No. 20-1191

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

WIKIMEDIA FOUNDATION,

Plaintiff–Appellant,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants–Appellees.

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

JOINT APPENDIX—VOLUME 4 OF 7 (JA2353–JA2889)

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

Counsel for Defendants–Appellees

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

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

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

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

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

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

JOINT APPENDIX
Table of Contents

VOLUME 1

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

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

Exhibits to Wikimedia Foundation's Motion to Compel

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

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

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

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

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

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

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

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

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

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

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

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

Opinion & Order Denying Wikimedia Foundation's Motion to Compel

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

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

Exhibits to Defendants' Motion for Summary Judgment

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

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

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

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

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

VOLUME 2

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

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

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

VOLUME 3

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

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

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

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

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

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

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

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

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

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

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

VOLUME 4

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

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

Exhibit 12: Wikimedia document compiling German-user-

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

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

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

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

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

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

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

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

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

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

VOLUME 5

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Exhibit 42: Wikimedia's Supplemental Exhibit C in response

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

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

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

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

VOLUME 6

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

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

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

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

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

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

Exhibit 11: Relevant Portions of the Deposition of Michelle

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

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

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

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

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

VOLUME 7

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

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

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

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

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

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

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

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

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

Opinion & Order Granting Defendants' Motion for Summary Judgment

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

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

Wikimedia Foundation's Notice of Appeal

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

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

Plaintiff's Exhibit 11

Steward requests/Global permissions

< Steward requests

This is an archived version of this page, as edited by Rusliko (talk | contribs) at 11:21, 8 September 2017. It may differ significantly from the current version.

(diff) ← Older revision | Latest revision (diff) | Newer revision → (diff)

← Requests and proposals **Steward requests** (Global permissions) latest archive→

This page hosts requests for global permissions. To make a request, read the relevant policy (global rollback, global sysop, global rename, …) and make a request below. Explain why membership is needed for that group, and detail prior experience or qualifications.

This is not a vote and any active Wikimedia editor may participate in the discussion.

Successful global rollback requests require no fewer than 5 days of discussion, while successful global renamer and global sysop discussions require no fewer than 2 weeks.

Search in this page hierarchy

Contents

Requests for global rollback permissions
Global rollback for Asaf (WMF)
Requests for global sysop permissions
Requests for global IP block exemption
Global IP block exempt for TemTem
Requests for global rename permissions
Requests for other global permissions
remove global OTRS member for Wikitanvir
remove global OTRS member for Panyd
remove global OTRS member for Kh80
See also

Cross-wiki requests

- CheckUser information
- Global blocks/locks
- Permissions (global)
- Permissions (bot)
- Permissions (other)
- Username changes/ usurpation requests
- Miscellaneous requests
- URL blacklisting
- Title/username blacklisting
- Email blacklisting

Meta-Wiki requests

- CheckUser information
- Deletion
- Permissions
- Requests for help

Requests for global rollback permissions

Please be sure to follow the instructions below:

Your request might be rejected if you don't follow the instructions, and not doing so would reflect poorly on your suitability. Please also review the Global rollback policy.

Please note that global rollbacker discussions are not votes. Comments must present specific points in favor of or against a user's approval.

Instructions for making a request **[Expand]**

Global rollback for Asaf (WMF)

Status: **In progress**

- Global user: Asaf (WMF) (edits • CA • global groups (https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/Asaf_(WMF)?user-reason=%5B%5BSpecial:Permalink/17203746%5D%5D) • crosswiki-ness (h

Rationale: I work in many wikis, and every now and then encounter vandalism (especially on old pages I still watch), like this (https://meta.wikimedia.org/w/index.php?title=Grants%3APEG%2FWM_CZ%2FCommunities&type=revision&diff=17194610&oldid=10953431), where the rollback function would be useful. I am a longtime trusted user and staffer, and I humbly suggest there is zero risk in giving me the rollback tool so I can rollback vandalism when I encounter it, even though I'm not proactively patrolling most wikis. Also see this discussion (https://meta.wikimedia.org/wiki/Wikimedia_Forum#Standalone_rollbacker_permission.3F). Asaf (WMF) (talk) 14:57, 6 September 2017 (UTC)

Not ending before 11 September 2017 14:57 UTC

- Do you have a community account in addition to a WMF one? Ruslik (talk) 18:42, 6 September 2017 (UTC)

  Certainly. This is it. Also linked from the first line under About me on my staff account. Ijon (talk) 22:46, 6 September 2017 (UTC)

