this possibility. The communications of U.S. persons can be acquired when a U.S. person is in contact with a foreign target (who need not be involved in wrongdoing in order to be targeted), when the government makes a mistake, and in certain other situations. The government's ability to query its databases for the communications of specific U.S. persons, and to retain and disseminate such communications under certain circumstances, heightens the potential for privacy intrusions.

The Board has been impressed with the rigor of the government's efforts to ensure that it acquires only those communications it is authorized to collect, and that it targets only those persons it is authorized to target. Moreover, the government has taken seriously its obligations to establish and adhere to a detailed set of rules regarding how it handles U.S. person communications that it acquires under the program. Available figures suggest, consistent with the Board's own assessment, that the primary focus of the Section 702 program remains monitoring non-U.S. persons located overseas for valid foreign intelligence purposes. Nevertheless, there are some indications that the government may be gathering and utilizing a significant amount of information about U.S. persons under Section 702. While the Board has seen no evidence of abuse of this information for improper purposes, the collection and examination of personal communications can be a

privacy intrusion even in the absence of abuse, and a number of the Board's recommendations are motivated by a desire to provide more clarity and transparency regarding the government's activities in the Section 702 program.

II. Value of the Section 702 Program

A. Advantages and Unique Capabilities

The Section 702 program makes a substantial contribution to the government's efforts to learn about the membership, goals, and activities of international terrorist organizations, and to prevent acts of terrorism from coming to fruition. Section 702 allows the government to acquire a greater range of foreign intelligence than it otherwise would be able to obtain, and it provides a degree of flexibility not offered by comparable surveillance authorities.

Because the oversight mandate of the Board extends only to those measures taken to protect the nation from terrorism, our focus in this section is limited to the counterterrorism value of the Section 702 program, although the program serves a broader range of foreign intelligence purposes.[457]

Section 702 enables the government to acquire the contents of international telephone and Internet communications in pursuit of foreign intelligence. While this ability is to some degree provided by other legal authorities, particularly "traditional" FISA and Executive Order 12333, Section 702 offers advantages over these other authorities.

In order to conduct electronic surveillance under "traditional" FISA (i.e., Title I of the Foreign Intelligence Surveillance Act of 1978), the government must persuade the Foreign Intelligence Surveillance Court ("FISC" or "FISA court"), under a standard of probable cause, that an individual it seeks to target for surveillance is an agent of a foreign power, and that the telephone number or other communications facility it seeks to monitor is used, or is about to be used, by a foreign power or one of its agents.[458] In addition, a high-level executive branch official must certify (with a supporting statement of facts) that a significant purpose of the surveillance is to obtain foreign intelligence, and that the information sought cannot reasonably be obtained through normal investigative techniques.[459] To meet these requirements and satisfy the probable cause standard, facts must be gathered by the Intelligence Community, a detailed FISA court application must be drafted by the DOJ, the facts in the application must be vetted for accuracy, the senior

457 See page 25 of this Report.

458 50 U.S.C. § 1805(a)(2).

459 50 U.S.C. § 1804(a)(6).

government official's certification must be prepared, the Attorney General must approve the application, and the application must be submitted to the FISA court, which must review it, determine if the pertinent standards are met, and, if so, grant it.[460] These steps consume significant time and resources.[461] In practice, FISA applications are lengthy and the process not infrequently takes weeks from beginning to final approval.[462]

This system is deliberately rigorous, for it was designed to provide a check on the government's surveillance of U.S. persons and other people located in the United States. Its goal was to prevent the abusive and politically motivated surveillance of U.S. persons and domestic activists that had occurred under the guise of foreign intelligence surveillance in the mid-twentieth century. Under FISA, electronic surveillance may be directed only at individuals who are acting at the behest of a foreign power (such as a foreign government or international terrorist organization), only for legitimate foreign intelligence purposes, and only where the aims of the surveillance cannot be achieved by other means.[463] The statute's procedural hurdles help to ensure that surveillance takes place only after detailed analysis, a strong factual showing, measured judgment by high-level executive branch officials, and approval by a neutral judge.

Although the FISA process was designed for surveillance directed at people located in the United States, the government later sought and obtained approval from the FISA court to use this process to target foreign persons located outside the United States as well. Developments in communications technology and the Internet services industry meant that such surveillance could feasibly be conducted from within the United States in some instances.[464] Utilizing the process of traditional FISA to target significant numbers of individuals overseas, however, required considerable time and resources, and government officials have argued that it slowed and sometimes prevented the acquisition of important intelligence.[465]

---

460 *See* 50 U.S.C. §§ 1804, 1805.

461 These steps also must be repeated each time the government wishes to continue the surveillance beyond the time limit specified in the original order. *See* 50 U.S.C. § 1805(d).

462 FISA permits surveillance to begin prior to court approval in emergency situations, but in order to exercise this option the Attorney General must make a determination that an emergency exists and that the factual basis required for the surveillance exists, and an application must be submitted to the FISA court for the normal probable cause determination within seven days. *See* 50 U.S.C. § 1805(e).

463 Moreover, when the target of surveillance is a U.S. person, that person must be "knowingly" acting on behalf of a foreign power. *See* 50 U.S.C. § 1801(b)(1), (2). An exception to the requirement that the target be acting on behalf of a foreign power permits a so-called "lone wolf" with no apparent connection to a foreign power to be targeted, if there is probable cause that the person is engaged in international terrorism or proliferation of weapons of mass destruction. *See* 50 U.S.C. §§ 1801(b)(1)(C), (D), 1805(a)(2)(A).

464 See pages 16-18 of this Report.

465 See pages 18-19 of this Report.

Section 702 imposes significantly fewer limits on the government when it targets non–U.S. persons located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted.[466] Rather than approving or denying individual targeting requests, the FISA court authorizes the surveillance program as a whole, approving the certification in which the government identifies the types of foreign intelligence information sought and the procedures the government uses to target people and handle the information it obtains.[467] Targets of surveillance need not be agents of foreign powers; instead, the government may target any non-U.S. person overseas whom it reasonably believes has or is likely to communicate designated types of foreign intelligence.[468] The government need not have probable cause for this belief, or for its belief that the target uses the particular selector, such as a telephone number or email address, to be monitored. There is no requirement that the information sought cannot be acquired through normal investigative techniques. Targeting decisions are made by NSA analysts and reviewed only within the executive branch.[469] Once monitoring of a particular person begins, it may continue until new information indicates that the person no longer is an appropriate target. Whether a person remains a valid target must be reviewed annually.[470]

These differences allow the government to target a much wider range of foreigners than was possible under traditional FISA. For instance, people who might have knowledge about a suspected terrorist can be targeted even if those people are not themselves involved in terrorism or any illegitimate activity.

In addition to expanding the pool of potential surveillance targets, Section 702 also enables a much greater degree of flexibility, allowing the government to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISA court for each targeting decision.

As a result of these two factors, the number of people who can feasibly be targeted is significantly greater under Section 702 than under the traditional FISA process. And

---

466 Under FISA and the FISA Amendments Act, the term "United States person" includes U.S. citizens, legal permanent residents, unincorporated associations with a substantial number of U.S. citizens or legal permanent residents as members, and corporations incorporated in the United States. It does not include associations or corporations that qualify as a "foreign power." *See* 50 U.S.C. § 1801(i).

467 50 U.S.C. § 1881a(a), (i).

468 NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 4 (April 16, 2014) ("NSA DCLPO REPORT"), *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

469 NSA DCLPO REPORT, *supra*, at 4-5.

470 Analysts are required to review the communications acquired from a target at least annually, to ensure that the targeting is still expected to provide the foreign intelligence sought and that the person otherwise remains an appropriate target under Section 702. *See* NSA DCLPO REPORT, *supra*, at 6.

indeed, the number of targets under the program has been steadily increasing since the statute was enacted in 2008.

The government also conducts foreign intelligence surveillance outside of the United States against non-U.S. persons under the authority of Executive Order 12333. In some instances, this surveillance can capture the same communications that the government obtains within the United States through Section 702. And because this collection takes place outside the United States, it is not restricted by the detailed rules of FISA outlined above.[471] Nevertheless, Section 702 offers advantages over Executive Order 12333 with respect to electronic surveillance. The fact that Section 702 collection occurs in the United States, with the compelled assistance of electronic communications service providers, contributes to the safety and security of the collection, enabling the government to protect its methods and technology. In addition, acquiring communications with the compelled assistance of U.S. companies allows service providers and the government to manage the manner in which the collection occurs. By helping to prevent incidents of overcollection and swiftly remedy problems that do occur, this arrangement can benefit the privacy of people whose communications are at risk of being acquired mistakenly.

B. Contributions to Counterterrorism

The Section 702 program has proven valuable in a number of ways to the government's efforts to combat terrorism. It has helped the United States learn more about the membership, leadership structure, priorities, tactics, and plans of international terrorist organizations. It has enabled the discovery of previously unknown terrorist operatives as well as the locations and movements of suspects already known to the government. It has led to the discovery of previously unknown terrorist plots directed against the United States and foreign countries, enabling the disruption of those plots.

While the Section 702 program is indeed a *program*, operating to some degree as a cohesive whole and approved by the FISA court accordingly, its implementation consists entirely of targeting specific individuals about whom the government already knows something. Because surveillance is conducted on an individualized basis where there is reason to target a particular person, it is perhaps unsurprising that the program yields a great deal of useful information.

The value of the Section 702 program is to some extent reflected in the breadth of NSA intelligence reporting based on information derived from the program. Since 2008, the number of signals intelligence reports based in whole or in part on Section 702 has

---

471 FISA does not generally cover surveillance conducted outside the United States, except where the surveillance intentionally targets a particular, known U.S. person, or where it acquires radio communications in which the sender and all intended recipients are located in the United States and the acquisition would require a warrant for law enforcement purposes. *See* 50 U.S.C. §§ 1801(f), 1881c.

increased exponentially. A significant portion of those reports relate to counterterrorism, and the NSA disseminates hundreds of reports per month concerning terrorism that include information derived from Section 702. Presently, over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. These reports are used by the recipient agencies and departments for a variety of purposes, including to inform senior leaders in government and for operational planning.

More concretely, information acquired from Section 702 has helped the Intelligence Community to understand the structure and hierarchy of international terrorist networks, as well as their intentions and tactics. In even the most well-known terrorist organizations, only a small number of individuals have a public presence. Terrorist groups use a number of practices to obscure their membership and activities. Section 702 has enabled the U.S. government to monitor these terrorist networks in order to learn how they operate and to understand how their priorities, strategies, and tactics continue to evolve.

Monitoring these networks under Section 702 has led the government to identify previously unknown individuals who are involved in international terrorism. Identifying such persons allows the government to pursue new efforts focusing on those individuals and the disruption of their activities, such as taking action to prevent them from entering the United States. Finally, the flexibility of Section 702 surveillance enables the government to effectively maintain coverage on particular individuals as they add or switch their modes of communications.

As important as discovering the identities of individuals engaged in international terrorism is determining where those individuals are located. Modern communications permit the members of a terrorist group, and even a small number of people involved in a specific plot, to be spread out all over the world. Information acquired from Section 702 has been used to monitor individuals believed to be engaged in terrorism.

In one case, for example, the NSA was conducting surveillance under Section 702 of an email address used by an extremist based in Yemen. Through that surveillance, the agency discovered a connection between that extremist and an unknown person in Kansas City, Missouri. The NSA passed this information to the FBI, which identified the unknown person, Khalid Ouazzani, and subsequently discovered that he had connections to U.S.-based Al Qaeda associates, who had previously been part of an abandoned early stage plot to bomb the New York Stock Exchange. All of these individuals eventually pled guilty to providing and attempting to provide material support to Al Qaeda.

Finally, pursuit of the foregoing information under Section 702 has led to the discovery of previously unknown terrorist plots and has enabled the government to

disrupt them. By providing the sites of specific targets of attacks, the means being contemplated to carry out the attacks, and the identities and locations of the participants, the Section 702 program has directly enabled the thwarting of specific terrorist attacks, aimed at the United States and at other countries.

For instance, in September 2009, the NSA monitored under Section 702 the email address of an Al Qaeda courier based in Pakistan. Through that collection, the agency intercepted emails sent to that address from an unknown individual located in the United States. Despite using language designed to mask their true intent, the messages indicated that the sender was urgently seeking advice on the correct mixture of ingredients to use for making explosives. The NSA passed this information to the FBI, which used a national security letter to identify the unknown individual as Najibullah Zazi, located near Denver, Colorado. The FBI then began intense monitoring of Zazi, including physical surveillance and obtaining legal authority to monitor his Internet activity. The Bureau was able to track Zazi as he left Colorado a few days later to drive to New York City, where he and a group of confederates were planning to detonate explosives on subway lines in Manhattan within the week. Once Zazi became aware that law enforcement was tracking him, he returned to Colorado, where he was arrested soon after. Further investigative work identified Zazi's co-conspirators and located bomb-making components related to the planned attack. Zazi and one of his confederates later pled guilty and cooperated with the government, while another confederate was convicted and sentenced to life imprisonment. Without the initial tip-off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702, the subway-bombing plot might have succeeded.

In cases like the Zazi and Ouazzani investigations, one might ask whether the government could have monitored the communications of the overseas extremists without Section 702, using the traditional FISA process. In some instances, that might be the case. But the process of obtaining court approval for the surveillance under the standards of traditional FISA may, for the reasons explained above, limit the number of people the government can feasibly target and increase the delay before surveillance on a target begins, such that significant communications could be missed.

The Board has received information about other instances in which the Section 702 program has played a role in counterterrorism efforts. Most of these instances are included in a compilation of 54 "success stories" involving the Section 215 and 702 programs that was prepared by the Intelligence Community last year in the wake of Edward Snowden's unauthorized disclosures. Other examples have been shared with the Board more recently. Information about these cases has not been declassified, but some general information about them can be shared. In approximately twenty cases that we have reviewed, surveillance conducted under Section 702 was used in support of an already existing counterterrorism investigation, while in approximately thirty cases, Section 702

information was the initial catalyst that identified previously unknown terrorist operatives and/or plots. In the vast majority of these cases, efforts undertaken with the support of Section 702 appear to have begun with narrowly focused surveillance of a specific individual whom the government had a reasonable basis to believe was involved with terrorist activities, leading to the discovery of a specific plot, after which a short, intensive period of further investigation ensued, leading to the identification of confederates and arrests of the plotters. A rough count of these cases identifies well over one hundred arrests on terrorism-related offenses. In other cases that did not lead to disruption of a plot or apprehension of conspirators, Section 702 appears to have been used to provide warnings about a continuing threat or to assist in investigations that remain ongoing. Approximately fifteen of the cases we reviewed involved some connection to the United States, such as the site of a planned attack or the location of operatives, while approximately forty cases exclusively involved operatives and plots in foreign countries.[472]

C. Contributions to Other Foreign Intelligence Efforts

As noted above, the oversight mandate of our Board extends only to those measures taken by the government to protect the nation from terrorism. Some governmental activities, including the Section 702 program, are not aimed exclusively at preventing terrorism but also serve other foreign intelligence and foreign policy goals. The Section 702 program, for instance, is also used for surveillance aimed at countering the efforts of proliferators of weapons of mass destruction.[473] Given that these other foreign intelligence purposes of the program are not strictly within the Board's mandate, we have not scrutinized the effectiveness of Section 702 in contributing to those other purposes with the same rigor that we have applied in assessing the program's contribution to counterterrorism. Nevertheless, we have come to learn how the program is used for these other purposes, including, for example, specific ways in which it has been used to combat weapons proliferation and the degree to which the program supports the government's efforts to gather foreign intelligence for the benefit of policymakers. Our assessment is that the program is highly valuable for these other purposes, in addition to its usefulness in supporting efforts to prevent terrorism.

---

472 The examples described in this paragraph do not represent an exhaustive list of all instances in which the Section 702 program has proven useful, even in counterterrorism efforts.

473 *See* S. Rep. No. 112-229, at 32 (2012) (appendix reproducing Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of the Director or National Intelligence) ("Section 702 . . . lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States.").

III. Privacy and Civil Liberties Implications of the Section 702 Program

A. Nature of the Collection under Section 702

1. Programmatic Surveillance

Unlike the telephone records program conducted by the NSA under Section 215 of the USA PATRIOT Act, the Section 702 program is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualized determination has been made. Once the government concludes that a specific non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information — and that this person uses a particular communications "selector," such as an email address or telephone number — the government acquires only those communications involving that particular selector.[474]

Every individual decision to target a particular person and acquire the communications associated with that person must be documented and approved by senior analysts within the NSA before targeting. Each targeting decision is later reviewed by an oversight team from the DOJ and the ODNI ("the DOJ/ODNI oversight team") in an effort to ensure that the person targeted is reasonably believed to be a non-U.S. person located abroad, and that the targeting has a legitimate foreign intelligence purpose. The FISA court does not approve individual targeting decisions or review them after they are made.

Although the "persons" who may be targeted under Section 702 include corporations, associations, and entities as well as individuals,[475] the government is not exploiting any legal ambiguity by "targeting" an entity like a major international terrorist organization and then engaging in indiscriminate or bulk collection of communications in order to later identify a smaller subset of communications that pertain to the targeted entity. To put it another way, the government is not collecting wide swaths of communications and then combing through them for those that are relevant to terrorism or contain other foreign intelligence. Rather, the government first identifies a communications identifier, like an email address, that it reasonably believes is used by the target, whether that target is an individual or an entity. It then acquires only those communications that are related to this identifier.[476] In other words, selectors are always

---

474 See pages 20-23 and 32-33 of this Report.

475 *See* 50 U.S.C. §§ 1801(m), 1881a(a).

476 The NSA's "upstream collection" (described elsewhere in this Report) may require access to a larger body of international communications than those that contain a tasked selector. Nevertheless, the government has no ability to examine or otherwise make use of this larger body of communications, except to promptly determine whether any of them contain a tasked selector. Only those communications (or more precisely, "transactions") that contain a tasked selector go into government databases. See pages 36-41 of this Report.

unique communications identifiers used by the targeted persons. So under the Section 702 program, the government cannot, for instance, acquire communications because they are associated with a particular region where the government believes it is likely to find information related to one of its targets. Collection is instead limited to the communications identifiers of the targets themselves.

Likewise, although the selectors that the government could use are not limited to telephone numbers and email addresses, the government is not creatively interpreting the meaning of "selectors" to engage in bulk collection under Section 702. Even in the complex realm of Internet communications, a selector always must be associated with a specific person or entity. Thus, acquisition is always based on selecting communications that are associated with the target.[477]

2. Contents of Private Telephone and Internet Communications

Under Section 702, the government acquires the *contents* of international communications — collecting Internet communications like emails and recording telephone calls — as well as the addressing information or "metadata" associated with those communications. The contents of such communications may be highly personal and sensitive. U.S. persons and people located in the United States may not be targeted under Section 702, but their communications nevertheless can be acquired, including when they are in contact with a foreigner located abroad who has been targeted. Thus, the chance of government intrusion into private matters may be comparatively higher for individuals who maintain frequent contact with family members, friends, acquaintances, or professional contacts outside of the United States.

After being acquired by the government, communications obtained through Section 702 are stored in databases for default periods of time.[478] There, they are subject to being examined by NSA, CIA, and FBI analysts or agents in pursuit of foreign intelligence or evidence of a crime. Subject to the separate minimization procedures at each agency, communications can be identified and retrieved from these databases for examination based on their addressing information (such as the telephone numbers or email addresses involved), while Internet communications are also retrievable by scanning their contents for the presence of certain words or terms.

3. Scope of Targeting and Collection

While the Section 702 program is based entirely on individual targeting decisions, it nevertheless results in an extremely large amount of collection. In part, this is because

---

[477] This is true even in the unique contexts of so-called "about" collection and "MCT" collection, both of which are discussed below.

[478] See page 60 of this Report.

modern technology, especially the ability to store huge amounts of data, makes it logistically feasible to target large numbers of people. The breadth of collection is also possible because, as explained above, the standards under which targeting is permitted under Section 702 are less rigorous than those governing other surveillance activities conducted within the United States. The government enjoys much more latitude when targeting foreigners located outside the United States under Section 702 than it does when targeting people located in the United States under other legal authorities, even for foreign intelligence purposes. The range of people whom the government may target and the permissible reasons for that targeting are much broader, while the level of suspicion required and the legal steps the government must take before initiating surveillance are much lower. In particular, the FISA court approves the government's targeting and minimization procedures but plays no role in reviewing individual targeting decisions.[479]

As a result, the number of people targeted under Section 702 is considerable and collection has steadily grown. During the year 2013, 89,138 persons were targeted for collection under Section 702.

Thus, while the Board does not regard Section 702 as a "bulk" collection program, because it is based entirely on targeting the communications identifiers of specific people, neither does the program resemble traditional domestic surveillance conducted pursuant to individualized court orders based on probable cause. The FISA court instead determines whether to approve the surveillance program as a whole and plays a role in overseeing whether it stays within statutory and constitutional limits. The Section 702 program, in short, is perhaps best characterized by the term "programmatic surveillance."[480]

B. Acquisition of the Communications of U.S. Persons under Section 702

While the scope of targeting under Section 702 is broad, that targeting cannot include U.S. persons or people located in the United States. As a result, this program does not allow the government to gain comprehensive access to any U.S. person's communications: the government will not be able to hear every telephone call a U.S. person makes, for instance, or collect every email sent or received by that person. Instead, absent mistake or abuse, Section 702 enables the government to obtain only those communications that occur where a U.S. person is in contact with a targeted overseas foreigner, as well as those that are acquired in the unique circumstances of "about" and "MCT" collection (discussed below).

---

479 See pages 26-31 of this Report.

480 The Section 215 program, in contrast, represents both a bulk collection program and an example of programmatic surveillance.

Because it disallows *comprehensive* monitoring of any U.S. person, and prohibits deliberately acquiring even a single communication that is known to be solely among people located within the United States, the program would serve as a relatively poor vehicle to repress domestic dissent, monitor American political activists, or engage in other politically motivated abuses of the sort that came to light in the 1970s and prompted the enactment of FISA.

Nevertheless, as described below, under certain circumstances the program permits the government to collect a communication where one party is a U.S. person, including communications that are sensitive and private, and where the U.S. person may have taken steps to preserve the confidentiality of the communication. There are four main ways in which the Section 702 program, notwithstanding its focus on targeting foreigners located abroad, can lead to the acquisition of U.S. persons' communications.

1. Incidental Collection

A person targeted for surveillance who speaks on the phone or communicates over the Internet is communicating with someone else. That other person's communications with the target are said to have been "incidentally" acquired. In the context of the Section 702 program, the term "incidental collection" is used to refer to situations in which U.S. persons or people located in the United States have their communications acquired because they were in contact with a targeted foreigner located overseas. While the government cannot target U.S. persons or people located in the United States, it is permitted to acquire and in some cases retain and use communications in which a U.S. person is in contact with a target.

The term "incidental" is appropriate because such collection is not accidental or inadvertent, but rather is an anticipated collateral result of monitoring an overseas target.[481] But the term should not be understood to suggest that such collection is infrequent or that it is an inconsequential part of the Section 702 program.