  I think you should request global rollback for your volunteer account. We are not in business here assigning permissions to staff accounts. If you want it for your staff account, you should ask someone in WMF. Ruslik (talk) 20:29, 7 September 2017 (UTC)

- I was under the impression that staff were supposed to keep non-work-related edits to articles to volunteer accounts, including reverting vandalism. Is that correct? --**Rschen7754** 00:13, 7 September 2017 (UTC)

yes, that is correct. I suppose the global rollback tool would be useful to me in *both* accounts. The example diff above is on an old gratg page, which I watch in my staff capacity, so I think rolling back the vandalism would have been fine under my staff account. I may well encounter random vandalism (say on article space) on some wiki I visit in the course of my work that would be more appropriately reverted through my volunteer account. I am happy to request separately under my volunteer account as well. Asaf (WMF) (talk) 18:59, 7 September 2017 (UTC)

- **Oppose** little to zero reverting of vandalism on smaller wiki's under the volunteer account. Not on the staff account either. Policy states the following: *For consideration, users must be demonstrably active in cross-wiki countervandalism or anti-spam activities (for example, as active members of the Small Wiki Monitoring Team) and make heavy use of revert on many wikis.* These criteria are certainly not met. Natuur12 (talk) 20:15, 7 September 2017 (UTC)

  This is somewhat unusual case. We can make an exception. Ruslik (talk) 20:29, 7 September 2017 (UTC)

- **Oppose** Given rationale applies to many users, but is still out of scope of global rollback. Sorry. --Krd 10:40, 8 September 2017 (UTC)

Requests for global sysop permissions

Please be sure to follow the instructions below:

Your request might be rejected if you don't follow the instructions, and not doing so would reflect poorly on your suitability.
Please also review the Global sysops policy.

Stewards
When you give someone global sysop rights, please list them on Users with global sysop access and ask them to subscribe to the global sysops mailing list.

Please note that global sysop discussions are not votes. Comments must present specific points in favor of or against a user's approval.

Instructions for making a request **[Expand]**

Requests for global IP block exemption

Please be sure to follow the instructions below:

Your request might be rejected if you don't follow the instructions. Please review Global IP block exemption.
Please note: Global IP block exemption does NOT make one immune to locally-created blocks of any sort, only *global* blocks.

Instructions for making a request **[Expand]**

Global IP block exempt for TemTem

Status: Done

- Global user: TemTem (edits • CA • global groups (https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/TemTem?user-reason=%5B%5BSpecial:Permalink/17203746%5D%5D) • crosswiki-ness (https://toc

Hello, I would like to use Tor while editing Wikimedia wikis, but it seems Wikimedia blocks all Tor exit nodes. I have to use Tor because the country where I live in, the Philippines, is under a "War on Drugs". Martial law is also declared in Mindanao, and still in effect. I am concerned that my government will take hard measures like spying on Filipino citizens and collaborating with the NSA. That's why I am using Tor to prepare if this happens. Thanks, --TemTem (talk) 00:50, 3 September 2017 (UTC)

Is this your first account? Ruslik (talk) 17:33, 3 September 2017 (UTC)

Yes. TemTem (talk) 09:38, 4 September 2017 (UTC)

Is this a joke? I have been waiting for like four days and I still have no response? You don't trust me, fine, then I will gain your trust. by editing without tor. but remove the "If a Tor exception is granted to you and you don't have an account yet, the steward will also create one for you and you'll receive a temporary password to your email address" at "No open proxies", it seems its just a fantasy. TemTem (talk) 10:49, 8 September 2017 (UTC)

✓ **Done** Four days is not a long time. Ruslik (talk) 11:21, 8 September 2017 (UTC)

Requests for global rename permissions

Please be sure to follow the instructions below:

Your request might be rejected if you don't follow the instructions, and not doing so would reflect poorly on your suitability.
Please also review the Global rename policy.

Stewards
When you give someone global rename rights, please add them to the list of global renamers and ask them to subscribe to the global renamers' mailing list.

Please note that global renamer discussions are not votes. Comments must present specific points in favor of or against a user's approval.

Instructions for making a request **[Expand]**

Requests for other global permissions

Please be sure to follow the instructions below:

Your request might be rejected if you don't follow the instructions.