The number of communications collected under Section 702 to which one party is a U.S. person or located in the United States is not known. And one of the purposes of the program is to discover communications between a target overseas and a person in the United States. Executive and legislative branch officials have repeatedly emphasized to us that, with respect to terrorism, communications involving someone in the United States are

---

481 *See* Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 97 (Mar. 19, 2014) (statement of Robert Litt, General Counsel, ODNI), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

some of the "most important" communications acquired under the program.[482] And indeed, where the program has directly led to the discovery and disruption of terrorist plots, it has sometimes done so by helping to discover previously unknown operatives in the United States through their communications with terrorism suspects located abroad.[483]

From a privacy perspective, however, incidental collection under Section 702 differs in at least two significant ways from incidental collection that occurs in the course of a criminal wiretap or the traditional FISA process.

First, in the criminal or FISA context the targets of surveillance must be believed to be criminals or agents of a foreign power.[484] That means that innocent U.S. persons need not worry about the government listening to their phone conversations or reading their emails except to the extent that they are communicating with suspected criminals or agents of foreign powers. The range of people whom the government may target under Section 702, on the other hand, is much broader. It is not limited to suspected terrorists or others engaged in nefarious activities. Instead, under an approved certification, the government may target any overseas foreigner who has or is likely to communicate certain kinds of foreign intelligence — who, for instance, may possess information "with respect to a foreign power or foreign territory that relates to . . . the conduct of the foreign affairs of the United States."[485] That person need not be acting at the behest of a foreign power or be engaged in any activities that are hostile toward the United States or would violate any laws. For instance, someone who has information about a terrorist operative may be targeted under Section 702, even if that person has no involvement in terrorism.

Second, to engage in traditional FISA or criminal electronic surveillance, the government must obtain approval from a judge, who independently assesses the legitimacy of the targeting and must be persuaded that the government's beliefs about the person

---

482 *See* Privacy and Civil Liberties Oversight Board, Transcript of Public Workshop regarding surveillance programs operated pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, at 109 (July 9, 2013) (statement of Steven Bradbury, formerly DOJ Office of Legal Counsel) (stating that Section 702 "is particularly focused on communications in and out of the United States because . . . those are the most important communications you want to know about if you're talking about a foreign terrorist suspect communicating to somebody you don't know inside the United States"); *see id*. at 116 (statement of Kenneth Wainstein, formerly DOJ National Security Division/White House Homeland Security Advisor) (agreeing), *available at* http://www.pclob.gov/SiteAssets/9-july-2013/Public%20Workshop%20-%20Full.pdf; *see also FISA for the 21st Century: Hearing before the Senate Comm. on the Judiciary,* 109th Cong. 9 (2006) (statement of General Michael V. Hayden, Director, CIA).

483 See pages 107-110 of this Report.

484 *See* 50 U.S.C. § 1805(a)(2)(A); 18 U.S.C. § 2518(3)(a).

485 50 U.S.C. § 1801(e)(2)(B). The range of foreign intelligence that the government may seek under Section 702 is limited by the certifications approved by the FISA court. See pages 24-31 of this Report for a description of the certification process.

and/or communications facility being targeted are supported by probable cause.[486] By providing a neutral check on the government's authority to conduct electronic surveillance, these protections help assure innocent U.S. persons that their conversations will not be incidentally acquired in the course of improper surveillance directed at another person.

These restrictions and checks are absent under Section 702. To be clear, such absence does not mean that the government has free rein: targeting rules, a system of intra- and inter-agency oversight, programmatic supervision by the FISA court, and a host of reporting requirements all work to ensure that the government's decisions about whom to monitor stay within legal bounds. But the expansiveness of the governing rules, combined with the technological capacity to acquire and store great quantities of data, permit the government to target large numbers of people around the world and acquire a vast number of communications. By 2011, for instance, the government was annually acquiring over 250 million Internet communications, in addition to telephone conversations.[487] The current number is significantly higher. Even if U.S. persons' communications make up only a small percentage of this total, the absolute number of their communications acquired could be considerable.

Minimization requirements to some degree compensate for the possibility of broad incidental collection. Those rules are described in detail earlier in this Report,[488] and their significance is discussed below. While the existence of minimization rules may temper the privacy impact of incidental collection, the scope of that collection may also bear on whether the minimization rules are adequate. The present lack of knowledge about the range of incidental collection under Section 702 therefore hampers attempts to gauge whether the program appropriately balances national security interests with the privacy of U.S. persons.

2. Inadvertent Collection

Sometimes the NSA acquires communications under Section 702 of U.S. persons or people located in the United States by mistake. This can occur when the NSA erroneously believes that a potential target is a foreigner or located outside the United States, and discovers the truth only after collection on that person begins. It can also occur as a result of human error, such as mistyping an email address in the targeting process. Additionally, mistakes can occur as a result of technological malfunctions. Finally, targets who were located outside the United States may travel into the country, making them no longer

---

486 *See* 50 U.S.C. § 1805; 18 U.S.C. § 2518.

487 Opinion at 29, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011) ("Bates October 2011 Opinion"), *available at* http://icontherecord.tumblr.com (noting submitted affidavits by the Director or Acting Director of NSA and the Director of FBI).

488 See pages 50-66 of this Report.

eligible for targeting, before the NSA discovers this fact. While all of these possibilities create risks that the NSA will acquire communications that it is not authorized to collect, the Board has been impressed by the seriousness with which the government attempts to ensure that this does not occur.

In any surveillance program as large in scope as the Section 702 program, particularly where collection involves highly sophisticated technology, mistakes are inevitable. The Board believes that the Section 702 program is implemented in a manner that reasonably avoids such errors. Furthermore, experience has shown that where there have been more significant mistakes, the government discovers them and complies with the reporting requirements that demand prompt disclosure of compliance incidents to the FISA court and to the oversight committees in Congress.

There have been a few significant large-scale implementation problems in the Section 702 program, all revolving around technological matters. As described earlier, technical problems have in some instances led the government to acquire communications not authorized for collection under the program. More recently, the checks that are designed to provide indications that a target is located inside the United States were substantially non-functioning for over a year. In yet another incident, the NSA discovered that its systems for purging data were not operating completely, leading to the retention of information that should have been destroyed.[489] In consultation with the FISA court, the government has resolved those issues appropriately and has worked to remedy the errors that were discovered.

Inadvertent collection can also occur on an individualized basis, such as where the NSA targets people whom it mistakenly believes are foreigners or located outside the United States. Commentators have questioned the rigor of the agency's "foreignness" determinations, particularly whether they rely on certain default assumptions where information about a person is lacking. The notion also has arisen that the agency employs a "51% test" in assessing the location and nationality of a potential target — in other words, that analysts need only be slightly more than half confident that the person being targeted is a non-U.S. person located outside the United States.

These characterizations are not accurate. In keeping with representations the government has made to the FISA court, NSA analysts consult multiple sources of information in attempting to determine a proposed target's foreignness, and they are obligated to exercise a standard of due diligence in that effort, making their determinations based on the totality of the circumstances. They also must document the information on

[489] See page 79 of this Report.

which they based their assessments, which must be reviewed and approved by two senior analysts prior to targeting, and which are subject to further review later.[490]

Available figures suggest that the percentage of instances in which the NSA accidentally targets a U.S. person or someone in the United States is tiny. In 2013, the DOJ reviewed one year of data to determine the percentage of cases in which the NSA's targeting decisions resulted in the "tasking" of a communications identifier that was used by someone in the United States or was a U.S. person. The NSA's error rate, according to this review, was 0.4 percent.[491] Moreover, once a targeting decision has been made, that is not the end of the story. Soon after collection on a selector begins, analysts must review a sample of the communications that have recently been collected, to ensure that the email address or other selector actually is associated with the person whom the NSA intended to target, and that this person is a foreigner located outside the United States. Additional measures are employed to re-verify the validity of continued collection against the selector.[492] In addition, the DOJ/ODNI oversight team reviews every targeting decision, including the documentation on which the "foreignness" determination was made. The oversight team conducts on-site reviews as part of this process, and when the documentation available is not sufficient to demonstrate the basis of a foreignness determination, the oversight team requests and obtains additional information.[493] The NSA counts the number of instances in which it discovers that a selector is or may be being used by someone in the United States — either because the target traveled to the United States or because the original targeting decision was erroneous. The percentage of such instances is also very small, with the total annual number of instances representing less than 1.5 percent of the average number of selectors targeted at any given moment.

To date, the DOJ/ODNI oversight team has not discovered any instances in which an analyst intentionally violated the statute, targeting procedures, or minimization procedures. In the history of the program, the government has identified only two instances of "reverse targeting" — that is, the prohibited targeting of overseas foreigners for the purpose of acquiring the communications of persons in the United States with whom they are in contact.[494]

---

490 NSA DCLPO REPORT, *supra*, at 4-5.

491 See pages 71-72 of this Report.

492 See pages 48-49 of this Report; NSA DCLPO REPORT, *supra*, at 6.

493 NSA DCLPO REPORT, *supra*, at 10.

494 See page 79 of this Report. In one case, the targeting resulted in no collection of communications. In the other case, all of the collection was purged.

In sum, as noted above, the Board is impressed by the rigor with which the government attempts to ensure that the persons it targets under Section 702 truly are non-U.S. persons located outside the United States.[495]

3. "About" Collection

One of the most controversial aspects of the Section 702 program is the practice of so-called "about" collection. This term describes the NSA's acquisition of Internet communications that are neither to nor from an email address — but that instead merely include a reference to that selector.[496] For instance, a communication between two third parties might be acquired because it contains a targeted email address in the body of the communication.[497]

The fact that the NSA acquires certain communications based on what is contained within the body of the communication has apparently led some to believe that the government is scanning the contents of U.S. persons' international communications to see if they are discussing particular subjects or using particular key words. Initial news articles describing "about" collection may have contributed to this perception, reporting that the NSA "is searching the contents of vast amounts of Americans' email and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance[.]"[498] This belief represents a misunderstanding of a more complex reality. "About" collection takes place exclusively in the NSA's acquisition of Internet communications through its upstream collection process. That is the process whereby the NSA acquires communications as they transit the Internet "backbone" within the United States. This process is distinguished from the NSA's PRISM collection, in which U.S.-based Internet service providers transmit communications to the government

---

495 See below for a discussion of what happens when the NSA discovers that it inadvertently acquired the communications of a U.S. person or someone in the United States.

496 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 13 (statement of Rajesh De, General Counsel, NSA).

497 *See* The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, at 4 (2012) (describing differences between targeting individuals under traditional FISA electronic surveillance provisions and targeting pursuant to Section 702). This document accompanied a 2012 letter sent by the Department of Justice and the Office of the Director of National Intelligence to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence urging the reauthorization of Section 702. *See* Letter from Kathleen Turner, Director of Legislative Affairs, ODNI, and Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, DOJ to the Hon. Dianne Feinstein, Chairman, Senate Committee on Intelligence, et. al. (May 4, 2012), *available at* http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf.

498 Charlie Savage, *N.S.A. Said to Search Content of Messages to and From U.S.*, N.Y. TIMES (Aug. 8, 2013).

directly.[499] Whereas PRISM collection is a comparatively simple process, because the government obtains communications of a service provider's customers directly from that provider, the upstream process is more complex, depending upon the use of collection devices with technological limitations that significantly affect the scope of collection.[500] Because of the way that Internet communications are transmitted in the form of data packets, the NSA's collection devices acquire what the agency and the FISA court have termed Internet "transactions."[501] As a result of this acquisition technique, the FISA court has explained, "the NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it[.]"[502]

This means that an Internet communication between third parties, not involving the target, can be acquired by the NSA if it contains a reference, for instance, to the email address of a target.[503] For this reason, "about" collection raises at least two serious concerns, one relatively simple, the other more complex.

First, "about" collection may be more likely than other forms of collection to acquire wholly domestic communications — something not authorized by Section 702. Because "about" communications are not to or from the email address that was tasked for acquisition,[504] which is used by a person reasonably believed to be located outside the United States, there is no guarantee that any of the participants to the communication are located outside the United States. In part to compensate for this problem, the NSA takes additional measures with its upstream collection to ensure that no communications are acquired that are entirely between people located in the United States. These measures can include, for instance, employing Internet protocol filters to acquire only communications that appear to have at least one end outside the United States.[505] In this process, Internet communications are first filtered to eliminate potential domestic communications, and then are screened to capture only communications containing a tasked selector.

---

499 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4; NSA DCLPO REPORT, *supra*, at 5. See pages 33-34 of this Report.

500 Bates October 2011 Opinion, *supra*, at 30, 2011 WL 10945618, at *10.

501 Bates October 2011 Opinion, *supra*, at 30, 2011 WL 10945618, at *10.

502 Bates October 2011 Opinion, *supra*, at 31, 2011 WL 10945618, at *11.

503 Joint Statement of Lisa O. Monaco, Assistant Attorney General, National Security Division, Dept. of Justice, et. al., *Hearing Before the House Permanent Select Comm. on Intelligence: FISA Amendments Act Reauthorization*, at 7 (Dec. 8, 2011) ("December 2011 Joint Statement"), *available at* http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf.

504 As explained earlier, persons are *targeted* under Section 702 while the selectors used by those persons are *tasked*.

505 NSA DCLPO REPORT, *supra*, at 5-6.

While we believe that the measures taken by the NSA to exclude wholly domestic "about" communications may be reasonable in light of current technological limits, they are not perfect.[506] Even where both parties to a communication are located in the United States, in a number of situations the communication might be routed internationally, in which case it could be acquired by the NSA's upstream collection devices.[507] There are reasons to suppose that this occurs rarely, but presently no one knows how many wholly domestic communications the NSA may be acquiring each year as a result of "about" collection.[508]

The more fundamental concern raised by "about" collection is that it permits the government to acquire communications exclusively between people about whom the government had no prior suspicion, or even knowledge of their existence, based entirely on what is contained within the contents of their communications.[509] This practice fundamentally differs from "incidental" collection, discussed above. While incidental collection also permits the government to acquire communications of people about whom it may have had no prior knowledge, that is an inevitable result of the fact that conversations generally involve at least two people: acquiring a target's communications by definition involves acquiring his communications with other people. But no effort is made to acquire those other peoples' communications — the government simply is acquiring the target's communications. In "about" collection, by contrast, the NSA's

---

506 December 2011 Joint Statement, *supra*, at 7 (acknowledging that the NSA's efforts "are not perfect").

507 *See generally* Bates October 2011 Opinion, *supra*, at 34, 2011 WL 10945618, at *11.

508 Although the NSA conducted a study in 2011, at the behest of the FISA court, to estimate how many wholly domestic communications it was annually acquiring as a result of collecting "MCTs" (discussed below), the study did not focus on how many domestic communications the NSA may be acquiring due to "about" collection where the communication acquired was not an MCT but rather a single, discrete communication. Bates October 2011 Opinion, *supra*, at 34 n.32, 2011 WL 10945618, at *11, n.32. At the urging of the FISA court, the NSA subsequently spent some time examining this question, but ultimately did not provide an estimate, instead explaining to the court the logistical reasons that the chance of acquiring domestic communications in "about" collection "should be smaller — and certainly no greater — than potentially encountering wholly domestic communications within MCTs." *Id*. This statement prompted the FISA court to adopt the assumption that the percentage of wholly domestic communications within the agency's "about" collection might equal the percentage of wholly domestic communications within its collection of "MCTs," leading to an estimate of as many as 46,000 wholly domestic "about" communications acquired each year. *Id*. We do not view this as a particularly valid estimate, because there is no reason to suppose that the number of wholly domestic "about" communications matches the number of wholly domestic MCTs, but the fact remains that the NSA cannot say how many domestic "about" communications it may be obtaining each year.

509 *See* December 2011 Joint Statement, *supra*, at 7 ("[U]pstream collection allows NSA to acquire, among other things, communications about a target where the target is not itself a communicant."); The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 4 ("Upstream collection . . . lets NSA collect electronic communications that contain the targeted e-mail address in the body of a communication between two third parties.").

collection devices can acquire communications to which the target is not a participant, based at times on their contents.[510]

Nothing comparable is permitted as a legal matter or possible as a practical matter with respect to analogous but more traditional forms of communication. From a legal standpoint, under the Fourth Amendment the government may not, without a warrant, open and read letters sent through the mail in order to acquire those that contain particular information.[511] Likewise, the government cannot listen to telephone conversations, without probable cause about one of the callers or about the telephone, in order to keep recordings of those conversations that contain particular content.[512] And without the ability to engage in inspection of this sort, nothing akin to "about" collection could feasibly occur with respect to such traditional forms of communication. Digital communications like email, however, enable one, as a technological matter, to examine the contents of all transmissions passing through collection devices and acquire those, for instance, that contain a tasked selector anywhere within them.

The government values "about" communications for the unique intelligence benefits that they can provide. Although we cannot discuss the details in an unclassified public report, the moniker "about" collection describes a number of distinct scenarios, which the government has in the past characterized as different "categories" of "about" collection. These categories are not predetermined limits that confine what the government acquires; rather, they are merely ways of describing the different forms of communications that are neither to nor from a tasked selector but nevertheless are collected because they contain the selector somewhere within them.[513] In some instances, the targeted person actually is a participant to the communication (using a different communications selector than the one that was "tasked" for collection), and so the term "about" collection may be misleading.[514] In other instances, a communication may not involve the targeted person, but for various logistical and technological reasons it will almost never involve a person located in the United States.

---

510 *See* December 2011 Joint Statement, *supra*, at 7.

511 *See United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *Ex parte Jackson*, 96 U.S. 727, 733 (1877).

512 *See Katz v. United States*, 389 U.S. 347 (1967).

513 Such communications include "any Internet transaction that references a targeted selector, regardless of whether the transaction falls within one of the . . . previously identified categories of 'about communications[.]'" Bates October 2011 Opinion, *supra*, at 31, 2011 WL 10945618, at *11.

514 The term *"about" communications* was originally devised to describe communications that were "about" the selectors of targeted persons — meaning communications that contained such a selector within the communication. But the term has been used more loosely by officials in a way that suggests these communications are "about" the targeted persons. References to targeted *persons* do not themselves lead to "about" collection; only references to the communications *selectors* of targeted persons lead to "about" collection.

Some forms of "about" collection, however, do potentially intrude on the privacy of U.S. persons and people in the United States, as when, for instance, a U.S. person sends or receives an international communication to or from a non-target that contains a tasked email address in the body of the communication. Because selectors that are designated for collection under Section 702 need not be affiliated with any nefarious activity themselves, as explained earlier, a U.S. person's use of a tasked selector in a communication does not necessarily indicate that the person is assisting a foreign power or engaged in any wrongdoing. Furthermore, that person's communication will have been acquired because the government's collection devices examined the *contents* of the communication, without the government having held any prior suspicion regarding that communication.

As noted above, however, all upstream collection — of which "about" collection is a subset — is "selector-based, i.e., based on . . . things like phone numbers or emails."[515] Just as in PRISM collection, a selector used as a basis for upstream collection "is not a 'keyword' or particular term (e.g., 'nuclear' or 'bomb') but must be a specific communications identifier (e.g., email address)."[516] In other words, the government's collection devices are not searching for references to particular topics or ideas, but only for references to specific communications selectors used by people who have been targeted under Section 702.

Moreover, the NSA's acquisition of "about" communications is, to a large degree, an inevitable byproduct of its efforts to comprehensively acquire communications that are to or from its targets. Because of the specific manner in which the NSA conducts upstream collection, and the limits of its current technology, the NSA cannot completely eliminate "about" communications from its collection without also eliminating a significant portion of the "to/from" communications it seeks. Only to a limited degree could the agency feasibly turn off its "about" collection without incurring this result, and the outcome would not only represent an incomplete solution but would also undermine confidence that communications to and from targets are being reliably acquired. Additionally, there is no way at present for the NSA to selectively choose among the different categories of "about" communications at the collection stage. Nor does the NSA currently have any means available to automatically segregate "about" communications from "to/from" communications after collection, or to segregate among different forms of "about" communications after collection. Thus, ending all "about" collection would require ending even those forms of "about" collection that the Board regards as appropriate and valuable, and that have very little chance of impacting the privacy of people in the United States.

---

515 PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA); *see id*. ("This is not collection based on key words, for example."); *id*. at 57 ("Abouts is a type of collection of information. . . . [A]ll collection of information is . . . focused on selectors, not key words . . . like terrorist, or like a generic name or things along those lines. . . . 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.").

516 NSA DCLPO REPORT, *supra*, at 4.

For now, therefore, "about" collection is an inextricable part of the NSA's upstream collection, which we agree has unique value overall that militates against eliminating it entirely. As a result, any policy debate about whether "about" collection should be eliminated in whole or in part may be, to some degree, a fruitless exercise under present conditions. From our perspective, given a choice between the status quo and crippling upstream collection as a whole, we believe the status quo is reasonable. As explained later, however, because of the serious and novel questions raised by "about" collection as a constitutional and policy matter, we recommend that the NSA develop technology that would allow it to selectively limit or segregate certain forms of "about" communications — so that a debate can be had in which the national security benefits of the different forms of "about" collection are weighed against their respective privacy implications.

We emphasize, however, that our acceptance of "about" collection rests on the considerations described above — the inextricability of the practice from a broader form of collection that has unique value, and the limited nature of what "about" collection presently consists of: the acquisition of Internet communications that include the communications identifier of a targeted person. Although those identifiers may sometimes be found in the body of a communication, the government is not making any effort to obtain communications based on the ideas expressed therein. We are not condoning expanding "about" collection to encompass names or key words, nor to its use in PRISM collection, where it is not similarly inevitable. Finally, our unwillingness to call for the end of "about" collection is also influenced by the constraints that presently govern the use of such communications after acquisition. As with all upstream collection, "about" communications have a default retention period of two years instead of five, are not routed to the CIA or FBI, and may not be queried using U.S. person identifiers.

4. Multi-Communication Transactions ("MCTs")

The technical means used to conduct the NSA's upstream collection result in another issue with privacy implications. Because of the manner in which the agency intercepts communications directly from the Internet "backbone," the NSA sometimes acquires communications that are not themselves authorized for collection (because they are not to, from, or "about" a tasked selector) in the process of acquiring a communication that *is* authorized for collection (because it is to, from, or "about" a tasked selector). In 2011, the FISA court held that the NSA's procedures for addressing this problem were inadequate, and that without adequate procedures this aspect of the NSA's collection practices violated the Fourth Amendment. The government subsequently altered its procedures to the satisfaction of the FISA court. Based on the Board's assessment of how those procedures are being implemented today, the Board agrees that existing practices strike a reasonable balance between national security and privacy.

Unlike in PRISM collection, where the government receives communications from the Internet service providers who facilitate them, in upstream collection the NSA obtains what it calls "transactions" that are sent across the backbone of the Internet. Communications travel across the Internet in the form of data packets: a single email, for instance, can be broken up into a number of data packets that take different routes to their common destination, where they are reassembled to reconstruct the email. A complement of data packets, in NSA parlance, is a "transaction."[517] These transactions will sometimes contain only a single, discrete communication, like a single email. At times, however, these transactions will contain a number of different individual communications. The NSA refers to the latter as an MCT.

An MCT is acquired by the NSA only if at least one individual communication within it meets the criteria for collection. That is, at least one of these individual communications must be to or from a tasked selector or contain reference to a tasked selector. But the MCT might also contain other individual communications that do not meet these criteria and that have no direct relationship to the tasked selector.[518] The NSA's collection devices are unable to distinguish, before the point of acquisition, whether or not a transaction is an MCT. Thus, in the process of intercepting a communication that is "to/from" or "about" a tasked selector, the NSA might simultaneously obtain communications that are neither, because they are embedded within an MCT that contains a different communication meeting the standards for collection.[519] These other communications might be to or from U.S. persons or people located in the United States. They also might be domestic communications, *exclusively* between people located in the United States.

When the FISA court first began approving the Section 702 program in 2008, it did not understand that the NSA's upstream process acquired "transactions" or that the agency was acquiring MCTs that included communications, including wholly domestic communications, that were not themselves authorized for collection. Only in 2011, after the government submitted a clarifying letter to the FISA court, did these aspects of upstream collection become clear to the court.[520] After extensive briefing, a hearing, and the

---

517 "The government describes an Internet 'transaction' as '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.'" Bates October 2011 Opinion, *supra*, at 28 n.23, 2011 WL 10945618, at *9 n.23.

518 *See* December 2011 Joint Statement, *supra*, at 7.

519 "About" collection and "MCT" collection are separate but overlapping categories. An MCT can be acquired if one of the communications within it is "about" a tasked selector (i.e., contains reference to a tasked selector), but an MCT also can be acquired if one of the communications within it is to or from a tasked selector. Thus, while "about" collection and "MCT" collection are both unique results of the upstream collection process, there is no inherent relationship between the two.

520 Bates October 2011 Opinion, *supra,* at 27-28, 30, 2011 WL 10945618, at *2, *9-11.

implementation of a study to estimate how many purely domestic communications were being acquired, the FISA court concluded that the NSA's practices were inconsistent with the Fourth Amendment and with the statutory requirement to minimize the retention of information about U.S. persons consistent with foreign intelligence needs. The FISA court accepted that the continued acquisition of MCTs was legitimate, but that the procedures in place to handle them after collection did not adequately protect the privacy interests of U.S. persons whose communications were acquired solely because they were contained within an MCT that also included a communication involving a tasked selector.

The government later resolved this issue to the FISA court's satisfaction by implementing new procedures for handling MCTs. Most notably, the NSA implemented procedures to segregate and restrict access to certain MCTs after collection, and established that any MCT found to contain a wholly domestic communication must be destroyed upon recognition. It also shortened the default retention period for communications acquired through upstream collection to two years.[521] These rules are now embodied in the NSA's minimization procedures. To address concerns about collection that occurred before these new procedures were implemented, the NSA later decided to purge all data in its repositories that it could identify as having been acquired through upstream before the date of these new procedures.[522]

The Board has inquired into how the NSA's new procedures for handling MCTs are being implemented, and it has learned — at a level of operational detail greater than what is reflected in the agency's minimization procedures — about the precise manner in which the segregation of MCTs occurs and the steps through which any use of a communication found in an MCT is permitted to occur. Based on this information, the Board believes that current practices adequately guard against the government's use of wholly domestic communications as well as other communications of U.S. persons that are not to, from, or about a tasked selector. Given the present impossibility of identifying, before collection, those MCTs that contain domestic communications or other U.S. persons' communications that are not themselves authorized for acquisition, we believe that the existing procedures strike a reasonable balance between national security and privacy. But we echo the FISA court's observation that it is incumbent upon the NSA to continue working to enhance its capability to limit its acquisitions to only targeted communications.[523]

---

521 *See* Memorandum Opinion at 7-11, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10947772, at *3-5 (FISA Ct. Nov. 30, 2011), *available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

522 *See* Memorandum Opinion at 30, [*Caption Redacted*], [Docket No. Redacted], 2012 WL 9189263, at *3 (FISA Ct. Sept. 25, 2012), *available at* http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf.

523 *See* Bates October 2011 Opinion, *supra,* at 58 n.54, 2011 WL 10945618, at *20 n.54.

C. Retention, Use, and Dissemination of U.S. Persons' Communications under Section 702

Examining the privacy implications of the Section 702 program cannot end with a discussion of what is collected, but also must consider how information about U.S. persons is treated after collection: how long it is kept, who has access to it, in what ways it may be analyzed, under what circumstances it may be disseminated, and what procedures and oversight mechanisms are in place to ensure compliance with applicable rules.[524]

Once communications are acquired under Section 702, they go into one or more databases at the NSA, CIA, and FBI.[525] At each agency, access to this Section 702 data is limited to those analysts or agents who have received training and guidance. In reviewing information contained in these databases, government personnel may come across communications involving U.S. persons. Data is frequently reviewed through queries, which identify communications that have particular characteristics specified in the query, such as containing a particular name or having been sent to or from a particular email address.[526]

Beginning first with inadvertent collection, if it is discovered that a Section 702 target is a U.S. person or was inside the United States at the time of targeting, the government must stop the collection immediately and generally must destroy any communications already acquired.[527] While the imperative to stop collection is absolute, each agency is permitted, in limited circumstances, to waive the general requirement that communications already collected must be destroyed. At the NSA, for instance, the Director or Acting Director may waive the destruction requirement, on a communication-by-

---

524 Everything that is collected under Section 702 is treated as a "communication" and therefore is protected by the applicable minimization procedures.

525 The CIA and FBI each receive only a select portion of the communications acquired under Section 702, and they receive only Internet communications acquired through PRISM collection, not telephone calls or Internet communications acquired through upstream collection. The National Counterterrorism Center ("NCTC") is not authorized to receive any unminimized Section 702 data, but instead has access to certain FBI systems containing minimized Section 702 data. The CIA holds all unminimized communications acquired through Section 702 in a standalone network that is separate from the CIA's other information processing systems.

526 Because "about" and "MCT" collection occur only in upstream collection, which NSA alone receives, FBI and CIA personnel have no access to such communications.

527 *See, e.g.*, 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, § 3(d)(2), 5 (Oct. 31, 2011) ("NSA 2011 Minimization Procedures"), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf. If the government learns that a target who previously was outside the United States has traveled into the United States, it also must stop collection immediately, and it must generally destroy those communications that were acquired after the target entered the United States, subject to the possibility of a waiver discussed above. *Id*. § 3(d).

communication basis, by determining in writing that the communication satisfies one of several criteria. The destruction requirement may be waived if the communication is reasonably believed to contain "significant foreign intelligence information," evidence of a crime, "technical data base information," or "information necessary to understand or assess a communications security vulnerability." Communications that indicate "a threat of serious harm to life or property" may also be preserved from destruction.[528] The FBI standards are similar, as are the CIA standards, except that CIA waivers are limited to communications containing significant foreign intelligence or evidence of a crime.

Although approval for these waivers must come from the highest levels of the agencies, the breadth of the circumstances in which they can be approved raises concern that the waiver provisions might permit excessive use of communications that the agencies never should have acquired. Allowing the government to exploit the fruits of mistaken targeting decisions may risk creating an incentive for lax adherence to targeting restrictions. Presently, however, it appears that the government has been invoking these waiver provisions in a restrained manner. In 2013, for instance, the NSA Director waived the destruction of approximately forty communications (none of which was a wholly domestic communication), involving eight targets, based on a finding that each communication contained significant foreign intelligence information. Neither the CIA nor FBI utilized their waiver provisions in 2013. Along with the rigor that we believe is applied to the government's determinations of foreignness during targeting, this sparing use of waivers helps to allay concern about their abuse. Furthermore, when an erroneous targeting was the result of a compliance incident, such as mistyping an email address, as opposed to a reasonable but mistaken belief about a target's status, the waiver provision is unavailable.

Apart from communications acquired inadvertently, U.S. persons' communications are not typically purged or eliminated from the government's Section 702 databases before the end of their default retention periods, even when the communications pertain to matters unrelated to foreign intelligence or crime. This is because the agencies do not scrutinize each communication that they acquire or attempt to identify those that are to or from a U.S. person or person in the United States. The NSA's minimization procedures, for instance, require the destruction of irrelevant communications of or concerning U.S. persons, but analysts are required to make such determinations only "at the earliest practicable point in the processing cycle," and only where the communication can be identified as "clearly" not relevant to the purpose under which it was acquired or containing evidence of a crime.[529] In practice, however, this destruction rarely happens. NSA analysts do not review all or even most communications acquired under Section 702

528 NSA 2011 Minimization Procedures, *supra*, § 5.

529 NSA 2011 Minimization Procedures, *supra*, § 3(b)(1).

as they arrive at the agency. Instead, those communications often remain in the agency's databases unreviewed until they are retrieved in response to a database query, or until they are deleted upon expiration of their retention period, without ever having been reviewed. Even when an analyst focuses on a particular communication, the destruction requirement is triggered only when analysts can affirm a negative: that the communication in question does *not* contain foreign intelligence or evidence of a crime.[530] But communications that appear innocuous at first may later take on deeper significance as more contextual information is learned, and it can be difficult for one analyst to be certain that a communication has no intelligence value to any other analyst. As a matter of course, therefore, there is no routine deletion from the NSA's Section 702 databases of information that involves U.S. persons but is not pertinent to the agency's foreign intelligence mission. Therefore, although a communication must be "destroyed upon recognition" when an NSA analyst recognizes that it involves a U.S. person and determines that it clearly is not relevant to foreign intelligence or evidence of a crime,[531] in reality this rarely happens. Nor does such purging occur at the FBI or CIA: although their minimization procedures contain age-off requirements, those procedures do not require the purging of communications upon recognition that they involve U.S. persons but contain no foreign intelligence information.

Information that remains in the government's Section 702 databases may be queried to find the communications of specific U.S. persons under certain circumstances.[532] Queries are a key mechanism through which analysts access Section 702 information in the government's databases.[533] They may involve "telephone numbers, key words or phrases, or other discriminators" as selection terms.[534] Queries can be used to search both the content of communications and the addressing information, or "metadata," associated with the communications. At the NSA, content queries based on identifiers associated with specific U.S. persons — such as a name or email address — can be performed if they are "reasonably likely to return foreign intelligence information."[535] No showing or suspicion is required that the U.S. person is engaged in any form of wrongdoing. In recent months, NSA analysts have performed queries using U.S. person identifiers to find information

---

530 NSA 2011 Minimization Procedures, *supra*, § 3(c). In addition, the communication must be "known" to contain information of or concerning U.S. persons. *Id*.

531 NSA 2011 Minimization Procedures, *supra*, § 3(b)(1), (c)(1).

532 The NSA and CIA first obtained approval to conduct queries using U.S. person identifiers in 2011. *See* Bates October 2011 Opinion, *supra*.

533 *See, e.g.*, NSA DCLPO REPORT, *supra*, at 6 ("[Analysts] access the information via 'queries,' which may be date-bound, and include alphanumeric strings such as telephone numbers, email addresses, or terms that can be used individually or in combination with one another.").

534 *See, e.g.*, NSA 2011 Minimization Procedures, *supra*, § 3(b)(6).

535 NSA 2011 Minimization Procedures, *supra*, § 3(b)(6); *see* NSA DCLPO REPORT, *supra*, at 7.

concerning, among other things, "individuals believed to be involved in international terrorism." The CIA and FBI standards for content queries are essentially the same, except that the FBI, given its law enforcement role, is permitted to conduct queries to seek evidence of a crime as well as foreign intelligence information.

At the NSA, prior approval must be obtained to use content query terms that involve U.S. person identifiers. The agency records each term that is approved, though not the number of times any particular term is actually used to query a database. The NSA performs checks of its analysts' queries. Prior approval is not required at the CIA; instead, the agency has developed audit capability. This system requires CIA personnel using U.S. person identifiers as query terms (or any other query term intended to return information about a particular U.S. person) write a contemporaneous foreign intelligence justification, which is documented along with a record of the query. Review of queries is also provided by the DOJ/ODNI oversight team, which reviews every U.S. person term approved for querying at the NSA as well as every U.S. person query performed at the CIA, reporting their numbers and any compliance issues to congressional oversight committees.

In 2013, the NSA approved the use of 198 terms involving U.S. person identifiers to perform content queries of its Section 702–acquired communications. During the same year, the CIA conducted approximately 1,900 queries of its unminimized Section 702–acquired communications, of which approximately forty percent were at the request of other U.S. intelligence agencies.[536] Outside of those queries conducted on behalf of other intelligence agencies, CIA queries might involve, for instance, U.S. persons located overseas that intelligence indicates may be engaged in planning terrorist attacks or otherwise facilitating international terrorism.

While the FBI maintains records of content queries used to search its Section 702 data, it does not separately designate those that employ U.S. person identifiers, and so the number of U.S. person queries performed by the FBI is not known.

At the NSA, metadata queries, like content queries, must be reasonably designed to return foreign intelligence information when they involve U.S. person identifiers. Prior approval is not required, but the analyst must supply a written justification for the query, and all queries are recorded and subject to audit.[537] The DOJ/ODNI oversight team reviews every NSA metadata query that involves a U.S. person identifier. In 2013, NSA analysts

---

536 Approximately 27 percent of these queries were duplicative of previous queries that employed the same query terms.

537 NSA DCLPO REPORT, *supra*, at 7.

performed approximately 9,500 queries of metadata acquired under Section 702 using U.S. person identifiers.[538]

The CIA also has the capability to conduct metadata-only queries against metadata derived from Section 702 collection. However, the CIA does not track how many metadata-only queries using U.S. person identifiers have been conducted. The CIA's minimization procedures do not contain any specific standard with respect to metadata queries involving U.S. person identifiers, although such queries are regulated under internal CIA regulations that govern queries of FISA and non-FISA information, and FISA itself requires that information collected be used only be for lawful purposes.[539] The FBI requires that metadata queries, like content queries, be reasonably designed to return foreign intelligence or evidence of a crime. As noted above, however, the FBI does not separately track which of its queries involve U.S. person identifiers, and so the number of such metadata queries is not known.

As illustrated above, rules and oversight mechanisms are in place to prevent U.S. person queries from being abused for reasons other than searching for foreign intelligence or, in the FBI's case, for evidence of a crime. In pursuit of the agencies' legitimate missions, however, government analysts may use queries to digitally compile the entire body of communications that have been incidentally collected under Section 702 that involve a particular U.S. person's email address, telephone number, or other identifier, with the exception that Internet communications acquired through upstream collection may not be queried using U.S. person identifiers.[540] In addition, the manner in which the FBI is employing U.S. person queries, while subject to genuine efforts at executive branch oversight, is difficult to evaluate, as is the CIA's use of metadata queries.

If the NSA, CIA, or FBI wishes to permanently retain a communication of or concerning a U.S. person (beyond the default retention periods), personnel must make a determination that retention is justified under certain criteria established in their minimization procedures. Those criteria demand a legitimate governmental interest in the communication, but are fairly broad with respect to the types of needs and purposes that justify retention. The NSA, for instance, permits retention if the identity of the U.S. person "is necessary to understand foreign intelligence information or asses its importance," or if

538 According to the DOJ/ODNI oversight team, the NSA's counting of its own metadata queries typically is overinclusive, often counting queries that do not actually include a U.S. person identifier as well as other queries where it is unclear whether a U.S. person identifier is involved.

539 *See* 50 U.S.C. §§ 1806(a).

540 *See* NSA 2011 Minimization Procedures, *supra*, § 3(b)(6).

the communication contains evidence of a crime, among other reasons.[541] The CIA's and FBI's rules are comparable.

Agencies that receive Section 702 communications may disseminate to another agency foreign intelligence information of or concerning a U.S. person, or evidence of a crime concerning a U.S. person, that was acquired from those communications. This is done most frequently by the NSA, reflecting the nature of its mission. When making such disseminations, NSA personnel typically "mask" the information about that U.S. person that could be used to identify him or her — replacing a proper name with, for instance, "a U.S. person" — but they may "unmask" such information upon request (with supervisory approval) when the requesting agency is deemed to legitimately require the information for its mission.[542] The number of disseminated reports containing references to U.S. person identifiers are reported annually to congressional oversight committees. As with U.S. person queries, these rules guard against the unjustified use of information about U.S. persons for illegitimate ends, but they do not significantly restrict the use of such information for legitimate intelligence and law enforcement aims.[543]

In 2013, the vast majority of the intelligence reports disseminated by the NSA that were based on intelligence derived from Section 702 contained no reference to any U.S. person. A significant number of such reports, however (albeit a small percentage of the total), did include references to U.S. persons. As noted, U.S. person information in these reports typically is initially "masked" to hide personally identifying information.

In response to requests from recipients of those reports (primarily intelligence and law enforcement agencies), last year the NSA "unmasked" approximately 10,000 U.S. person identities where the information was not included in the original reporting.[544]

Apart from this intelligence reporting, the NSA is permitted to pass on information showing possible violations of the law to the DOJ and the FBI. In 2013, the agency passed on such information only ten times.

---

541 NSA 2011 Minimization Procedures, *supra*, § 6(a), (b)(2).

542 NSA DCLPO REPORT, *supra*, at 7-8; NSA 2011 Minimization Procedures, *supra*, § 6(b).]

543 Under similar rules and additional internal restrictions, the NSA may share communications involving U.S. persons with foreign governments. NSA 2011 Minimization Procedures, *supra*, § 8(a). The NSA also is permitted to use and disseminate U.S. persons' privileged attorney-client communications, subject to approval from its Office of General Counsel, as long as the person is not known to be under criminal indictment in the United States and communicating with an attorney about that matter. *Id*. § 4. The CIA and FBI minimization procedures contain comparable provisions.

544 According to the NSA, fewer than a quarter of these identifiers were proper names of individuals or their titles; the remainder were U.S. corporation names, U.S. educational institution names, U.S.-registered IP addresses, websites hosted in the United States, email addresses or telephone numbers potentially used by U.S. persons, and other identifiers potentially used by U.S. persons.

In the Board's view, the protections contained in the agencies' minimization procedures are reasonably designed and implemented to ward against exploitation of information acquired under Section 702 for illegitimate purposes. The Board has seen no trace of any such illegitimate activity associated with the program, or any attempt to intentionally circumvent legal limits.

Depending on the scope of collection, however, the applicable rules may allow a substantial amount of private information about U.S. persons to be acquired by the government, examined by its personnel, and used in ways that may have a negative impact on those persons. Although it is not known how many communications involving U.S. persons or people in the United States are acquired under Section 702, the limited figures available may provide some indication of the extent to which the government presently could be using such communications. Some of these figures illustrate that the Section 702 program remains primarily focused on monitoring non-U.S. persons located outside the United States. By the same token, the overall scope of collection under the program and the quantity of intelligence reporting derived from this collection involving U.S. persons suggest that the government may be gathering and utilizing a significant amount of information about U.S. persons under Section 702.

If so, this would raise legitimate concern about whether a collection program that is premised on targeting foreigners located outside the United States without individual judicial orders now acquires substantial information about U.S. persons without the safeguards of individualized court review. Emphasizing again that we have seen no indication of abuse, nor any sign that the government has taken lightly its obligations to establish and adhere to a detailed set of rules governing the program, the collection and examination of U.S. persons' communications represents a privacy intrusion even in the absence of misuse for improper ends. The Board's desire to provide more clarity and transparency regarding the government's activities under Section 702, particularly insofar as they involve the acquisition and handling of U.S. persons' communications, underlies a number of our recommendations.

Part 6:

RECOMMENDATIONS

The Board has conducted an in-depth study of the Section 702 program. We have carefully considered whether the program as implemented complies with the statute and is consistent with constitutional requirements. The Board has also evaluated whether the program strikes the right balance between national security and privacy and civil liberties as a policy matter. The Board recognizes the considerable value that the Section 702 program provides in the government's efforts to combat terrorism and gather foreign intelligence, and finds that at its core, the program is sound. However, some features outside of the program's core, particularly those impacting U.S. persons, raise questions regarding the reasonableness of the program. The Board therefore offers a series of policy recommendations to ensure that the program includes adequate and appropriate safeguards for privacy and civil liberties.

The Board has identified five key areas where operations of the Section 702 program could strike a better balance between privacy, civil rights, and national security. They include the manner in which targeting and tasking is implemented, the manner in which queries using U.S. person identifiers are conducted, and the Foreign Intelligence Surveillance Court's ("FISC" or "FISA court") role in the certification process. Additional areas for improvement include the government's collection of upstream Internet transactions, transparency in the operations of the Section 702 program. We also make a recommendation, not limited only to Section 702, about evaluation of the efficacy of government surveillance programs. Based on our independent review and the conclusions we have drawn, the Board offers the following recommendations.

I. Targeting and Tasking

Recommendation 1: ***The NSA's targeting procedures should be revised to (a) specify criteria for determining the expected foreign intelligence value of a particular target, and (b) require a written explanation of the basis for that determination sufficient to demonstrate that the targeting of each selector is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. The NSA should implement these revised targeting procedures through revised guidance and training for analysts, specifying the criteria for the foreign intelligence determination and the kind of written explanation needed to support it. We expect that the FISA***

court's review of these targeting procedures in the course of the court's periodic review of Section 702 certifications will include an assessment of whether the revised procedures provide adequate guidance to ensure that targeting decisions are reasonably designed to acquire foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court. Upon revision of the NSA's targeting procedures, internal agency reviews, as well as compliance audits performed by the ODNI and DOJ, should include an assessment of compliance with the foreign intelligence purpose requirement comparable to the review currently conducted of compliance with the requirement that targets are reasonably believed to be non-U.S. persons located outside the United States.

In order to target a person under Section 702, two basic criteria must be satisfied: the person must be a non-U.S. person located outside the United States (the "foreignness determination") and the surveillance must be conducted to collect foreign intelligence information (the "foreign intelligence purpose determination").

The Board's review of the Section 702 program showed that the procedures for documenting targeting decisions within the NSA, and the procedures for reviewing those decisions within the executive branch, focus primarily on the foreignness determination — — establishing that a potential target is a non-U.S. person reasonably believed to be located abroad. The process for documenting and reviewing the foreign intelligence purpose of a targeting is not as rigorous. Agency personnel have not been required to articulate or explain these determinations in any detail as a matter of course, and typically indicate what category of foreign intelligence information they expect to obtain from targeting a particular person in a single brief sentence that contains only minimal information about why the analyst believes that targeting this person will yield foreign intelligence information. As a result, the Section 702 oversight team from the DOJ and the ODNI cannot scrutinize these foreign intelligence purpose determinations with the same rigor that it scrutinizes foreignness determinations. In contrast, NSA analysts are required to articulate a rationale to a much greater degree regarding their foreignness determinations, and oversight is accordingly more in-depth.

The Board recognizes that this distinction stems from the different treatment of the foreignness and foreign intelligence purpose determinations in Section 702 itself. Section 702(d), the subsection of the statute outlining the requirements for targeting procedures, specifically requires that the procedures be reasonably designed to ensure that targeting is limited to persons reasonably believed to be located outside the United States, but there is no comparable requirement in this subsection specifying that targeting procedures must be reasonably designed to ensure that targeting has a valid foreign intelligence purpose. Likewise, when the FISA court assesses whether the government's targeting procedures

comply with statutory requirements, the court is directed by Section 702(i), to consider the adequacy of those procedures with respect to the foreignness determination, but there is no comparable provision specifically requiring a review of the foreign intelligence purpose determination.

Despite the fact that the statute treats these two determinations differently, it also demands that *all* targeting be intended "to acquire foreign intelligence information." Thus, the foreign intelligence purpose determination is a critical part of the statutory framework. From a constitutional perspective, moreover, at least insofar as Section 702 surveillance incidentally collects communications to and from U.S. persons, the foreign intelligence purpose is what provides the basis for the government to conduct Section 702 surveillance without a warrant. As a result, we conclude that there should be something closer to parity between the foreignness determination and foreign intelligence purpose determination in terms of what level of explanation is required of an analyst and how rigorous the oversight of that explanation is.