Instructions for making a request [Expand]

remove global OTRS member for Wikitanvir

Status: ▒ **Done**

- Global user: Wikitanvir (edits • CA • global groups (https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/Wikitanvir?user-reason=%5B%5BSpecial:Permalink/17203746%5D%5D) • crosswiki-ness (https://

Thx. --Krd 10:31, 5 September 2017 (UTC)

✓ **Done**.--HakanIST (talk) 10:59, 5 September 2017 (UTC)

remove global OTRS member for Panyd

Status: ▒ **Done**

- Global user: Panyd (edits • CA • global groups (https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/Panyd?user-reason=%5B%5BSpecial:Permalink/17203746%5D%5D) • crosswiki-ness (https://tools.wr

Thx. --Krd 09:27, 7 September 2017 (UTC)

✓ **Done**.--HakanIST (talk) 09:30, 7 September 2017 (UTC)

remove global OTRS member for Kh80

Status: ▒ **Done**

- Global user: Kh80 (edits • CA • global groups (https://meta.wikimedia.org/wiki/Special:GlobalGroupMembership/Kh80?user-reason=%5B%5BSpecial:Permalink/17203746%5D%5D) • crosswiki-ness (https://tools.wmfl

Thx. --Krd 11:26, 7 September 2017 (UTC)

✓ **Done**.--HakanIST (talk) 11:39, 7 September 2017 (UTC)

See also

- User groups — Information on user groups
- Global rights log — Log of global permissions changes
- Archive
  - 2010: 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
  - 2011: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
  - 2012: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
  - 2013: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
  - 2014: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
  - 2015: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
  - 2016: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
  - 2017: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12
  - 2018: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12

General requests for: help from a Meta sysop or bureaucrat • deletion (speedy deletions: local • multilingual) • URL blacklisting • new languages • interwiki map

Personal requests for: username changes • permissions (global) • bot status • adminship on Meta • an account on WMF wiki • CheckUser information (local) • local administrator help

Cooperation requests for: comments (local) (global) • translation • logos

Retrieved from "https://meta.wikimedia.org/w/index.php?title=Steward_requests/Global_permissions&oldid=17203746"

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of Use for details.

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

Plaintiff's Exhibit 12

Handling our user data - an appeal and a response

(Today we are posting an English translation of a blog post from German Wikipedians outlining concerns about the handling of Wikipedia user data, or metadata. Above that post you will find the Foundation's response to those concerns.)

Response to user appeal

In June this year, the Wikimedia Foundation (WMF) started to solicit community input on our privacy policy, and since September we have been inviting participation in a discussion of the draft for a new privacy policy. The purpose of this discussion has been to review and improve our privacy policy, and ensure that all members of the Wikimedia community have an opportunity to be heard and contribute.

This discussion has already helped us to understand the diverse range of views in our large, international community (each month, more than 75,000 users contribute to Wikimedia projects in more than 200 languages). As part of this discussion, about 120 German Wikipedia contributors who advocate for more stringent privacy rules have made a statement and published it on the German chapter's blog (English translation below). We welcome the contribution of these editors, and hope that the resulting discussion will strengthen the policy. However, while we hear and respect these concerns, the WMF was not invited to explain its position during the drafting of the statement, and so we'd like to do so here.

Existing practices

As the authors of the statement mention, the past year has seen increased global concern about privacy and the activities of intelligence agencies in both the US and Europe. The Wikimedia Foundation is extremely sensitive to those concerns, and we have taken several steps to address them, including joining activism here in the US, encrypting more traffic to and from the Wikimedia sites, and assuring readers that we have not been contacted under the surveillance programs at issue.

The Wikimedia Foundation also protects its readers by collecting very little information, particularly relative to most major websites. Editors who create an account do not have to connect their account to a real-world identity unless they choose to do so. It is possible to read and use the Wikimedia sites without providing your real name, home address, email address, gender, credit card or financial information. In all but a few cases (related to abuse prevention), we delete IP addresses of logged-in editors after 90 days. All in all, there is small incentive for governments to contact WMF and request information about Wikimedia users.

Requested changes

As part of the normal operation of a wiki, the Wikimedia sites have always published certain information about edits, particularly when the edit was made, and what page was edited. This information can be collected to make educated guesses about an account, such as what time zone an account is in (based on when edits occur).