Therefore, the Board recommends that the NSA's targeting procedures be updated to require a more detailed written explanation of the foreign intelligence purpose of each targeting decision and to specify the criteria that would be sufficient to demonstrate that this standard has been met. Changes to the targeting procedures that provide more guidance to analysts and require more explanation regarding the foreign intelligence purpose of a targeting will help analysts better articulate this element of their targeting decisions. When analysts articulate at greater length the bases for their targeting decisions, the executive branch oversight team that later reviews those decisions will be better equipped to meaningfully review them.

The Board does not believe that a statutory change is needed to implement this recommendation. The government already has the authority to amend its targeting procedures, subject to FISA court approval. We believe that it would be helpful for the FISA court, when reviewing Section 702 certifications, to assess whether the government's targeting procedures are reasonably designed to ensure that targeting is limited to persons of foreign intelligence value, much like the court now assesses whether targeting procedures are reasonably designed to ensure that targeting is limited to persons located outside the United States. We believe that, without statutory change, the government could request that the FISA court assume this additional task, as the FISA court already must and does consider how fully the Section 702 program is geared toward acquiring foreign intelligence, in order to ensure that the program is authorized by the statute and consistent with the Fourth Amendment.

Once the revised targeting procedures are in place, analysts should be trained on their implementation, to ensure that the analysts are appropriately articulating the rationale for foreign intelligence purpose determinations. The NSA should also modify its

internal agency reviews to ensure that the new targeting procedures have been adopted by its analysts. The executive branch compliance audits should also be modified to reflect the new targeting procedures and to include more rigorous scrutiny of whether valid foreign intelligence purpose determinations are being properly articulated.

II. U.S. Person Queries

Recommendation 2: The FBI's minimization procedures should be updated to more clearly reflect actual practice for conducting U.S. person queries, including the frequency with which Section 702 data may be searched when making routine queries as part of FBI assessments and investigations. Further, some additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non–foreign intelligence criminal matters.

When an FBI agent or analyst initiates a criminal assessment or begins a new criminal investigation related to any type of crime, it is routine practice, pursuant to the Attorney General Guidelines for Domestic FBI Operations, to conduct a query of FBI databases in order to determine whether they contain information on the subject of the assessment or investigation. The databases queried may include information collected under various FISA authorities, including data collected under Section 702. The FBI's rules relating to queries do not distinguish between U.S. persons and non-U.S. persons; as a domestic law enforcement agency, most of the FBI's work concerns U.S. persons. If a query leads to a "hit" in the FISA data (i.e., if a communication is found within a repository of Section 702 data that is responsive to the query), then the agent or analyst is alerted to the existence of the hit. If the agent or analyst has received training on how to handle FISA-acquired materials, he or she is able to view the Section 702 data that was responsive to the query; however, if the agent or analyst has not received FISA training he or she is merely alerted to the existence of the information but cannot access it. The agent or analyst would have to contact a FISA-trained agent or analyst and ask him or her to review the information.

Even though FBI analysts and agents who solely work on non–foreign intelligence crimes are not *required* to conduct queries of databases containing Section 702 data, they are *permitted* to conduct such queries and many do conduct such queries. This is not clearly expressed in the FBI's minimization procedures, and the minimization procedures should be modified to better reflect this actual practice. The Board believes that it is important for accountability and transparency that the minimization procedures provide a clear representation of operational practices. Among other benefits, this improved clarity will better enable the FISA court to assess statutory and constitutional compliance when

the minimization procedures are presented to the court for approval with the government's next recertification application.

In light of the privacy and civil liberties implications of using Section 702 information, collected under lower thresholds and for a foreign intelligence purpose, in the FBI's pursuit of non–foreign intelligence crimes, the Board believes it is appropriate to place some additional limits on what can be done with Section 702 information. Members of the Board differ on the nature of the limitations that should be placed on the use of that information. Board Members' proposals and a brief explanation of the reasoning supporting each are stated below, with elaboration in the two separate statements.

Additional Comment of Chairman David Medine and Board Member Patricia Wald

For acquisitions authorized under Section 702, FISA permits the FBI for law enforcement purposes, to retain and disseminate evidence of a crime. However, there is a difference between obtaining a U.S. person's communications when they are in plain view as an analyst reviews the target's communications, and the retrieval of a U.S. person's communications by querying the FBI's Section 702 holdings collected over the course of years.[545] Therefore, consistent with our separate statement regarding Recommendation 3, we believe that U.S. persons' privacy interests regarding 702 data should be protected by requiring that each identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702, other than in exigent circumstances. The court should determine, based on documentation submitted by the government, whether the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return information relevant to an assessment or investigation of a crime. As discussed in more detail in our separate statement, this judicial review would not be necessary for U.S. persons who are already suspected terrorists and subject to surveillance under other government programs.

Additional Comment of Board Members Rachel Brand and Elisebeth Collins Cook

As explained in our separate statement, we would support a requirement that an analyst conducting a query in a non–foreign intelligence criminal matter obtain supervisory approval before accessing any Section 702 information that was responsive to the query. We would also support a requirement of higher-level Justice Department approval, to the extent not already required, before Section 702 information could be used

---

[545] On June 25, 2014, the United States Supreme Court ruled unanimously that a search of a cell phone seized by the police from an individual who has been arrested required a warrant. *Riley v. California*, No. 13-132, 2014 WL 2864483 (U.S. June 25, 2014). The Court distinguished between reviewing one record versus conducting an extensive records search over a long period: "The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years." *Id.* at *18. Likewise, observing evidence of a crime in one email does not justify conducting a search of an American's emails over the prior five years to or from everyone targeted under the Section 702 program.

in the investigation or prosecution of a non–foreign intelligence crime (such as in the application for a search warrant or wiretap, in the grand jury, or at trial). We would not require any additional approvals before an analyst could conduct a query of databases that include FISA data.

Additional Comment of Board Member James Dempsey

It is imperative not to re-erect the wall limiting discovery and use of information vital to the national security, and nothing in the Board's recommendations would do so. The constitutionality of the Section 702 program is based on the premise that there are limits on the retention, use and dissemination of the communications of U.S. persons collected under the program. The proper mix of limitations that would keep the program within constitutional bounds and acceptable to the American public may vary from agency to agency and under different circumstances. The discussion of queries and uses at the FBI in this Report is based on our understanding of current practices associated with the FBI's receipt and use of Section 702 data. The evolution of those practices may merit a different balancing. For now, the use or dissemination of Section 702 data by the FBI for non-national security matters is apparently largely, if not entirely, hypothetical. The possibility, however, should be addressed before the question arises in a moment of perceived urgency. Any number of possible structures would provide heightened protection of U.S. persons consistent with the imperative to discover and use critical national security information already in the hands of the government.[546]

Recommendation 3: The NSA and CIA minimization procedures should permit the agencies to query collected Section 702 data for foreign intelligence purposes using U.S. person identifiers only if the query is based upon a statement of facts showing that the query is reasonably likely to return foreign intelligence information as defined in FISA. The NSA and CIA should develop written guidance for agents and analysts as to what information and documentation is needed to meet this standard, including specific examples.

Under the NSA and CIA minimization procedures for the Section 702 program, analysts are permitted to perform queries of databases that hold communications acquired under Section 702 using query terms that involve U.S. person identifiers. Such queries are designed to identify communications in the database that involve or contain information relating to a U.S. person.

---

546 *See* Presidential Policy Directive — Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435, § 2, (Jan. 17, 2014) (limiting the use of signals intelligence collected in bulk to certain enumerated purposes), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

The internal processes employed by the two agencies with respect to U.S. person queries differ. Under the NSA's minimization procedures, all queries that involve U.S. person identifiers (whether they search content or metadata) must be constructed so as to be "reasonably likely to return foreign intelligence information." The NSA also requires analysts to provide written justifications for the use of all query terms that involve U.S. person identifiers. More specifically, with respect to querying the metadata of Section 702 communications (which includes, for instance, the email address from which a communication was sent), analysts must document the basis for queries that involve U.S. person identifiers, which are subject to audit. With respect to queries that scan the contents of Section 702 communications, analysts must obtain prior approval for any query term that involves a U.S. person identifier. (Subsequent uses of an already approved query term do not require new permission.)

Under the CIA's minimization procedures, personnel must document the foreign intelligence basis for queries of content queries that involve U.S. person identifiers, which are subject to audit, but need not document a justification or obtain prior approval for queries of metadata.

Although the Board recognizes that NSA and CIA queries are subject to rigorous oversight by the DOJ's National Security Division and the ODNI (with the exception of metadata queries at the CIA, which are not reviewed by the oversight team), we believe that NSA and CIA analysts, before conducting a query involving a U.S. person identifier, should provide a statement of facts illustrating why they believe the query is reasonably likely to return foreign intelligence information.[547] To assist in this process, the government should develop written guidance for the benefit of analysts who are authorized to perform such queries to clearly explain the meaning of the standard "reasonably likely to return foreign intelligence information." It should also provide illustrative examples of permissible and impermissible queries as well as proper and improper bases on which to conclude that a query is reasonably likely to return foreign intelligence. This guidance should reflect the fact that the statutory definition of "foreign intelligence information" under FISA is narrower when the information in question involves U.S. persons than it is when information pertains only to non-U.S. persons.

Implementing these measures will help to ensure that analysts at the NSA and CIA do not access or view communications acquired under Section 702 that involve or concern U.S. persons when there is no valid foreign intelligence reason to do so.

---

[547] Board Member Elisebeth Collins Cook would not extend a new requirement to this effect to metadata queries.

III. FISC Role

Recommendation 4: To assist in the FISA court's consideration of the government's periodic Section 702 certification applications, the government should submit with those applications a random sample of tasking sheets and a random sample of the NSA's and CIA's U.S. person query terms, with supporting documentation. The sample size and methodology should be approved by the FISA court.

The FISA court reviews the government's proposed targeting and minimization procedures each time the government seeks approval or re-approval of a certification, typically annually. To assist the FISA court in its review, the government should provide the court with a random sample of targeting decisions (reflected in "tasking" sheets) and a random sample of NSA and CIA query terms that involve U.S. person identifiers.[548] The FISC should approve the methodology used to select the samples and the size of those samples.

Providing a random sample of targeting decisions would allow the FISC to take a retrospective look at the targets selected over the course of a recent period of time. The data could help inform the FISA court's review process by providing some insight into whether the government is, in fact, satisfying the foreignness and foreign intelligence purpose requirements, and it could signal to the court that changes to the targeting procedures may be needed, or prompt inquiry into that question. The data could provide verification that the government's representations during the previous certification approval were accurate, and it could supply the FISC with more information to use in determining whether the government's acquisitions comply with the statute and the Fourth Amendment.

Similarly, a retrospective sample of U.S. person query terms and supporting documentation will allow the FISC to conduct a fuller review of the government's minimization procedures. Such a sample could allow greater insight into the methods by which information gathered under Section 702 is being utilized, and whether those methods are consistent with the minimization procedures. While U.S. person queries by the NSA and CIA are already subject to rigorous executive branch oversight (with the exception of metadata queries at CIA), supplying this additional information to the FISC could help guide the court by highlighting whether the minimization procedures are being followed and whether changes to those procedures are needed.

---

548 Chairman David Medine and Board Member Patricia Wald see no reason to exclude the FBI's query process from FISA court oversight. While it is correct that the FBI does not distinguish between queries using U.S. person identifiers and those that do not, as a domestic law enforcement agency it clearly conducts a significant number of queries using identifiers belonging to U.S. persons. Therefore, a sample of the queries performed by the FBI could inform the FISA court's review.

Recommendation 5: As part of the periodic certification process, the government should incorporate into its submission to the FISA court the rules for operation of the Section 702 program that have not already been included in certification orders by the FISA court, and that at present are contained in separate orders and opinions, affidavits, compliance and other letters, hearing transcripts, and mandatory reports filed by the government. To the extent that the FISA court agrees that these rules govern the operation of the Section 702 program, the FISA court should expressly incorporate them into its order approving Section 702 certifications.

The government's operation of the Section 702 program must adhere to the targeting and minimization procedures that are approved by the FISA court, as well as to the pertinent Attorney General guidelines and the statute itself. The government also makes additional representations to the FISA court through compliance notices and other filings, as well as during hearings, that together create a series of more rigorous precedents and a common understanding between the government and the court regarding the operation of the program. More than once, the government has implemented rules for the Section 702 program that are more detailed than what is reflected in the text of the targeting and minimization procedures themselves, although these rules typically are viewed as an interpretation of those procedures. These more detailed rules are not centrally located but are contained in compliance letters, affidavits, mandatory reports, hearing transcripts, and other sources that arise from the interaction between the government and the FISC. Such rules have precedential value and create real consequences, as the government considers itself bound to abide by the representations it makes to the FISA court. To the extent that the rules which have emerged from these representations and this interactive process govern the operation of the Section 702 program, they should be memorialized in a single place and incorporated into the FISC's certification review.

This recommendation is influenced by the Board's recognition that FISC judges and legal advisors do not serve on the court forever. As judges rotate out of FISC service, the risk that important information about the contours of the Section 702 program will be lost due to attrition, or not fully appreciated by new judges, greatly increases when the body of precedent that has developed over the course of the program's existence is not centrally located. Adopting this recommendation would ensure that each judge who may come to render decisions about the program will have ready access to a centralized source that encapsulates this body of precedent, to help inform his or her decisions and understanding of the program. This consolidation of rules will also facilitate congressional oversight of the Section 702 program. Accordingly, the Board views this recommendation as a measure to promote good government.

Additionally, incorporating the series of precedents described above into a comprehensive source will provide a single reference point for every government lawyer, agent, officer, and analyst within the Intelligence Community who has responsibilities under the Section 702 program. These precedents and rules, given their dispersed location within a range of different FISA court filings and documents, may not be readily accessible to the lawyers tasked with helping to implement the requirements specified in those documents or to the agents and analysts operating the program. A complete, readily accessible legal framework will assist lawyers and analysts throughout the government in their efforts to comply with the requirements of the Section 702 program.

IV. Upstream and "About" Collection

Recommendation 6: To build on current efforts to filter upstream communications to avoid collection of purely domestic communications, the NSA and DOJ, in consultation with affected telecommunications service providers, and as appropriate, with independent experts, should periodically assess whether filtering techniques applied in upstream collection utilize the best technology consistent with program needs to ensure government acquisition of only communications that are authorized for collection and prevent the inadvertent collection of domestic communications.

In PRISM collection, through which the government obtains communications directly from Internet service providers, the government acquires only those communications sent to or from selectors used by targeted persons. Obtaining only communications sent to and from those selectors helps ensure that no wholly domestic communications are acquired — because the targeted person who uses the selector always must be someone reasonably believed to be located outside the United States.

In upstream collection, by contrast, the NSA obtains communications directly from the Internet "backbone," with the compelled assistance of companies that maintain those networks, rather than Internet service providers that supply particular modes of communication. The success of this process depends on collection devices that can reliably acquire data packets associated with the proper communications. In addition, through "about" collection, the upstream process includes acquiring communications that contain reference to selectors used by targeted persons, even if the communication is not sent to or from the account of that selector. Because the targeted person may not be a party to the communication, it is possible that neither participant in the communication is located outside the United States, although the NSA takes additional measures, including the use of IP filters, to try to avoid collecting wholly domestic communications.

As a result, upstream collection involves a greater risk that the government will acquire wholly domestic communications, which it is not authorized to intentionally collect under Section 702. Ensuring that the upstream collection process comports with statutory limits and with agency targeting procedures involves an important technical process of filtering out wholly domestic communications. The government acknowledges, however, that the technical methods used to prevent the acquisition of domestic communications do not completely prevent them from being acquired. Even if domestic communications were to constitute a very small percentage of upstream collection, this could still result in a large overall number of purely domestic communications being collected. Mindful of these considerations, the Board believes that there should be an ongoing dialogue, both within the government and in cooperation with telecommunications providers or independent experts, to ensure that the means being used to filter for domestic communications use the best technology. We also believe that the determination about whether this is the case should be continually revisited.

Recommendation 7: The NSA periodically should review the types of communications acquired through "about" collection under Section 702, and study the extent to which it would be technically feasible to limit, as appropriate, the types of "about" collection.

In the upstream collection process, as in the PRISM collection process, the NSA acquires Internet communications sent to and from the selector, such as an email address, used by a targeted person. In upstream, however, the NSA also acquires Internet communications that are not sent to or from this email address, but instead contain reference to the selector, sometimes in the body of the communication. These are termed "about" communications, because they are not to or from, but rather "about" the communication selectors of targeted persons. In addition, for technical reasons, "about" collection is needed even to acquire some communications that actually are "to" or "from" a target.

A number of different scenarios result in a communication containing reference to a particular selector when the communication is not to or from that selector. Thus, there are a number of different categories or types of "about" communications acquired by the NSA. Some forms of "about" communications are actually the communications of targeted persons. Other types of "about" collection can result in the acquisition of communications between two non-targets, thereby implicating greater privacy concerns. For instance, when a person in the United States sends or receives an international communication that contains a targeted email address in the body of the communication, that communication may be acquired by the NSA, even if the sender and recipient are not targets themselves and were completely unknown to the government before its collection devices examined

the contents of their communication. Moreover, the permissible scope of targeting in the Section 702 program is broad enough that targets need not themselves be suspected terrorists or other bad actors. Thus, if the email address of a target appears in the body of a communication between two non-targets, it does not necessarily mean that either of the communicants is in touch with a suspected terrorist.

All of these types of "about" communications can provide intelligence value, helping the government learn more about terrorist networks and their plans or obtain other foreign intelligence. While "about" collection is valued by the government for its unique intelligence benefits, it is, to a large degree, an inevitable byproduct of the way the NSA conducts much of its upstream collection. As discussed earlier in this Report, because of the technical manner in which this collection is performed, the NSA cannot entirely stop acquiring "about" communications without also missing a significant portion of "to/from" communications. Nor does the agency have the capability to selectively acquire certain types of "about" communications but not others.

At least some forms of "about" collection present novel and difficult issues regarding the balance between privacy and national security. But current technological limits make any debate about the proper balance somewhat academic, because it is largely unfeasible to limit "about" collection without also eliminating a substantial portion of upstream's "to/from" collection, which would more drastically hinder the government's counterterrorism efforts.

We therefore recommend that the NSA work to develop technology that would enable it to identify and distinguish among the types of "about" collection at the acquisition stage, and then selectively limit or modify its "about" collection, as may later be deemed appropriate. If it is not possible for collection devices to identify or differentiate among types of "about" communications at the acquisition stage, we urge the NSA to develop technology that would allow it to automatically segregate all "about" communications after collection (and, if possible, to individually segregate different types of "about" communications from one another after collection). With such mechanisms in place, it will be possible to have a policy discussion about whether or not the privacy impacts of particular types of "about" collection justify treating those types of communications in a different way or eliminating their collection entirely.

V. Accountability and Transparency

Recommendation 8: To the maximum extent consistent with national security, the government should create and release, with minimal redactions, declassified versions of the FBI's and CIA's Section 702 minimization procedures, as well as the NSA's current minimization procedures.

The Board believes that the public would benefit from understanding the procedures that govern the acquisition, use, retention, and dissemination of information collected under Section 702. The Board respects the government's need to protect its operational methods and practices, but it also recognizes that transparency enables accountability to the public that the government serves. Therefore, the Board urges the government to engage in a declassification review and, to the greatest extent possible without jeopardizing national security, release unredacted versions of the FBI, CIA, and NSA minimization procedures.

Recommendation 9: The government should implement five measures to provide insight about the extent to which the NSA acquires and utilizes the communications involving U.S. persons and people located in the United States under the Section 702 program. Specifically, the NSA should implement processes to annually count the following: (1) the number of telephone communications acquired in which one caller is located in the United States; (2) the number of Internet communications acquired through upstream collection that originate or terminate in the United States; (3) the number of communications of or concerning U.S. persons that the NSA positively identifies as such in the routine course of its work; (4) the number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles, or other identifiers potentially associated with individuals; and (5) the number of instances in which the NSA disseminates non-public information about U.S. persons, specifically distinguishing disseminations that includes names, titles, or other identifiers potentially associated with individuals. These figures should be reported to Congress in the NSA Director's annual report and should be released publicly to the extent consistent with national security.

Under Section 702, the government acquires the contents of telephone calls and Internet communications from within the United States, without individualized warrants or court orders, so long as the acquisition involves targeting non-U.S. persons reasonably believed to be located outside the United States, for foreign intelligence purposes.

Those targeted persons, of course, may communicate with U.S. persons or people located in the United States, resulting in the "incidental" collection of their communications. Since the enactment of the FISA Amendment Act in 2008, the extent to which the government acquires the communications of U.S. persons under Section 702 has been one of the biggest open questions about the program, and a continuing source of public concern. Lawmakers and civil liberties advocates have called upon the executive branch to disclose how many communications of U.S. persons are being acquired. In turn,

the executive branch has responded that it cannot provide such a number — because it is often difficult to determine from a communication the nationality of its participants, and because the large volume of collection under Section 702 would make it impossible to conduct such determinations for every communication that is acquired. The executive branch also has pointed out that any attempt to document the nationality of participants to communications acquired under Section 702 would actually be invasive of privacy, because it would require government personnel to spend time scrutinizing the contents of private messages that they otherwise might never access or closely review.

As a result of this impasse, lawmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under Section 702.

Based on information provided by the NSA, the Board believes that certain measures can be adopted that could provide insight into these questions without unduly burdening the NSA or disrupting the work of its analysts, and without requiring the agency to further scrutinize the contents of U.S. persons' communications. We believe that the NSA could implement five measures, listed above, that collectively would shed some light on the extent to which communications involving U.S. persons or people located in the United States are being acquired and utilized under Section 702. While the measures we have proposed will provide only partial insight into this question (they will not, for instance, reveal the number of communication obtained under PRISM collection, which accounts for the vast majority of Internet acquisitions), they will provide a snapshot, albeit imperfect, of the degree to which the NSA under Section 702 acquires communications involving U.S. persons, queries them, retains them permanently, and disseminates information from them to other agencies.

The number of queries and disseminations involving U.S. person information are already tracked by the NSA, but we believe that these figures should be annually reported in a central document along with the new figures we have proposed counting, and that the NSA's annual reporting of its queries and disseminations should highlight those that potentially involve *individuals* (as opposed to businesses or institutions), which are of special interest from a privacy perspective. It is possible that with respect to the first two measures above, the information that the NSA feasibly can document might turn out to be insufficiently comprehensive to yield dependable numbers, but this will not be known until the NSA attempts to implement the recommendation.

Adopting the measures that we have proposed will supply policymakers and the public with important information about one of the most frequently discussed aspects of the Section 702 program, enabling more informed judgments to be made about the program in the future.

VI. Efficacy

Recommendation 10: The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs.

The efficacy of any particular counterterrorism program is difficult to assess. Even when focusing only on programs of *surveillance*, such programs can serve a variety of functions that contribute to the prevention of terrorism. Most obviously, a surveillance program may reveal the existence of a planned terrorist attack, enabling the government to disrupt the attack. But the number of "plots thwarted" in this way is only one measure of success. Counterterrorism surveillance programs can enable the government to learn about the identities and activities of the individuals who make up terrorist networks. They can help the government to understand the goals and intentions of those organizations, as well as the ways in which the organizations fund their pursuits and coordinate the activities of their members. All of this knowledge can aid the government in taking steps to frustrate the efforts of these terrorist organizations — potentially stymieing their endeavors long before they coalesce around the plotting and implementation of a specific attack. Because the nature of counterterrorism efforts can vary, measures of success may vary as well.

Moreover, individual counterterrorism programs are not typically used in isolation; rather, these programs can support and mutually reinforce one another. Therefore, the success of a particular program may not be susceptible to evaluation based on what it produces in a vacuum. Any evaluation must instead seek to understand how a particular program fits within the government's overall counterterrorism efforts, and to what degree it aids those efforts relative to other programs.

Despite these complications, determining the efficacy and value of particular counterterrorism programs is critical. Without such determinations, policymakers and courts cannot effectively weigh the interests of the government in conducting a program against the intrusions on privacy and civil liberties that it may cause. In addition, government counterterrorism resources are not unlimited, and if a program is not working, those resources should be redirected to programs that are more effective in protecting us from terrorists. Accordingly, the Board believes that the government should develop a methodology to gauge and assign value to its counterterrorism programs, and use that methodology to determine if particular programs are meeting their stated goals. The Board is aware that the ODNI conducts studies to measure the relative efficacy of different types of intelligence activities to assist in budgetary decisions. The Board believes that this important work should be continued, as well as expanded so as to differentiate more precisely among individual programs, in order to assist policymakers in making informed, data-driven decisions about governmental activities that have the potential to invade the privacy and civil liberties of the public.

Part 7:

CONCLUSION

One of the Board's goals in developing this Report has been to provide greater transparency and clarity to the public regarding the operation of the Section 702 program. This is a complex program, and, in the wake of the unauthorized disclosures about the program, there has been a great deal of misinformation circulated to the public. The Board is grateful to the Intelligence Community and the Department of Justice for its employees' tireless efforts to educate Board Members and staff about the program's operation, and to work with us to declassify information in the public interest. The Board also appreciates the work of the many government officials and employees, congressional staff, privacy and civil liberties advocates, academics, trade associations, and technology and communications companies who provided input into the Board's study of the program.

In addition to this effort to explain the Section 702 program, the Board has set forth a series of policy recommendations designed to ensure that the program appropriately balances national security concerns with privacy and civil liberties. We note that this is only the start of the dialogue. We do not believe that any of the recommendations we offer would require legislative changes, and the Board welcomes the opportunity for further discussion of these pressing issues and how to best implement the Board's recommendations. We hope that this Report contributes to "a way forward that secures the life of our nation while preserving the liberties that make our nation worth fighting for."[549]

[549] Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

INDEX TO ANNEXES

A. Separate Statement by Chairman David Medine and Board Member Patricia Wald

B. Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook

C. July 9, 2013 Workshop Agenda and Link to Workshop Transcript

D. November 4, 2013 Hearing Agenda and Link to Hearing Transcript

E. March 19, 2014 Hearing Agenda and Link to Hearing Transcript

F. Request for Public Comments on Board Study

G. Reopening the Public Comment Period

H. Index to Public Comments on www.regulations.gov

ANNEX A

Separate Statement of Chairman David Medine and Board Member Patricia Wald

I. Recommendation Regarding U.S. Person Queries for Foreign Intelligence Purposes

We do not believe that the Board's Recommendation 3 goes nearly far enough to protect U.S. persons' privacy rights when their communications are incidentally collected as a consequence of targeting a non-U.S. person located abroad under Section 702. The Section 702 program has collected hundreds of millions of Internet communications. Even if only a small percentage of those communications are to or from an American, the total number of Americans' communications is likely significant. Furthermore, these communications, which may be maintained for many years in government databases in searchable form, may contain sensitive and confidential matters having nothing to do with the foreign intelligence purposes of the Section 702 program. Although such queries must be conducted for a foreign intelligence purpose, currently, the government can query several years of such communications without court approval, which could potentially produce a composite picture of a significant slice of an American's private life.

This practice raises two related concerns with constitutional, statutory, and policy implications. First, are sufficient protections in place to purge Americans' communications that have no foreign intelligence value? Second, are there sufficient restrictions on when the government can query data collected under Section 702 to seek Americans' communications? We offer the following proposals to address each of these concerns.

Recommendation

Minimization procedures that govern the use of Americans' communications collected under Section 702 should require the following:

(1) No later than when the results of a U.S. person query of Section 702 data are generated, Americans' communications should be purged of information that does not meet the statutory definition of foreign intelligence information relating to Americans.[550] This process should be subject to judicial oversight.

(2) Each U.S. person identifier should be submitted to the FISA court for approval before the identifier may be used to query data collected under Section 702 for a foreign

[550] U.S. person communications may also be responsive to queries using non-U.S. person identifiers. The same purge procedure should apply in such cases.

intelligence purpose,[551] other than in exigent circumstances or where otherwise required by law.[552] The court should determine, based on documentation submitted by the government, whether the use of the U.S. person identifier for Section 702 queries meets the standard that the identifier is reasonably likely to return foreign intelligence information as defined under FISA.[553]

Discussion

As explained in Part 3 above, under Section 702, the government may lawfully collect the communications of an American where that individual is communicating with a targeted non-U.S. person who is reasonably believed to be located outside the United States.[554] The government refers to the collection of such Americans' information as "incidental" collection, because the American will not be, and cannot be, the target of Section 702 surveillance. Although we understand that the government does not currently count the number of incidentally collected American communications, it is likely that the scope and extent of the Americans' information collected under Section 702 is substantial: as of 2011, the NSA was acquiring approximately 250 million Internet communications annually, and even if only a small percentage of these total involved Americans the number would be large in absolute terms.[555]

We recognize that a query of collected Section 702 data seeking information about a specific American[556] may not provide as complete a picture of the individual's activities as it would for an actual target of surveillance. Nonetheless, such queries are capable of

---

551 Queries for criminal purposes are governed by the proposal in Part II of this statement.

552 *See, e.g., Brady v. Maryland*, 373 U.S. 83 (1963); Fed. R. Crim. P. 16 (a)(1)(B); and 18 U.S.C. § 3500 (Jenks Act).

553 Subsequent queries using a FISA court–approved U.S. person identifier would not require court approval.

554 Through "about" collection, the NSA may also collect the communication of an American who is not in direct contact with a Section 702 target if a targeted selector appears within the communication. In addition, the NSA may collect the communications of an American who is not in direct contact with a Section 702 target through acquiring an "MCT." However, such communications are acquired only through upstream collection and, thus, they may not be queried using U.S. person identifiers under current minimization procedures.

555 The NSA minimization procedures state that permanent retention of communications of Americans is permitted if they are of foreign intelligence value or certain other standards are met, including communications in which the identity of the American is necessary to understand foreign intelligence information or assess its importance. 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, § 6(b)(2) (Oct. 31, 2011) ("NSA 2011 Minimization Procedures").

556 We are not proposing that the parties to every communication be investigated to determine if one or more of the parties are Americans. Such reviews themselves could raise privacy and civil liberties concerns. However, where there is a reasonable basis to conclude that a party is an American, the recommended procedures should apply.

revealing a significant slice of the American's life. This is particularly the case for Americans who correspond frequently with foreigners, including relatives, business associates, and others. Because the scope of the legitimate foreign intelligence purposes that may justify surveillance under Section 702 is broad, going beyond counterterrorism, an American could be in contact with several targets of Section 702 surveillance and yet be innocent of any complicity in terrorist or other activity of foreign intelligence interest. Since Section 702 does not require any particularized judicial finding to support the initial collection of information from either the foreign target or the American who communicated with the target, further safeguards should be required to limit the permissible scope of U.S. person queries. Under present rules, querying of the communications to which the American was a party can be justified either on the grounds that they are likely to have foreign intelligence value or contain evidence of a crime.[557] Moreover, there is currently no external check outside of the executive branch on the process of making such queries or purging of non–foreign intelligence material from query results.

We agree that legitimate foreign intelligence matters which appear in these Americans' incidentally collected communications can be retained. However, we feel strongly that the present internal agency procedures for reviewing communications and purging those portions that are of no foreign intelligence value prior to use of the information[558] are wholly inadequate to protect Americans' acknowledged constitutional rights to protection for private information or to give effect to the statutory definition of foreign intelligence information, which, as discussed below, provides a more stringent test for information relating to Americans. Minimization guidelines approved by the FISA court were intended to afford these protections, but in their present form they do not. As a practical matter, most collected communications are not reviewed for the purging of non–foreign intelligence matters upon collection, or at any set time thereafter prior to use. The NSA guidelines require only that "upon review" the analyst should purge material that is "clearly" non–foreign intelligence information. The practice, when applying the "clearly" criteria for purging Americans' communications, is to err on the side of insuring that any piece of private information is retained that might in the future conceivably take on value or that some other analyst in the intelligence community might find to be of value. We do not think this is the intent of the statute.

Some argue that the process of reviewing and purging of private information that has no intelligence value is more intrusive than permitting the information to remain in agency databases for years subject to viewing by intelligence personnel in multiple

---

557 *See* Section II of this Separate Statement regarding FBI queries relating to evidence of a crime.

558 NSA 2011 Minimization Procedures, *supra*, § 3.

agencies. In our view, there is no legitimate basis to maintain potentially personal, sensitive information that has no bearing on either foreign intelligence or criminal conduct. Nor do the restrictions on use of FISA data in criminal investigations requiring only Attorney General approval provide adequate protections to the vast majority of Americans whose communications have been incidentally collected, who will never be subjected to such proceedings, but whose information can be probed and queried and used to pursue investigations against them.

Our conclusion that more controls are required for this query process is informed by constitutional, statutory, and policy concerns. As discussed above, under the Fourth Amendment, the reasonableness of this program must be assessed based on the totality of the circumstances.[559] The government recognizes that the initial collection of Americans' communications under Section 702 constitutes a search under the Fourth Amendment. The reasonableness of this surveillance depends upon whether there are sufficient safeguards, including targeting and minimization procedures, to adequately protect the Fourth Amendment interests of persons whose communications may be collected, used, and disseminated. Since there are no prior determinations that any Americans whose communications have been collected are involved in terrorism or other activities of foreign intelligence interest (because Americans cannot be targeted), there should be compensatory safeguards governing the access, use, dissemination, and retention of the contents of their communications when those communications are acquired in the course of targeting others.

In this regard, we do not believe that the Fourth Amendment analysis justifying, in other contexts, the use of queries directed at individuals who are not themselves surveillance targets applies with equal force to querying U.S. person communications acquired in the Section 702 program. As discussed above, the incidental collection of information through a Title III wiretap meets Fourth Amendment standards based on the prior judicial review, showing of probable cause, and particularity in the wiretap order, which justifies the surveillance both with respect to known suspects and with respect to incidental interceptees.[560] Under Section 702, by contrast, there is no probable cause or other individualized finding by a judge — either with regard to the non-U.S. person who is the target of the surveillance or the American who communicates with the target. Nor is there any judicial review after the fact of targeting decisions or queries. It is troubling to allow the government without some form of judicial approval to compile and review private communications by U.S. persons who have not consented to the government's collection. To address these constitutional concerns, more robust safeguards should be

559 *Samson v. California*, 547 U.S. 843, 848 (2006).

560 *United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977).

required at the query stage, whenever the government seeks to conduct queries seeking information about U.S. person's communications, in order to support the reasonableness of the program. Existing query standards, which require no outside review, are insufficient to compensate for the lack of judicial review at the front end so as to provide assurance about the legitimacy and scope of the collection. On the other hand, judicial review would not be necessary for queries seeking communications of U.S. persons who are already approved as targets for collection under Title I or Sections 703/704 of FISA and identifiers that have been approved by the FISA court under the "reasonable articulable suspicion" standard for telephony metadata under Section 215.[561] As a result, this would not restrict queries regarding U.S. persons who are already suspected terrorists and are under surveillance.

The statutory framework of FISA further supports the need for enhanced safeguards for U.S. person information. The definition of foreign intelligence information under FISA, which is incorporated by reference into Section 702, sets forth several categories of information, including information regarding international terrorism or international proliferation of weapons of mass destruction. To meet the statutory definition, the information generally must "*relate* to" one of the listed categories, but if the information concerns a U.S. person, the definition specifically requires that the information must "be *necessary* to" the ability of the United States to protect against these threats.[562] At the query stage, this definition is relevant because the NSA minimization procedures require that queries using U.S. person identifiers must be reasonably likely to return foreign intelligence information. We believe that foreign intelligence information in the query context must track the statutory definition, which, for U.S. persons, involves the higher "necessary" standard.

When FISA was originally enacted, Congress made clear in passing the statute that enhanced safeguards were needed for U.S. person information. As the report of the House Permanent Select Committee on Intelligence explained:

> [T]he committee has adopted a definition of foreign intelligence information which includes any information relating to these broad security or foreign relations concerns, so long as the information does not concern U.S. persons. Where U.S. persons are involved, the definition is much stricter; it requires that the information be "necessary" to these security or foreign relations concerns.

---

561 It would also not be necessary if the query produces no results or the analyst purges all results from the given query as not containing foreign intelligence.

562 50 U.S.C. § 1801(e) (emphasis added).

> Where the term "necessary" is used, the committee intends to require more than a showing that the information would be useful or convenient. The committee intends to require a showing that the information is both important and required. The use of this standard is intended to mandate that a significant need be demonstrated by those seeking the surveillance. For example, it is often contended that a counterintelligence officer or intelligence analyst, if not the policymaker himself, must have every possible bit of information about a subject because it might provide an important piece of the larger picture. In that sense, any information relating to the specified purposes might be called "necessary" but such a reading is clearly not intended.[563]

To give effect to this definition of foreign intelligence information under FISA, and the cautionary words from both the House and Senate reports, we believe that the approval process for U.S. person queries under Section 702 must be tightened. The more stringent "necessity" test for foreign intelligence information relating to U.S. persons requires that queries seeking to identify incidentally collected communications of an American must be reasonably designed to produce information necessary to the ability of the United States to protect against the listed threats, or to assure the defense or security of the United States or the conduct of its foreign affairs. It is imperative that a process be instituted to assure compliance with this definition.

Finally, as a policy matter, we seek to find the appropriate balance that will enable the government to pursue its legitimate foreign intelligence purposes while still safeguarding legitimate privacy interests. The government urges that once information has been lawfully collected, it may be used for any lawful purposes, and that existing minimization rules under Section 702 provide sufficient safeguards against improper use. In contrast, on June 19, 2014, the U.S. House of Representatives, by a 293-to-123 bipartisan vote, approved a ban on U.S. person queries under Section 702.[564] The President's Review Group on Intelligence and Communications Technologies, many advocacy organizations, certain members of Congress, and others have urged that in order to conduct a U.S. person query of Section 702 data, the government should be required to obtain a FISA warrant under Title I of the statute and demonstrate probable cause that the U.S. person is a foreign power or an agent or employee of a foreign power. Last week, a federal district court judge noted that whether the Fourth Amendment requires a warrant for queries to be conducted

---

563 H.R. Rep. No. 95-1283, at 47 (1978); *see also* S. Rep. No. 95-701, at 31 (1978) (containing similar language).

564 The ban applies to agencies that would be funded under the proposed Defense Appropriations Act, 2015 (H.R. 4870), which would not include the FBI. *See* H.Amdt.935, 113th Cong. (2014), 160 CONG. REC. H5,544 (daily ed. June 19, 2014), *available at* http://www.gpo.gov/fdsys/pkg/CREC-2014-06-19/pdf/CREC-2014-06-19.pdf.

of Section 702 data was "a very close question."[565] He ultimately ruled the Fourth Amendment did not require a warrant even though such a requirement might "better protect Americans' privacy rights." We believe that the middle course we propose — not banning queries or requiring a warrant but instead requiring judicial approval of queries employing a more relaxed standard — more appropriately balances the government's legitimate foreign intelligence purposes with the privacy rights of Americans.

With regard to query results, it is important on both legal and policy grounds for the government to implement procedures under which Section 702 communications are reviewed to assess whether they meet the statutory definition of foreign intelligence information applicable to U.S. persons no later than when the results of a U.S. person query are generated, to insure that only those meeting the "necessary" standard are used, retained or disseminated and those not meeting the definition are purged.[566] At base we believe some external oversight of the review process is essential to counteract an understandable but strong reluctance of analysts to give up any information that might conceivably have some future remote value, despite the more restrictive statutory definitions of foreign intelligence for Americans' information.[567]

While we conclude that a particularized judicial finding should be required *before* a U.S. person query has been made, to ensure that it has a proper basis, we believe the FISA Title I standard for targeting is too demanding in the query context. Rather, the

---

565 *United States v. Mohamud*, No. 10-475, 2014 WL 2866749 at *26 (D. Or. June 24, 2014).

566 We recognize that some communications of Americans may never be returned as the result of a query or otherwise reviewed before they are "aged-off" of agency systems at the end of the data retention period.

567 One alternative in that regard would be for the FISA court to use a special master with a security clearance to regularly review representative samples of query results. The master would assess whether information that does not meet the statutory definition of foreign intelligence information had been properly purged and report to the court on the master's findings. *See In re U.S. Dep't of Defense*, 848 F.2d 232, 239 (D.C. Cir. 1988) ("[W]here a massive number of classified documents exists such that the judge and his law clerk simply cannot examine them all . . . appointment of a master to structure the judge's review of these documents is appropriate so long as the judge retains decisional authority over the issue in question."). If the FISA court concluded over time that the review and purging process was working properly, this review process could be relaxed or suspended. If, on the other hand, the FISA court, based on the master's report, concluded that Americans' communications were not being properly minimized, the court would have discretion to expand its oversight of this process to insure that the privacy interests of Americans with regard to non–foreign intelligence communications were being protected. There is some similarity between this proposal and the operation of federal wiretaps. Under federal law, "[i]mmediately upon the expiration of the [wiretap order] recordings shall be made available to the judge issuing such order and sealed under his directions." 18 U.S.C. § 2518(8)(a). This allows the court to assure itself that the government is getting the evidence that the warrant authorized. If the judge concludes that the government was collecting information outside of the scope of the warrant, the FISA court would be able to modify or terminate the wiretap authority or impose any other appropriate restrictions.

The ultimate goal of this would be to align agency practice with statutory and constitutional requirements.

government should be permitted to conduct U.S. person queries so long as the FISA court finds that the U.S. person identifier was reasonably likely to return foreign intelligence information as defined under FISA. If the Board's Recommendation 1 regarding targeting is adopted, the Section 702 program will provide sufficient front-end safeguards that we do not believe a probable cause standard is needed at the query stage. And, provided that the statutory definition of foreign intelligence information is strictly followed, including the requirement that the Americans' information sought be "necessary to" the government's ability to protect against international terrorism or other designated threats, we conclude that it is appropriate for the government to seek such information through U.S. person queries without demonstrating that the American in question is an agent of a foreign power.

At the end, the current system allows a U.S. person about whom there is no suspicion of being a terrorist or engaging in other illegal activity but who unknowingly corresponds with the target of a Section 702 proceeding — perhaps a relative or professional colleague or old friend — to have his or her correspondence with the target, over a period of several years, collected, reviewed at will by intelligence analysts, and retained in a FISA data bank. If the unknowing correspondent's emails or other Internet material do display information of foreign intelligence value, it can be used as such and we have no objection to that. But without any such determination, the correspondence in toto, however private or confidential, can be stored for years and it can be queried using the unknowing correspondent's name as a selector not only by a few but by many NSA foreign intelligence analysts. The unknowing correspondent's information may also be used under restrictions, but nonetheless used and disseminated outside the agency in reports or provided to a foreign government — all this with no prior review beyond that conducted within the intelligence community. The possibility of such an occurrence, even if rare, does not seem to us to come near the Fourth Amendment reasonableness standard for a significant component of Section 702 or to comply with the letter and spirit of FISA. We feel strongly that a neutral and detached judicial officer should approve the use of U.S. person identifiers. That requirement traditionally has been considered a critical component of Fourth Amendment protections against overbroad searches.[568] As the Supreme Court stated last week, noting the importance of judicial approval for government access to information, "the Founders did not fight a revolution to gain the right to government agency protocols."[569]

---

568 *See, e.g., United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.*, 407 U.S. 297, 309 (1972) ("*Keith*") (reasonableness under the Fourth Amendment "derives content and meaning through reference to the warrant clause").

569 *Riley v. California*, No. 13-132, 2014 WL 2864483, at *16 (U.S. June 25, 2014).

II. Recommendation Regarding FBI Queries for Criminal Purposes

The Board's unanimous Recommendation 2 states that additional limits should be placed on the FBI's use and dissemination of Section 702 data in connection with non–foreign intelligence criminal matters. In our view, these limits should include the requirement that the FBI obtain prior FISA court approval before using identifiers to query Section 702 data to ensure that the identifier is reasonably likely to return information relevant to a criminal assessment or investigation of a crime. In response, Board Members Brand and Cook, in their separate statement, refer to the practice of FBI's using the results of Section 702 data queries in the investigation and prosecution of crimes as largely theoretical. Yet the FBI has not only the capability to conduct such queries but has authorized them, and, in fact, criminal agents do conduct such queries routinely; the fact is that we do not know the precise number of times there is a subsequent use of any results from those queries.[570]

Privacy and civil liberties concerns regarding "incidentally" collected Section 702 information do not just arise when that information is used outside the FBI, such as to obtain a search warrant. The information can also be used inside the FBI to make determinations about Americans that adversely affect them, such as deciding to move from an assessment to a formal criminal investigation. A troubling precedent could be created by permitting a general search of Section 702 material, including incidental collections of innocent Americans' private information, which was collected with no articulable suspicion and particularized judicial approval and target-specific oversight. It could have implications when it comes to general access throughout the government to big data repositories collected for a specific purpose and under specific restrictions by a particular agency. In the case of domestic criminal law enforcement, which currently operates under a painstaking structure with deep roots in the Fourth Amendment and a myriad of particularized statutes and case law, a general permission to search such protected data without any need to demonstrate even an articulable suspicion about the named selector is especially worrisome. Finally, FISA court judges, who are drawn from the ranks of federal district judges and who preside over grand jury proceedings and criminal trials, have extensive experience in evaluating what is or is not relevant evidence in a criminal

---

570 Board Members Brand and Cook are concerned that any justification for a query at an early stage in a criminal investigation will often be unworkable. The alternative, however, is to permit queries of innocent subjects' Section 702 communications without even an articulable suspicion of wrongdoing or terrorist affiliations. We note also that there is nothing to support the assertion that these queries are less "intrusive" of privacy than the other techniques listed in the Attorney General's Domestic Rules as permissible in early stage investigations, i.e., public information, online resources, volunteered information, consent searches and requested information. Federal Bureau of Investigation, Domestic Investigations and Operations Guide, § 5.9.1 (Oct. 15, 2011), *available at* http://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/fbi-domestic-investigations-and-operations-guide-diog-2011-version.

investigation and our proposal that they be required to do so would not rule out queries essential to an investigation.

We do not anticipate that requiring judicial approval for queries in ordinary crime situations will erect any serious impediment to law enforcement. On the other hand, Board Members Cook and Brand's suggestion that FBI agents be allowed to use Section 702 data without judicial approval not only in the investigative stage but, with approval by Department of Justice officials, as the basis for a warrant or grand jury subpoena, raises the substantial statutory and constitutional questions discussed above.

Our proposal will not ban any queries regarding U.S. persons or others in investigations of either foreign intelligence or domestic crimes, but rather would interpose a time honored protection of approval by a detached judicial officer of government access to Americans' communications. This is the minimal protection that should be afforded to U.S. persons who have done nothing to merit forfeiture of all Fourth Amendment protection to their private papers.

ANNEX B

Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook

I. The Program is Legal and Effective

We hope that the length of the Board's report and its comprehensive discussion of the legal considerations surrounding the program will not obscure the Board's unanimous bottom-line conclusion: The core Section 702 program is clearly authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective intelligence tool.

To the extent that the Board had concerns about the program after our thorough review, they focused primarily on two particular aspects to the program's current operation: the practice of searching the database using a U.S. person identifier, and so-called "about" collection, both of which are discussed at length in the Board's report. The Board makes a few targeted recommendations to address concerns raised by these two aspects of the program. We stress that these are *policy*-based recommendations designed to tighten the program's operation and ameliorate the extent to which these aspects of the program could affect the privacy and civil liberties of U.S. persons. We do not view them to be essential to the program's statutory or constitutional validity.

II. Queries of Section 702 Information

The extent to which additional restrictions should apply to agencies' ability to query information collected pursuant to Section 702 using U.S. person identifiers has divided the Board. In the case of the FBI, this issue is intertwined with questions about querying Section 702 information for non–foreign intelligence purposes, the potential use of Section 702 information in criminal proceedings, and longstanding efforts to ensure information sharing within the agency. Specifically, the Board grappled with what to do about the fact that it is theoretically possible for a database query by an FBI analyst in a non–foreign intelligence criminal matter to return Section 702 information and for this information to be further used in the investigation and prosecution of that crime.[571] In addressing this issue, we believe it important to adopt a policy that matches the scope of the problem, can work as a practical matter, and will not unnecessarily impair the government's ability to conduct counterterrorism and other national security–related investigations.

---

571 The FBI receives only a small portion of Section 702 information and receives no information collected upstream. *See* Letter from Deirdre M. Walsh, Director of Legislative Affairs, to Hon. Ron. Wyden, United States Senate (June 27, 2014) (responding to question regarding number of queries using U.S. person identifiers of communications collected under Section 702).

The concern: As discussed at length in the Board's Report, Section 702 collection differs from traditional electronic surveillance in a few key ways, including a lower standard for collection and the absence of a particularized judicial finding for targeting decisions. Moreover, Section 702 has an explicit foreign intelligence purpose requirement for authorized collection, consistent with the longstanding distinction between foreign intelligence and criminal purposes reflected elsewhere in FISA. Given these factors, our key concerns were the querying of Section 702 collection for *non–foreign intelligence* purposes, and the potential subsequent use of that information to further a non–foreign intelligence criminal investigation or prosecution.[572]

Scope: According to initial information provided by the FBI, it seems clear that FBI agents and analysts routinely conduct queries across all FBI databases in non–foreign intelligence investigations and assessments. This is unsurprising, given that the FBI has traditionally considered the querying of information already within its possession to be among the least intrusive investigative techniques available, and the agency's overall efforts since 9/11 to foster information sharing and eliminate stovepipes. But the story is far different for the potential *use* of Section 702 information in the investigation or prosecution of non–foreign intelligence crimes. We are unaware of any instance in which a database query in an investigation of a non–foreign intelligence crime resulted in a "hit" on 702 information, much less a situation in which such information was used to further such an investigation or prosecution.

Our proposal: As stated in the Board's Report, we would not place limitations on the FBI's ability to include its FISA database among the databases *queried* in non–foreign intelligence criminal matters. We believe that querying information already in the FBI's possession is a relatively non-intrusive investigative tool, and the discovery of potential links between ongoing criminal and foreign intelligence investigations is potentially critical to national security.[573] Instead, we would require an analyst who has not had FISA training to seek supervisory approval before *viewing* responsive Section 702 information, to ensure that the information continues to be treated consistent with applicable statutory and court-imposed restrictions.

We believe that placing some additional limitations on the *use* of Section 702 information in non–foreign intelligence criminal matters may also be warranted because of the increased civil liberties concerns raised by the use of FISA information outside the foreign intelligence context. Conceptually, the appropriate point at which to potentially limit the use of that information is where it could infringe on a person's liberty by, for

---

572 *See In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. November 18, 2002).

573 See pages 108-10 of this Report. *See generally*, The Webster Commission, *Final Report of the William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009* (2012).

example, being used as the basis for obtaining a search warrant, wiretap, or other intrusive investigative tool, as the basis for a criminal indictment in a grand jury proceeding, or as evidence in a criminal prosecution. Where current policy does not already require the approval of at least the Assistant Attorney General,[574] we would require such approval before Section 702 information could be used in these contexts.

We note that it is already very unlikely that Section 702 information would be used in this way because of the existing significant hurdles to the use of *any* FISA-derived information in a criminal proceeding.[575] FISA requires the personal approval of the Attorney General, Deputy Attorney General, or Assistant Attorney General for National Security before FISA-derived information can be used as evidence at trial or in some of the more preliminary stages of the criminal process, such as before the grand jury.[576] FISA also requires that criminal defendants be notified if FISA-derived information will be used against them in a criminal proceeding. And since any decision to use Section 702 information risks revealing the intelligence community's sources and methods, there is always a strong disincentive to permit it. The hurdles imposed by these existing requirements result in Section 702 information being used rarely in the prosecution of even national security–related crimes, and perhaps never in the prosecution of other crimes. As such, our proposal would not create an entirely new and unknown set of rules, but would build an added level of protection for civil liberties into the existing structure.

Concerns with requiring court approval prior to querying: Chairman Medine and Member Wald would require the FBI to obtain FISC approval prior to querying FISA-obtained information, regardless of whether the query relates to a U.S. person, and even in the investigation of foreign intelligence crimes such as terrorism or espionage. For an FBI query for foreign intelligence purposes (not including investigation of foreign intelligence crimes), the FISC would have to first determine that the query was likely to return foreign intelligence information. For an FBI query in the investigation of any crime—including foreign intelligence crimes—the FISC would have to first determine that the query was likely to return evidence relevant to the investigation.[577] We have significant concerns

---

574 *See* Memorandum from Michael B. Mukasey, Attorney General, to all Federal Prosecutors, *Revised Policy on the Use or Disclosure of FISA Information*, at 2-7 (January 10, 2008).

575 50 U.S.C. § 1806(b).

576 *Id*. at §1806(c). We note that the Department of Justice has recently clarified its view of when information used in a criminal proceeding may be "derived from" prior Title VII FISA collection. *See, e.g., United States v. Mohamud*, No. 3:10-CR-475 slip op. at 3 (D. Or. June 24, 2014) (quoting government filing). In addition, the Department's FISA Use Policy imposes additional restrictions to the use of Section 702 information in the context of more routine criminal investigative activities.

577 Foreign intelligence investigations routinely encompass foreign intelligence crimes. How the FBI or the FISA Court would determine which of these standards applied is unclear.

about the implications of this approach, which would likely have significant detrimental consequences far greater than acknowledged (or perhaps intended) by our colleagues.

First and foremost, although the apparent motivation of this proposal is to protect U.S. persons, it could not be limited to U.S. persons in practice. The FBI (our domestic law enforcement agency) naturally does not distinguish between U.S persons and non-U.S. persons, which means this proposed requirement would apply by default to *all* queries of the FISA database, by *all* FBI personnel, in *any* FBI investigation of *any* crime. And requiring the FBI to determine whether the subject of a query is a U.S. person could result in more intrusive investigation of that person than would otherwise occur.[578]

Similarly, although the motivation of the proposal is to address incidental collection of U.S. person information through the Section 702 program, the FBI currently combines all FISA-obtained information in one database, which means that as a practical matter the proposal would prohibit the FBI from searching any FISA-obtained information without first obtaining a court order.

Although Chairman Medine and Member Wald reference a requirement for "judicial approval for queries in ordinary crime situations," the text of their proposal covers even foreign intelligence crimes, meaning that an FBI agent investigating an al Qaeda operative for terrorism would have to go to the FISA court to run a query of any FISA-obtained information. Requiring the FBI to undertake the lengthy and burdensome FISC approval process before an FBI analyst could even query the information would create practical challenges so daunting that it likely never would be pursued. Even if the FBI could obtain prior approval, this would result in significant delay of the investigation and potentially enormous burdens on the FISC. The practical effect of this proposal would be to prevent the FBI from using one of our most valuable foreign intelligence tools to investigate foreign intelligence crimes. It is hard to imagine adopting a rule that is so at odds with the recommendations of the 9/11 Commission, the Webster Commission, and others in the years following 9/11.[579]

In addition to requiring judicial approval, the proposal would impose a standard for the court's approval in investigations of crime that would be unworkable in many circumstances. Database queries are often used at the earliest stages of an investigation – such as during an assessment, perhaps to follow up on a tip. At this stage, an analyst knows very little and conducts a query to see if there is anything at all that creates a reason to

---

578 Although apparently grounded in Fourth Amendment principles, the proposal makes no distinctions between contents of communications and metadata—as to which there is *no* currently recognized Fourth Amendment interest.

579 *See* National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States,* at 78-80, 416-418 (2004); The *Webster Commission Report,* at 94-95 and 136-39.

further pursue the investigation. It is hard to imagine the basis on which the FISC could assess what, if anything, will be returned in a database query at this stage, which would require the FISC to deny the application.

Finally, the proposal could actually exacerbate civil liberties concerns in at least two respects. First, a query of information already in the FBI's possession has been considered one of the least intrusive investigative means available, and is therefore one of the first steps taken in any assessment or investigation. But now in order to use this preliminary investigative tool, our colleagues would require the FBI to assemble information sufficient to facilitate meaningful judicial review, which will inevitably require the use of *more* intrusive means. Second, because queries at the early stages of an investigation are often used to eliminate individuals from suspicion, discouraging queries could prevent the discovery of exculpatory information that otherwise might establish an individual's innocence.

NSA and CIA: Our colleagues also would require prior court approval for NSA and CIA queries of Section 702 information when they involve U.S. person identifiers. Based on our review of the current use and extensive oversight of U.S. Person queries at the NSA and CIA, which we have accurately characterized at "rigorous,"[580] the majority has declined to recommend such a requirement.[581]

---

580 Board Report at Recommendation 4.

581 We are also concerned about the potential implications of Chairman Medine and Member Wald's proposal regarding minimization. To the extent that their approach requires an analyst to review U.S. Person communications that the analyst would not otherwise review, we think it far from clear that it is more protective of privacy than leaving those communications in the database unreviewed until the end of the retention period.

ANNEX C

AGENDA OF PUBLIC WORKSHOP

HELD ON JULY 9, 2013

Link to Workshop transcript:

http://www.pclob.gov/All%20Documents/July%209,%202013%20Workshop%20Transcript.pdf

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act

July 9, 2013

Renaissance Mayflower Hotel – Grand Ballroom
1127 Connecticut Ave NW, Washington DC

AGENDA

09:00 **Doors Open**

09:30 – 09:45 **Introductory Remarks (David Medine, PCLOB Chairman)**

09:45 – 11:30 **Panel I: Legal/Constitutional Perspective**
Facilitators: Rachel Brand and Patricia Wald, Board Members

Panel Members:

- **Steven Bradbury (Formerly DOJ Office of Legal Counsel)**
- **Jameel Jaffer (ACLU)**
- **Kate Martin (Center for National Security Studies)**
- **Hon. James Robertson, Ret. (formerly District Court and Foreign Intelligence Surveillance Court)**
- **Kenneth Wainstein (formerly DOJ National Security Division/ White House Homeland Security Advisor)**

12:30 – 2:00 **Panel II: Role of Technology**
Facilitators: James Dempsey and David Medine, Board Members
Panel Members:

- **Steven Bellovin (Columbia University Computer Science Department)**
- **Marc Rotenberg (Electronic Privacy Information Center)**

- **Ashkan Soltani (Independent Researcher and Consultant)**
- **Daniel Weitzner (MIT Computer Science and Artificial Intelligence Lab)**

2:00 – 2:15 **Break**

2:15 – 4:00 **Panel III: Policy Perspective**
Facilitators: Elisebeth Collins Cook and David Medine, Board Members

Panel Members:

- **James Baker (formerly DOJ Office of Intelligence and Policy Review)**
- **Michael Davidson (formerly Senate Legal Counsel)**
- **Sharon Bradford Franklin (The Constitution Project)**
- **Elizabeth Goitein (Brennan Center for Justice)**
- **Greg Nojeim (Center for Democracy and Technology)**
- **Nathan Sales (George Mason School of Law)**

4:00 – 4:10 **Break**

4:10 – 4:30 **Open for Public Comment**

4:30 **Closing Comments (David Medine, PCLOB Chairman)**

Affiliations are listed for identification purposes only.

ANNEX D

AGENDA OF PUBLIC HEARING

HELD ON NOVEMBER 4, 2013

Link to Hearing transcript:

http://www.pclob.gov/SiteAssets/PCLOB%20Hearing%20-%20Full%20Day%20transcript%20Nov%204%202013.pdf

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
PUBLIC HEARING

Consideration of Recommendations for Change:
The Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act
November 4, 2013

Renaissance Mayflower Hotel – Grand Ballroom
1127 Connecticut Ave NW, Washington DC

AGENDA

08:45 **Doors Open**

09:15 – 09:30 **Introductory Remarks (David Medine, PCLOB Chairman, with Board Members Rachel Brand, Elisebeth Collins Cook, James Dempsey, and Patricia Wald)**

09:30 – 11:45 **Panel I: Section 215 USA PATRIOT Act and Section 702 Foreign Intelligence Surveillance Act**

- **Rajesh De (General Counsel, National Security Agency)**
- **Patrick Kelley (Acting General Counsel, Federal Bureau of Investigation)**
- **Robert Litt (General Counsel, Office of the Director of National Intelligence)**
- **Brad Wiegmann (Deputy Assistant Attorney General, National Security Division, Department of Justice)**

11:45 – 1:15 **Lunch Break (on your own)**

1:15 – 2:30 **Panel II: Foreign Intelligence Surveillance Court**

- **James A. Baker (formerly DOJ Office of Intelligence and Policy Review)**
- **Judge James Carr (Senior Federal Judge, U.S. District Court, Northern District of Ohio and former FISA Court Judge 2002-2008)**
- **Marc Zwillinger (Founder, ZwillGen PLLC and former Department of Justice Attorney, Computer Crime & Intellectual Property Section)**

2:30 – 2:45 Break

2:45 – 4:15 Panel III: Academics and Outside Experts

- **Jane Harman (Director, President and CEO, The Woodrow Wilson Center and former Member of Congress)**
- **Orin Kerr (Fred C. Stevenson Research Professor, George Washington University Law School)**
- **Stephanie K. Pell (Principal, SKP Strategies, LLC; former House Judiciary Committee Counsel and Federal Prosecutor)**
- **Eugene Spafford (Professor of Computer Science and Executive Director, Center for Education and Research in Information Assurance and Security, Perdue University)**
- **Stephen Vladeck (Professor of Law and the Associate Dean for Scholarship at American University Washington College of Law)**

4:15 Closing Comments (David Medine, PLCOB Chairman)

All Affiliations are listed for identification purposes only.

ANNEX E

AGENDA OF PUBLIC HEARING

HELD ON March 19, 2014

Link to Hearing transcript:

http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
PUBLIC HEARING

Hearing Regarding the Surveillance Program Operated Pursuant Section 702 of the Foreign Intelligence Surveillance Act

March 19, 2014

Renaissance Mayflower Hotel – Grand Ballroom
1127 Connecticut Ave NW, Washington DC

AGENDA

08:45 **Doors Open**

09:00 - 09:10 **Introductory Remarks (David Medine, PCLOB Chairman)**

09:15 - 10:45 **Panel I: Government Perspective on Section 702 Foreign Intelligence Surveillance Act**

Panelists:

- **James A. Baker (General Counsel, Federal Bureau of Investigation)**
- **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)**

10:45 - 11:00 **Break**

11:00 - 12:30 **Panel II: Legal Issues with 702 Foreign Intelligence Surveillance Act**

***Panelists*:**

- **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)**

12:30 - 1:45 **Lunch Break (on your own)**

Panel III: Transnational and Policy Issues

***Panelists*:**

- **John Bellinger (Partner, Arnold & Porter)**
- **Dean C. Garfield (President and CEO, Information Technology Industry Council)**

1:45 - 3:45

- **Laura Pitter (Senior National Security Researcher, Human Rights Watch)**
- **Eric Posner (Professor of Law, University of Chicago Law School)**
- **Ulrich Sieber (Director, Max Planck Institute for Foreign and International Criminal Law, Freiburg/Germany)**
- **Christopher Wolf (Partner, Hogan Lovells)**

3:45 **Closing Comments (David Medine, PCLOB Chairman)**

All Affiliations are listed for identification purposes only.

ANNEX F

Request for Public Comments on Board Study

The Federal Register

The Daily Journal of the United States Government

56952 Federal Register/Vol. 78, No. 179/Monday, September 16, 2013/Notices
PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

[Notice–PCLOB–2013–06; Docket No. 2013– 0005; Sequence No. 6]

Notice of Hearing

A Notice by the Privacy and Civil Liberties Oversight Board on 10/25/2013

Action

Notice Of A Hearing.

Summary

The Privacy and Civil Liberties Oversight Board (PCLOB) will conduct a public hearing with current and former government officials and others to address the activities and responsibilities of the executive and judicial branches of the federal government regarding the government's counterterrorism surveillance programs. This hearing will continue the PCLOB's study of the federal government's surveillance programs operated pursuant to Section 215 of the USA PATRIOT Act and Section 702 of Foreign Intelligence Surveillance Act. Recommendations for changes to these programs and the operations of the Foreign Intelligence Surveillance Court will be considered at the hearing to ensure that counterterrorism efforts properly balance the need to protect privacy and civil liberties. Visit www.pclob.gov for the full agenda closer to the hearing date. This hearing was re-scheduled from October 4, 2013, due to the unavailability of witnesses as a result of the federal lapse in appropriations.

DATES:

Monday, November 4, 2013; 9:00 a.m.-4:30 p.m. (Eastern Standard Time).

Comments:

You may submit comments with the docket number PCLOB-2013-0005; Sequence 7 by the following method:

- *Federal eRulemaking Portal:* Go to http://www.regulations.gov. Follow the on-line instructions for submitting comments.
- Written comments may be submitted at any time prior to the closing of the docket at 11:59 p.m. Eastern Time on November 14, 2013. This comment period has been extended from October 25, 2013, as a result of the new hearing date.

All comments will be made publicly available and posted without change. Do not include personal or confidential information.

ADDRESSES:

Mayflower Renaissance Hotel Washington, 1127 Connecticut Ave. NW., Washington DC 20036. Facility's location is near Farragut North Metro station.

FOR FURTHER INFORMATION CONTACT:

Susan Reingold, Chief Administrative Officer, 202-331-1986. For email inquiries, please email info@pclob.gov.

SUPPLEMENTARY INFORMATION:

Procedures for Public Participation

The hearing will be open to the public. Individuals who plan to attend and require special assistance, such as sign language interpretation or other reasonable accommodations, should contact Susan Reingold, Chief Administrative Officer, 202-331-1986, at least 72 hours prior to the meeting date.

Dated: October 21, 2013.

Diane Janosek,
Chief Legal Officer, Privacy and Civil Liberties Oversight Board.

https://www.federalregister.gov/articles/2013/10/25/2013-25103/notice-of-hearing

ANNEX G

Reopening the Public Comment Period

At the March 19, 2014 public hearing, the Privacy and Civil Liberties Oversight Board (PCLOB) Chairman announced the reopening of the public comment period to allow for additional submissions in light of the information discussed and submitted during the March 19, 2014 public hearing. All comments received were posted to the PCLOB Docket No. 2013-005 and can be viewed at http://www.regulations.gov/#!docketDetail;D=PCLOB-2013-0005.

ANNEX H

Index to Public Comments received to PCLOB Docket No. 2013-005 on www.regulations.gov.

Comments Received on PCLOB Docket No. 2013-005

Can also view all entries at: http://www.regulations.gov/#!docketDetail;D=PCLOB-2013-0005

Entity submitting comment - listed in order as they appear on docket	**Go to URL to see comment on Docket**	**Additional details:**
Global Network Initiative (GNI)	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0027	GNI is a multi-stakeholder group of companies, civil society organizations (including human rights and press freedom groups), investors and academics
Private individual	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0044	
Nathan Sales	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0022	Panel member at PCLOB Workshop

European Digital Rights (EDRi) and the Fundamental Rights European Experts Group (FREE)	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0024	EDRi is an association of 35 digital civil rights organizations from 21 European countries. FREE is an association whose focus is on monitoring, teaching and advocating in the EU.
Michael Davidson	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0020	Panel member at PCLOB Workshop
Project On Government Oversight (POGO), National Security Counselors, and OpenTheGovernment.org	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0029	
Center for National Security Studies	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0033	

Michael Davidson-second submission	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0028	Providing the July 30th opinion of the U.S. Court of Appeals for the Fifth Circuit in In re: Application of the United States of America for Historical Cell Site Data, No. 11-20884
Mr Juan Fernando López Aguilar, Chair of the European Parliament's Civil Liberties, Justice and Home Affairs Committee	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0059	
Ashkan Soltani	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0023	Panel member at PCLOB Workshop
Alliance for Justice	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0035	
Alan Charles Raul	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0065	Has four attachments
"Three former intelligence professionals - all former employees of the National Security Agency"	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0053	Statement submitted
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0014	

Coalition of 53 groups- letter	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0038	This is an updated coalition letter to PCLOB
The Constitution Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0009	Sharon Bradford Franklin was Panel member at PCLOB Workshop
Computer and Communications Industry Association	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0025	
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0017	
Electronic Frontier Foundation	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0030	
BSA /The Software Alliance Computer & Communications Industry Association (CCIA)/ Information Technology Industry Council (ITI)/ SIIA (Software & Information Industry Association)/ TechNet	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0061	

Ashkan Soltani	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0039	Revised submission, was a panel member at PCLOB Workshop
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0005	
Daniel J. Weitzner, Massachusetts Institute of Technology	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0040	Panel member at PCLOB Workshop
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0052	
Access - AccessNow.org	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0048	
Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0057	
Privacy Times	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0011	
Electronic Privacy Information Center	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0064	Marc Rotenberg was a panel member at PCLOB Workshop

ACLU Statement	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0032	Jameel Jaffer was a panel member at PCLOB Workshop and Hearing
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0046	
Mark Sokolow	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0018	
GodlyGlobal.org	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0019	A faith-based initiative based in Switzerland with global scope
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0041	
ACCESS NOW	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0047	Second posting
Coalition letter	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0010	
Center for Democracy & Technology, Gregory T. Nojeim	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0034	Gregory Nojeim was a panel member at PCLOB Workshop
Reporters Committee for Freedom of the Press	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0063	

Center for National Security Studies	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0060	
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0037	
Brennan Center for Justice's Liberty and National Security Program	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0049	Elizabeth Goitein was a panel member at PCLOB Workshop
Jeffrey H. Collins	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0043	
Jeffrey H. Collins	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0045	Amended
Steven G. Bradbury	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0012	Panel member at PCLOB Workshop
Human Rights Watch	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0036	
"Human rights organizations and advocates from around the world"	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0042	Dozens of countries represented

Steven M. Bellovin	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0021	Panel member at PCLOB Workshop
Board of the U.S. Public Policy Council of the Association for Computing Machinery	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0026	Eugene H. Spafford was a panel member at PCLOB Hearing
Private citizen	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0066	
Caspar Bowden, Prepared for the European Parliament LIBE Committee	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0068	
Stephanie Pell	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0069	Panel member at PCLOB hearing
Congressman Bennie Thompson	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0071	Ranking Member, Committee on Homeland Security
Government Accountability Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0072	
Jennifer S. Granick	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0090	
Private citizen anonymous	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0007	

Information Technology Industry Council	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0074	
Stephanie Pell	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0070	Panel member at PCLOB hearing
BSA | The Software Alliance, Computer & Communications Industry Association (CCIA), Information Technology Industry Council (ITI), SIIA – Software & Information Industry Association, TechNet	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0067	
Jameel Jaffer	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0082	Panel member at PCLOB workshop and hearing
Government Accountability Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0083	
Martin Scheinin	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0085	Panel member at PCLOB hearing
Marshall Erwin	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0089	
Electronic Frontier Foundation	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0100	

Christopher Wolf	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0087	Panel member at PCLOB hearing
Thomas Drake	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0102	Panel member at PCLOB hearing
Laura Pitter	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0079	Panel member at PCLOB hearing
NSA Director of Civil Liberties and Privacy Office Report on NSA's Implementation of FISA Section 702	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0101	
Laura K. Donohue	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0075	Panel member at PCLOB hearing
Julian G. Ku	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0086	Panel member at PCLOB hearing
PEN American Center	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0094	
Eric A. Posner	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0081	Panel member at PCLOB hearing
Hogan Lovell	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0088	
National Association of Criminal Defense Lawyers	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0091	

Ben Davis	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0084	
Amnesty International USA and the American Civil Liberties Union	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0096	
Brennan Center for Justice	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0093	
Christopher Wolf	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0078	Panel member at PCLOB hearing
Kevin Cahill	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0105	
The Constitution Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0099	
Center for Democracy & Technology	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0095	
Dean C. Garfield	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0077	Panel member at PCLOB hearing
Laura Donohue	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0104	Panel member at PCLOB hearing
Center for National Security Studies	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0098	
John B. Bellinger, III	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0076	Panel member at PCLOB hearing

William Binney, Thomas Drake, Edward Loomis, J. Kirk Wiebe, Ray McGovern, Elizabeth Murray, Coleen Rowley, Daniel Ellsberg	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0103	
Rachel Levinson-Waldman	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0080	Panel member at PCLOB hearing
Center for Democracy and Technology, Center for National Security Studies, National Association of Criminal Defense Lawyers, OpenTheGovernment.Org, The Constitution Project	http://www.regulations.gov/#!documentDetail;D=PCLOB-2013-0005-0106	

This Report is the Privacy and Civil Liberties Oversight Board's effort to analyze and review actions the executive branch takes to protect the Nation from terrorism to ensure the proper balancing of these actions with privacy and civil liberties.

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

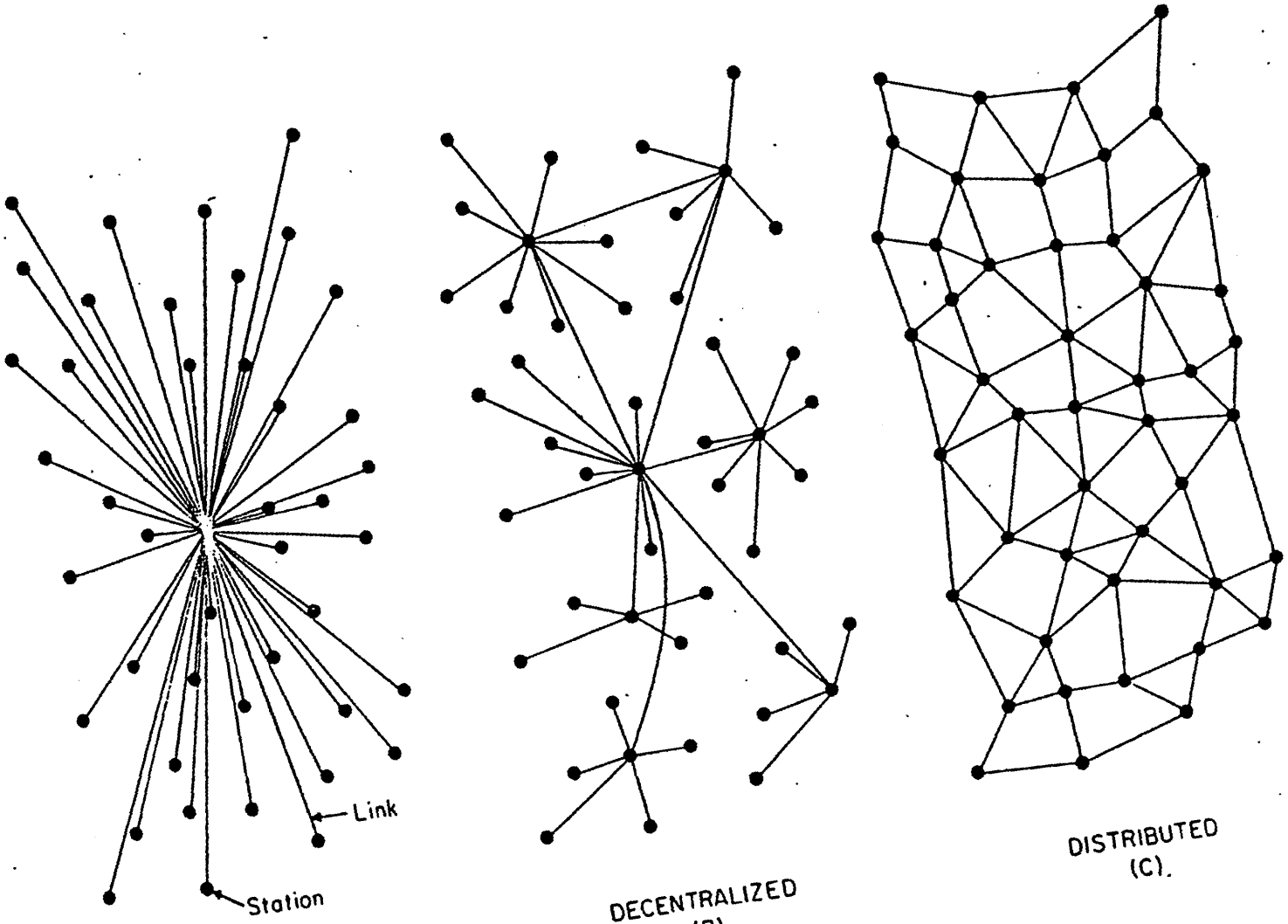


FIG. 1 – Centralized, Decentralized and Distributed Networks

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, $1\frac{1}{2}$, 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

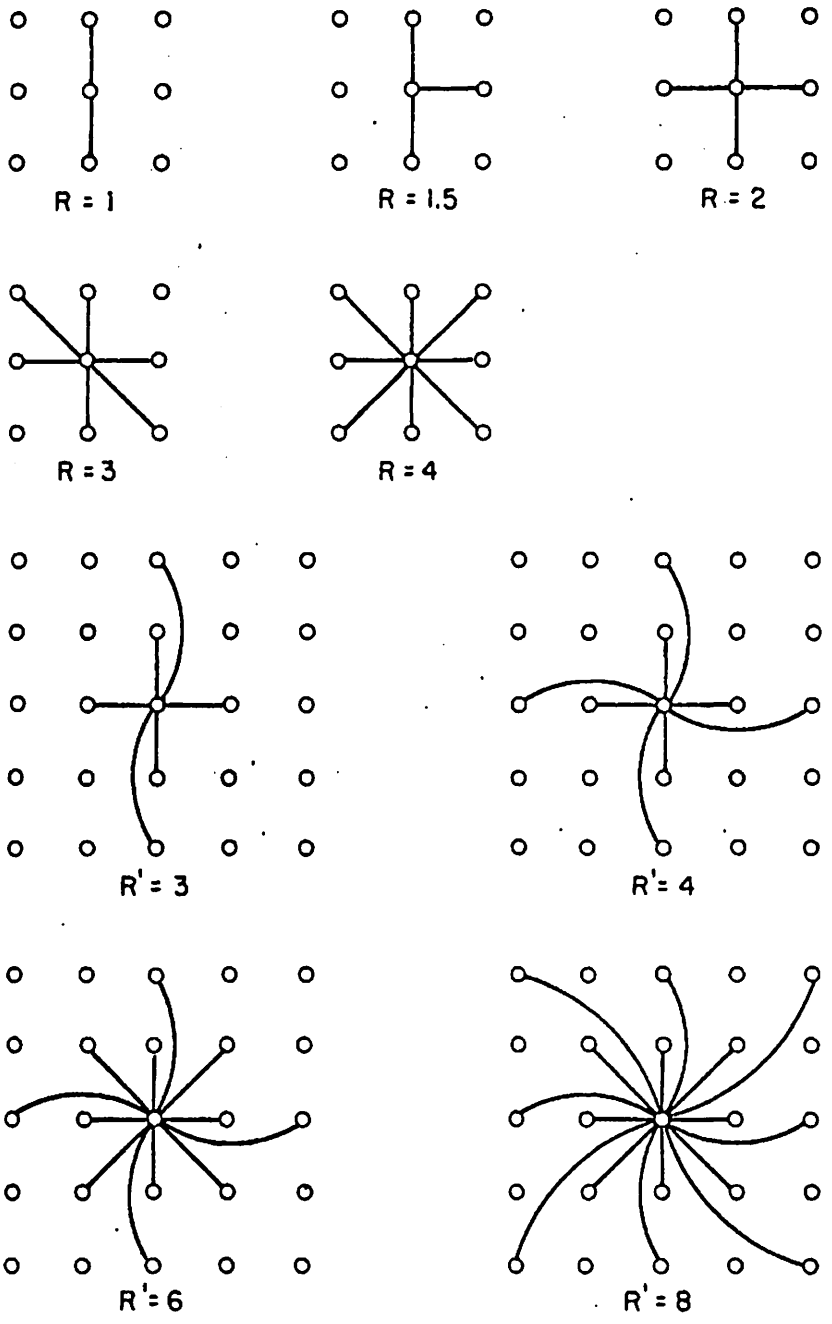


FIG. 2 – Definition of Redundancy Level

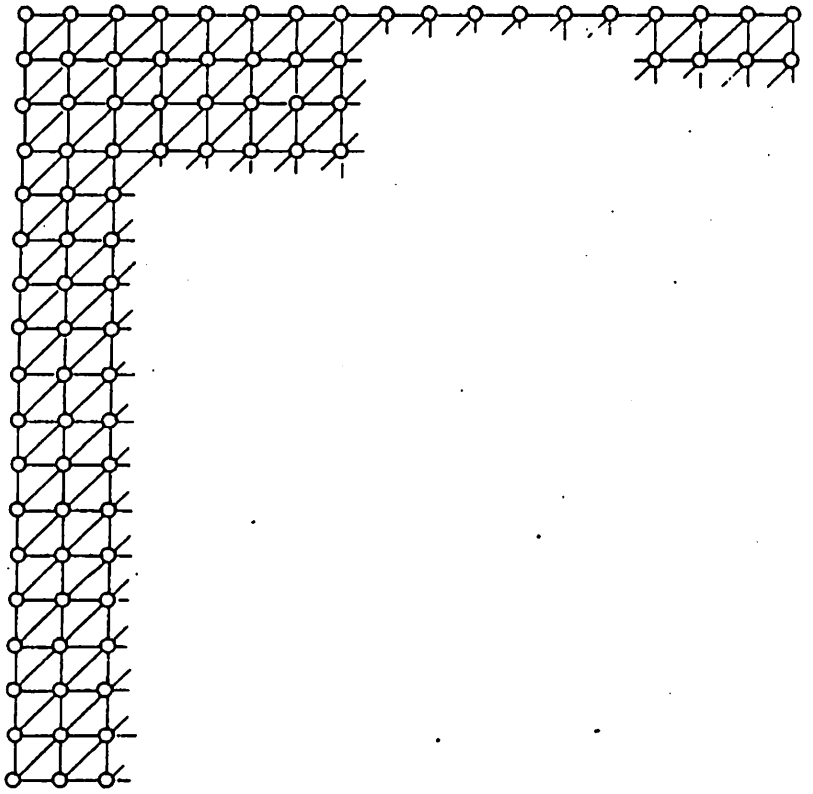


FIG. 3 — An Array of Stations

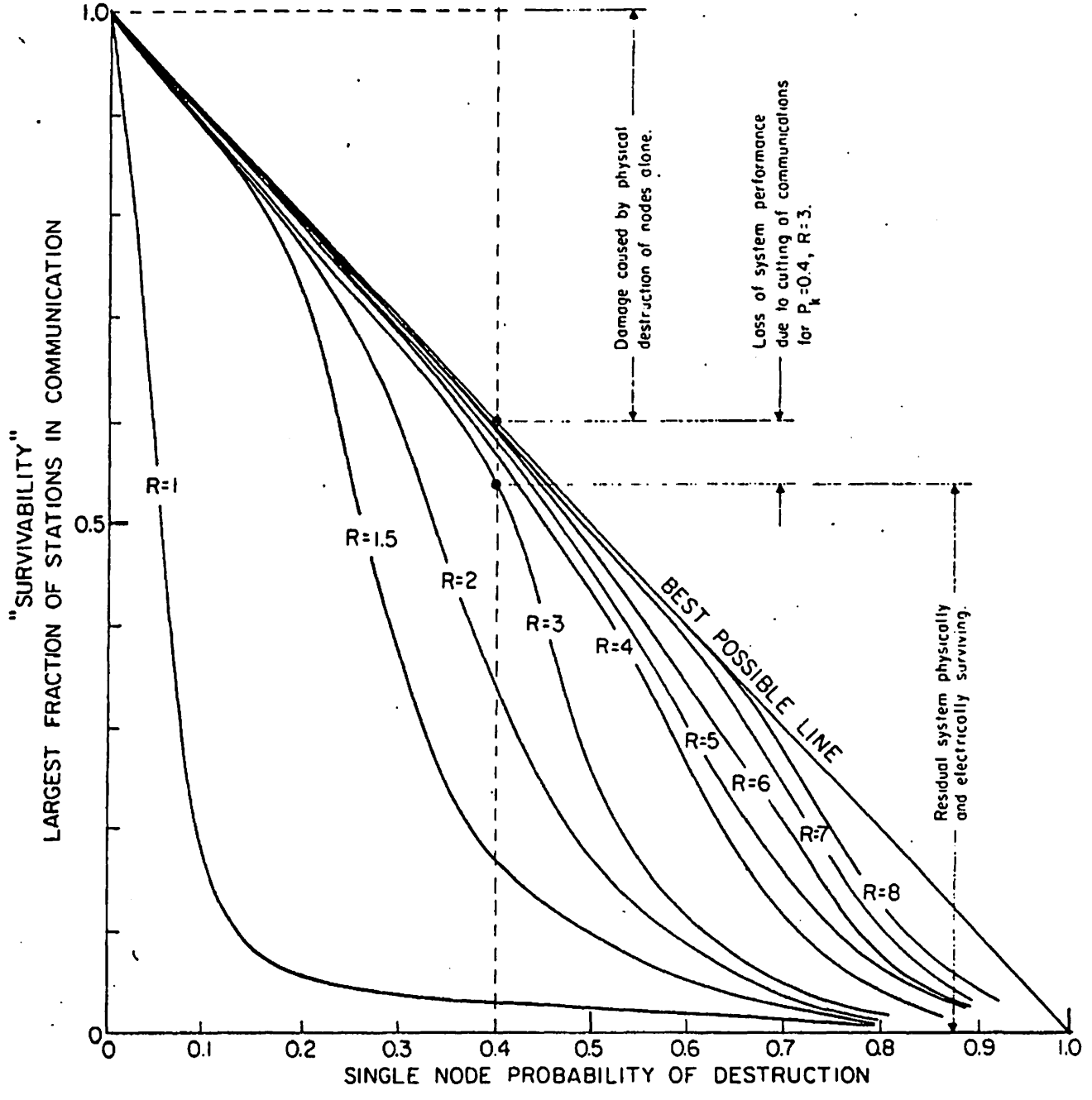


FIG. 4 — Perfect Switching in a Distributed Network — Sensitivity to Node Destruction, 100% of Links Operative.

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

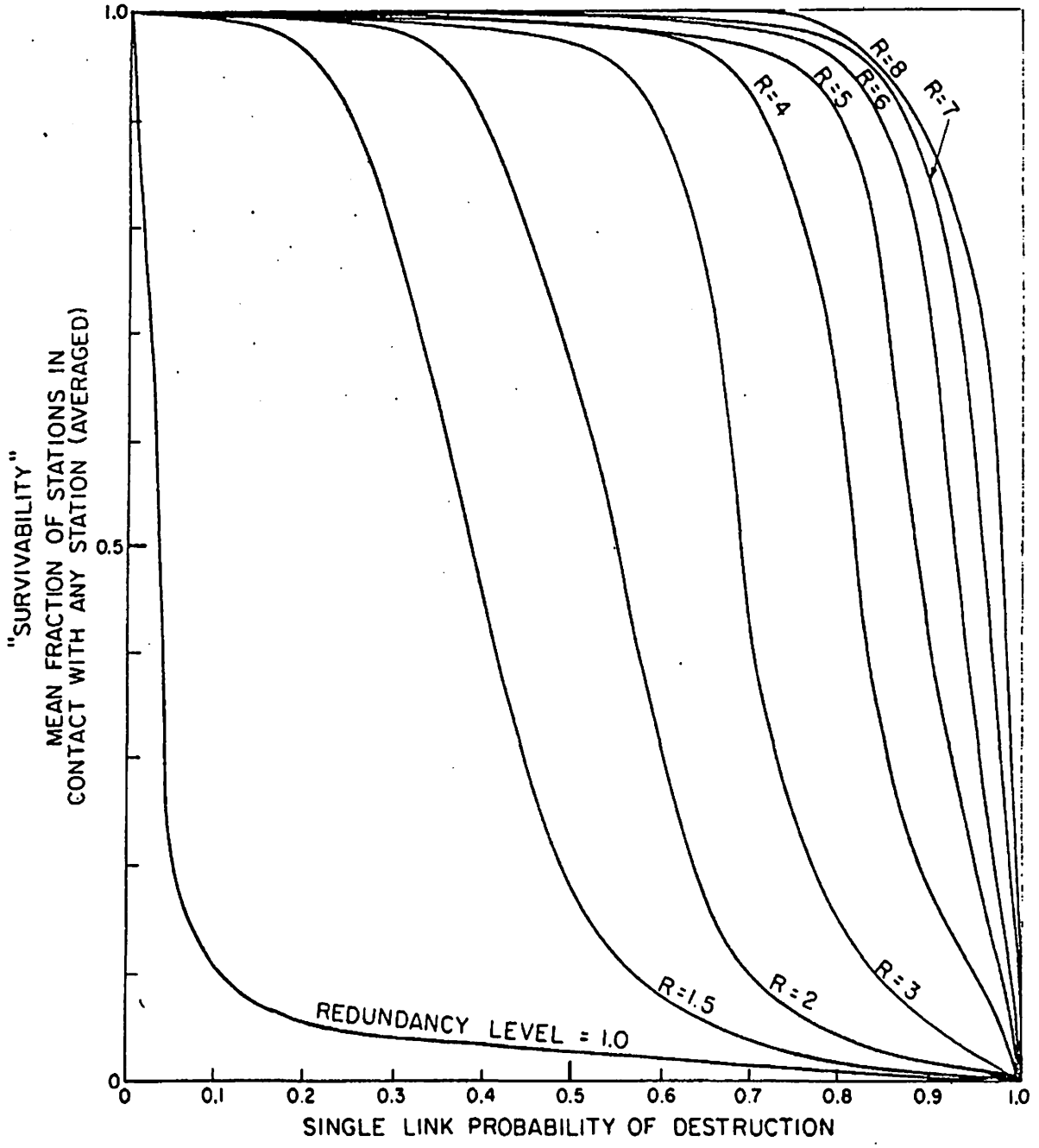


FIG. 5 — Perfect Switching in a Distributed Network — Sensitivity to Link Destruction, 100% of Nodes Operative.

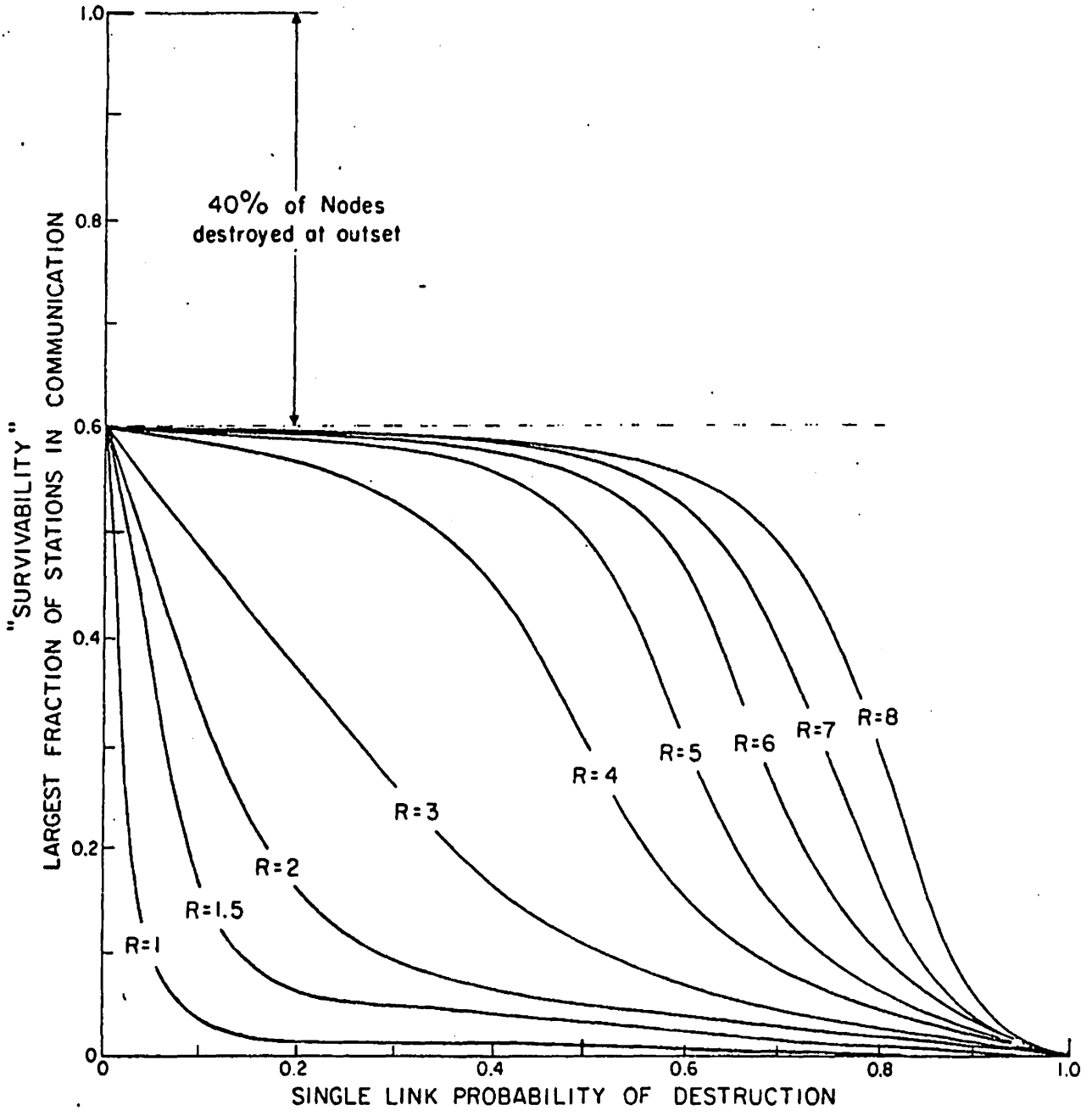


FIG. 6 – Perfect Switching in a Distributed Network — Sensitivity to Link Destruction After 40% Nodes Are Destroyed.

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

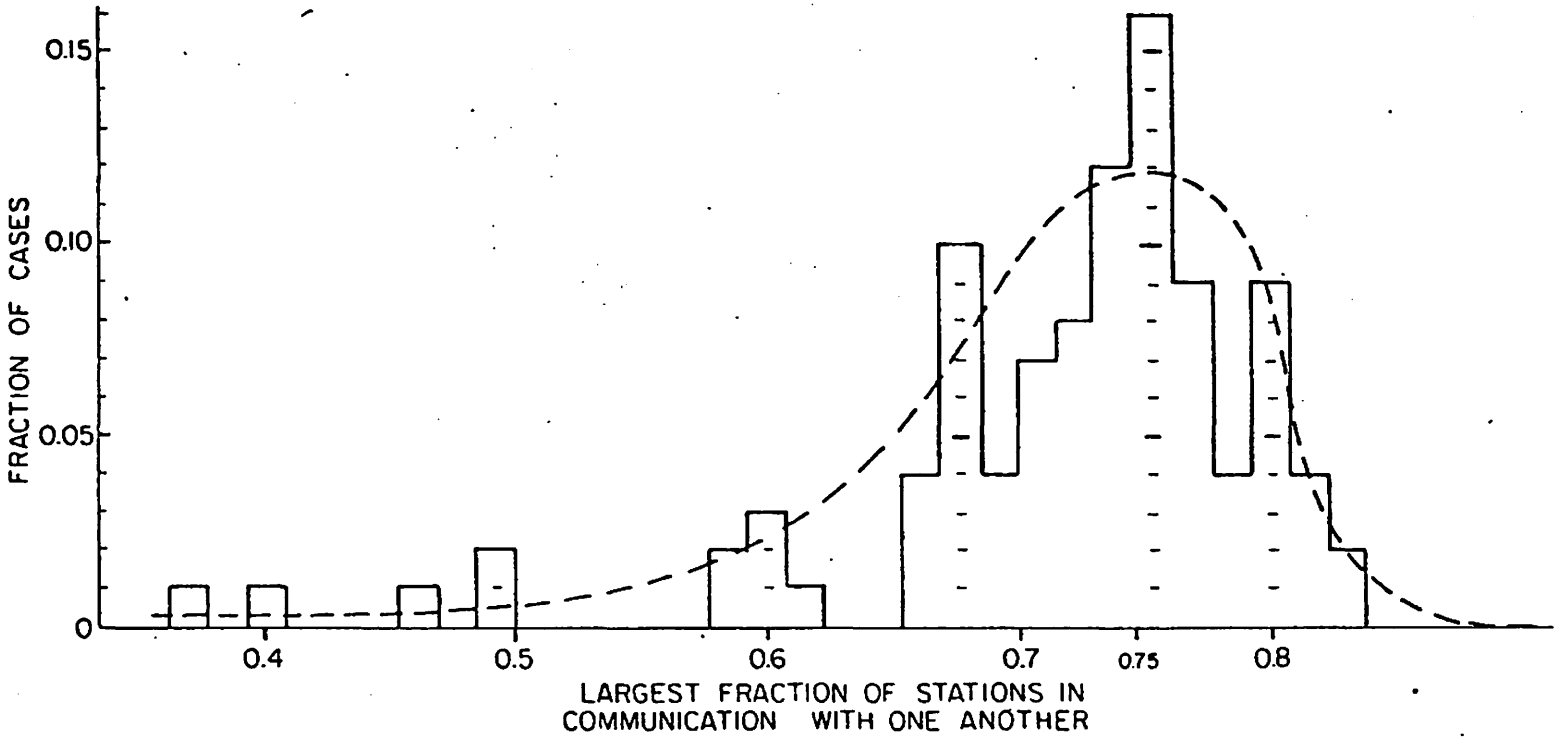


FIG. 7 — Probability Density Distribution of Largest Fraction of Stations in Communication
Perfect Switching, R = 3, 100 Cases, 80% Node Survival, 65% Link Survival.

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

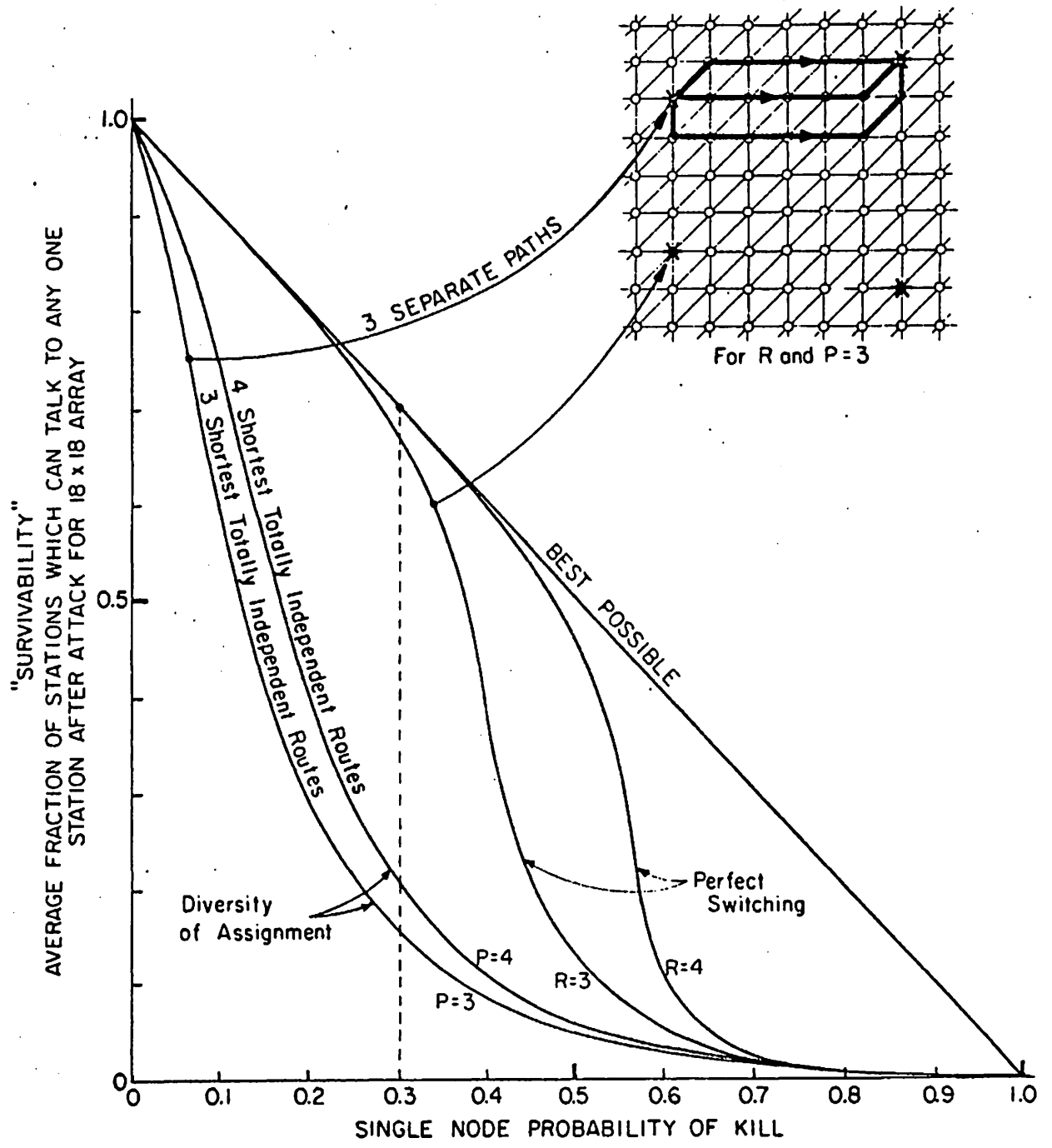


FIG. 8 – Diversity of Assignment vs. Perfect Switching in a Distributed Network.

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

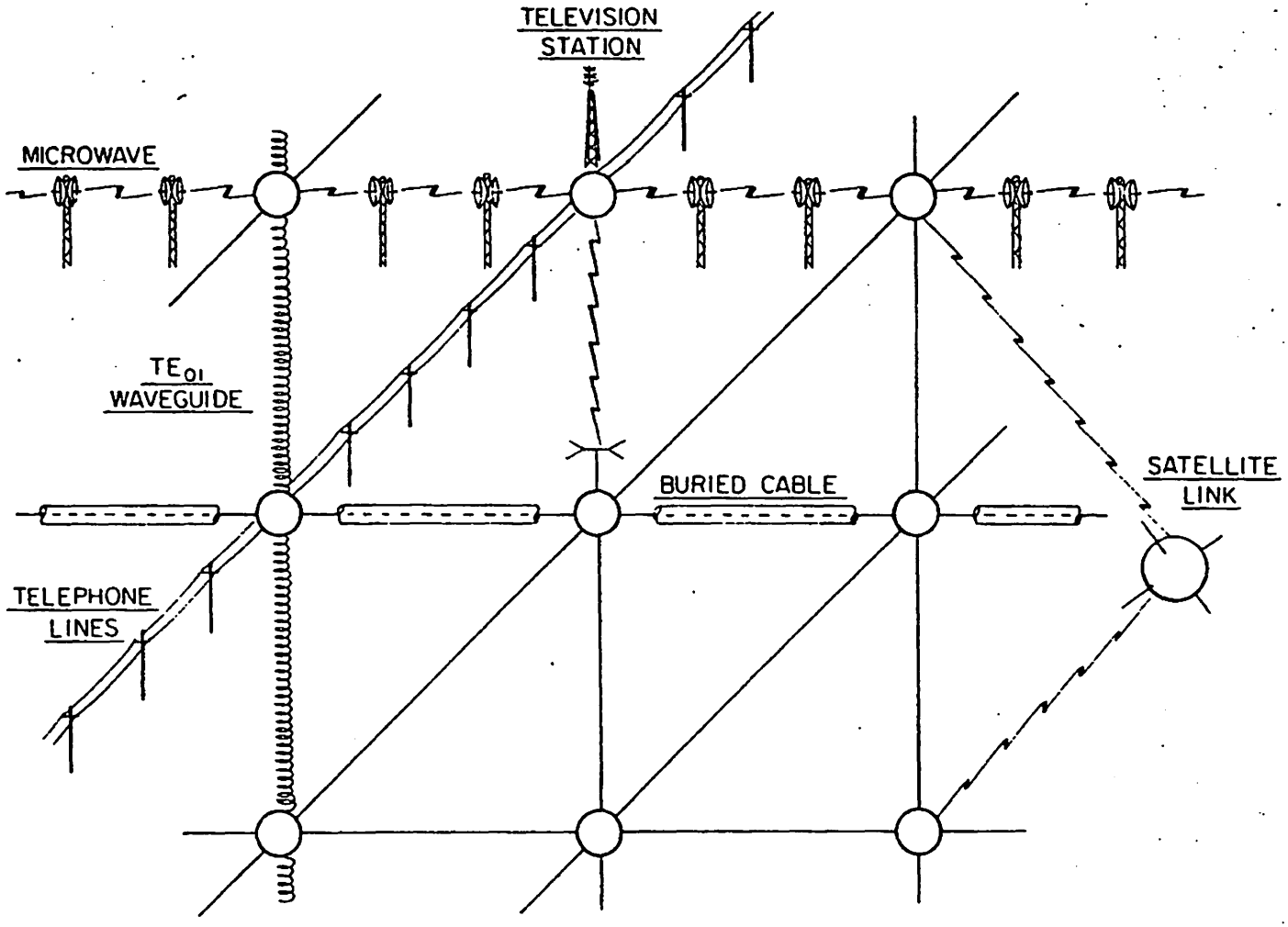


FIG. 9 - All Digital Network Composed of Mixture of Links

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

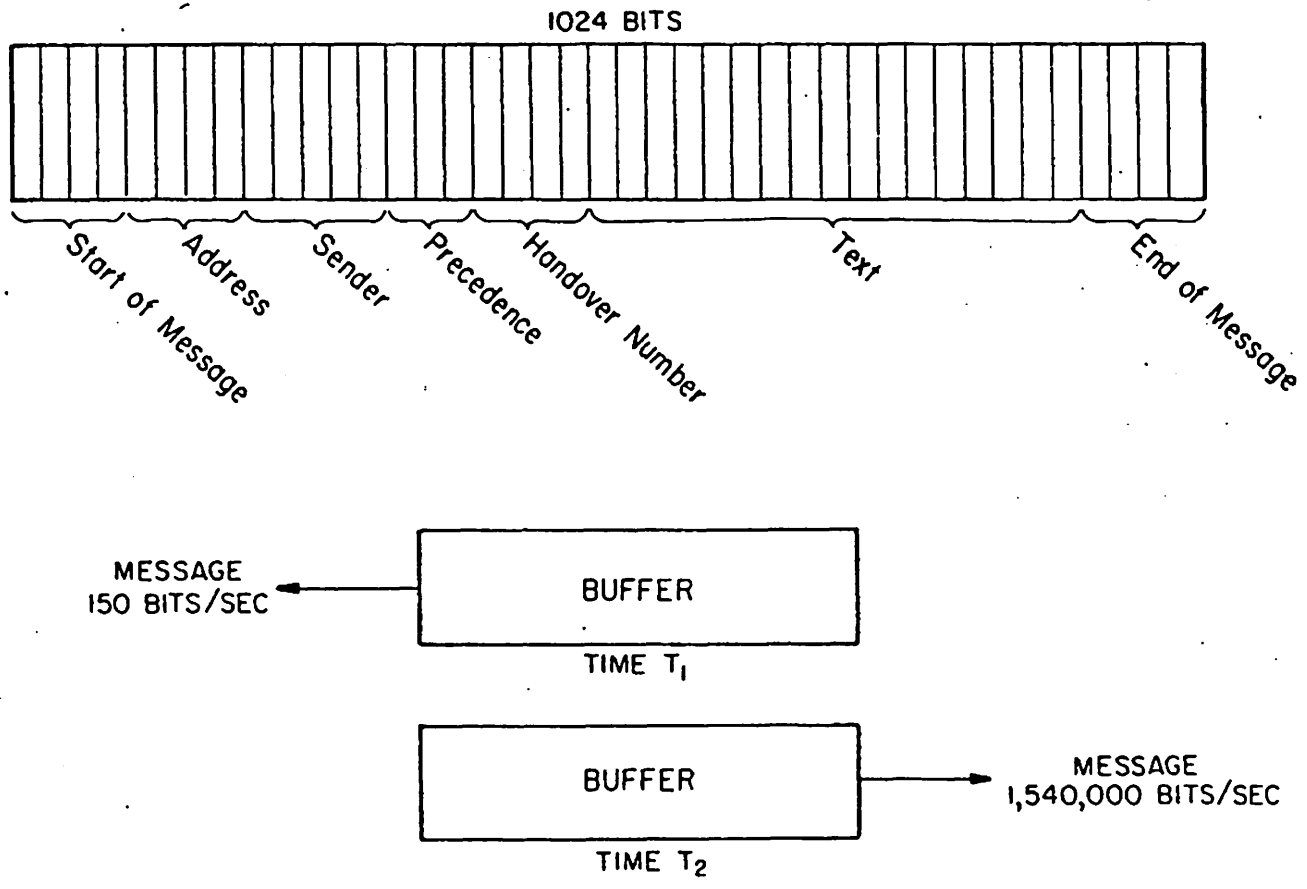


FIG. 10 — Message Block

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.

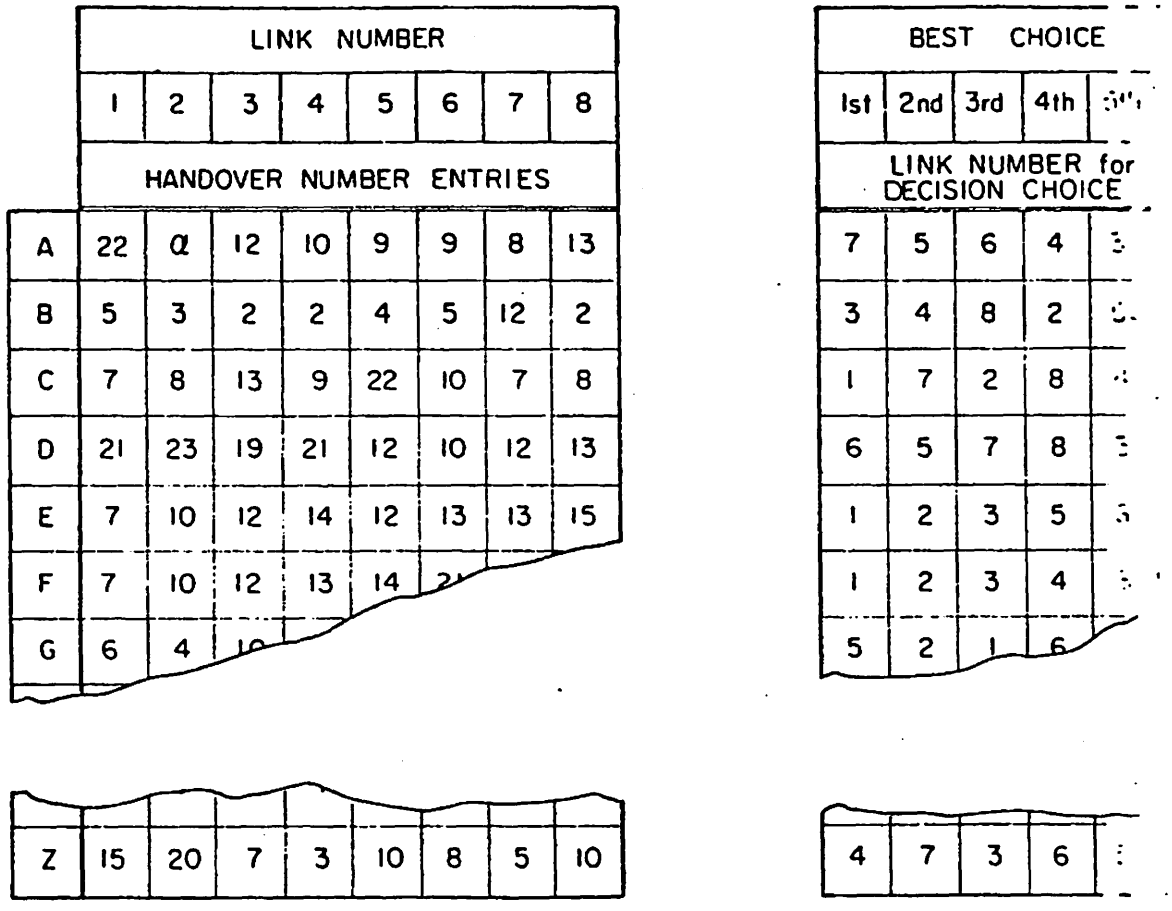
INDUCTIVE DETERMINATION OF BEST PATH

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	5
	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

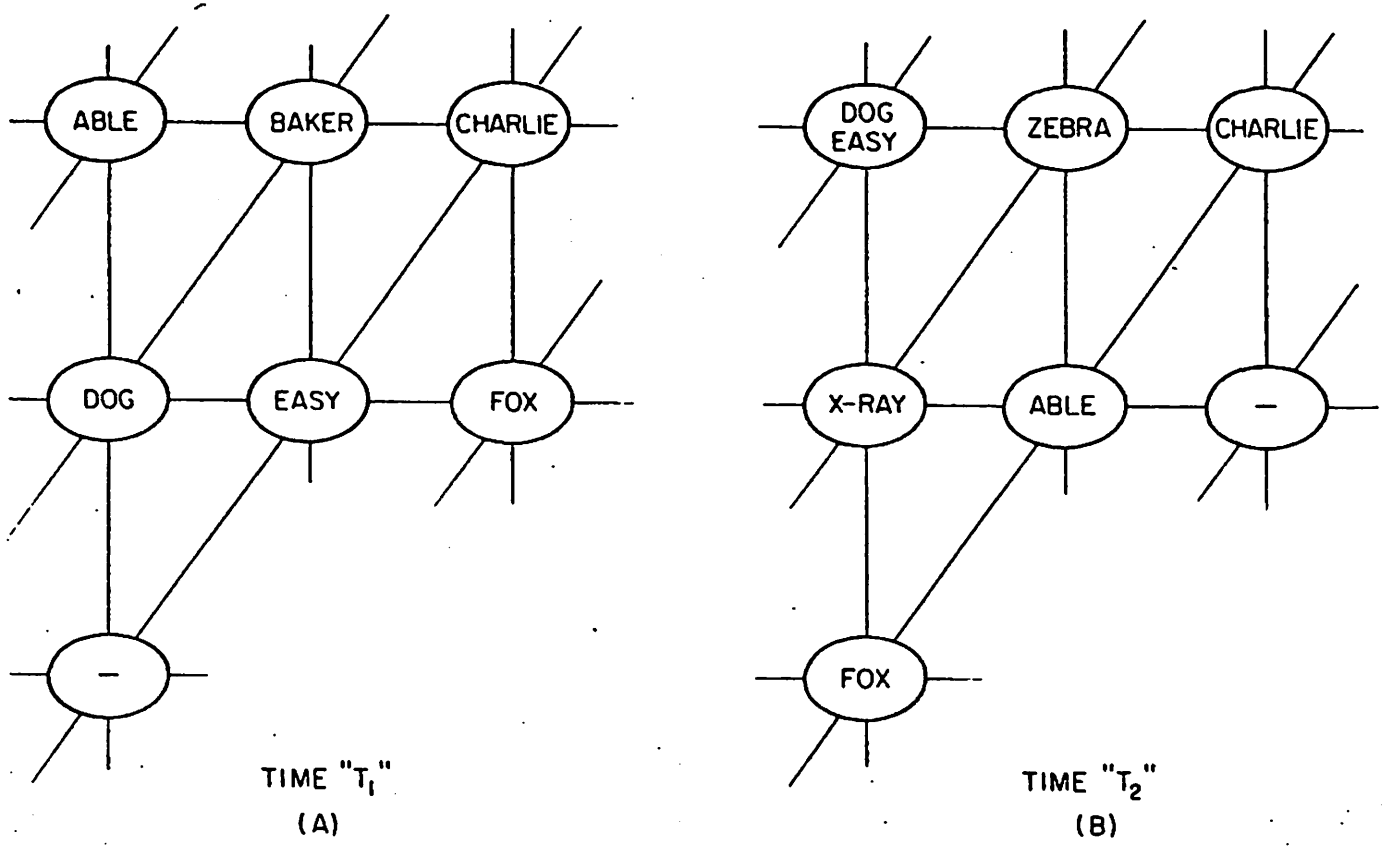


FIG. 12 – Adaptability to Change of User Location

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?