One part of the statement asks that we limit public access to this editing information. This information is used in a variety of places, many of which are important to the health and

~~PROTECTED FOIA Confidential Treatment Request~~

functioning of our projects:

- Protecting against vandalism, incorrect and inappropriate content: There are several bots that patrol Wikipedia's articles that protect the site. Without public access to metadata, the effectiveness of these bots will be much reduced, and it is impossible for humans to perform these tasks at scale.
- Community workflows: Processes that contribute to the quality and governance of the project will also be affected: blocking users, assessing adminship nominations, determining eligible participants in article deletion discussions.
- Automated tools: Certain community-created tools that help perform high-volume editing (such as Huggle, for vandalism fighting on several wikis) will be broken without public access to this metadata.
- Research: Researchers around the world use this public metadata for analysis that is essential to the site and the movement's understanding of itself.
- Forking: Allowing others to fork is an important principle of the movement, and that requires some exposure of metadata about how articles were built, and by whom.

The Foundation has been open and transparent about these data publication practices for years, so we do not currently plan to make the requested changes. Nevertheless, we welcome the appeal as part of the wider community discussion regarding the Foundation's privacy policy.

The statement also asks that we implement a new policy on the Wikimedia Labs experimental development servers. The predecessor to Labs, called Toolserver, had a policy that prohibited volunteer-developed software if the software aggregated certain types of account information without consent. The terms of use for Labs allows such software to be taken down at the WMF's discretion, but does not prohibit it explicitly. We have suggested a clarification to the Labs terms of use in the Privacy Policy discussion, and will continue to discuss that there.

We invite anyone interested in Wikimedia Foundation's privacy policy to get involved in the ongoing consultation with the Wikimedia community. You can read more about that process in the blog post that announced it. The consultation process will continue through January 15, 2013.

Luis Villa

Deputy General Counsel, Wikimedia Foundation

(Translated blog post from Wikimedia Deutschalnd follows - from https://meta.wikimedia.org/wiki/Wikimedia_Blog/Drafts/Handling_our_user_data_-_an_appeal)

Handling our user data - an appeal

Preface (Wikimedia Deutschland)

For several months, there have been regular discussions on data protection and the way Wikimedia deals

~~PROTECTED FOIA Confidential Treatment Request~~

with it, in the German-speaking community – one of the largest non-English-speaking communities in the Wikimedia movement. Of course, this particularly concerns people actively involved in Wikipedia, but also those active on other Wikimedia projects.

The German-speaking community has always been interested in data protection. However, this particular discussion was triggered when the Deep User Inspector *tool on Tool Labs nullified a long-respected agreement in the Toolserver, that aggregated personalized data would only be available after an opt-in by the user.*

As the Wikimedia Foundation is currently reviewing its privacy policy and has requested feedback and discussion her by 15 January, Wikimedia Deutschland has asked the community to draft a statement. The text presented below was largely written by User:NordNordWest and signed by almost 120 people involved in German Wikimedia projects. It highlights the many concerns and worries of the German-speaking community, so we believe it can enhance the discussion on these issues. We would like to thank everyone involved.

This text was published in German simultaneously in the Wikimedia Deutschland-blog and in the Kurier, an analogue to the English "Signpost". This translation has been additionally placed on the talkpage of the WMF-privacy-policy-draft at Meta.

(preface Denis Barthel (WMDE) (talk), 20.12.)

Starting position

The revelations by Edward Snowden and the migration of programs from the Toolserver to Tool Labs prompted discussions among the community on the subject of user data and how to deal with it. On the one hand, a diverse range of security features are available to registered users:

- Users can register under a pseudonym.
- The IP address of registered users is not shown. Only users with CheckUser permission can see IP addresses.
- Users have a right to anonymity. This includes all types of personal data: names, age, background, gender, family status, occupation, level of education, religion, political views, sexual orientation, etc.
- As a direct reaction to Snowden's revelations, the HTTPS protocol has been used as standard since summer 2013 (see m:HTTPS), so that, among other things, it should no longer be visible from outside which pages are called up by which users and what information is sent by a user.

On the other hand, however, all of a user's contributions are recorded with exact timestamps. Access to this data is available to everyone and allows the creation of user profiles. While the tools were running on the Toolserver, user profiles could only be created from aggregated data with the consent of the user concerned (opt-in procedure). This was because the Toolserver was operated by Wikimedia Deutschland and therefore subject to German data protection law, one of the strictest in the world. However, evaluation tools that were independent of the Foundation and any of its chapters already existed.

One example is Wikichecker, which, however, only concerns English-language Wikipedia. The migration of programs to ToolLabs, which means that they no longer have to function in accordance with German data protection law, prompted a survey of whether a voluntary opt-in system should still be mandatory for

~~PROTECTED FOIA Confidential Treatment Request~~

X!'s Edit Counter or whether opt-in should be abandoned altogether. The survey resulted in a majority of 259 votes for keeping opt-in, with 26 users voting for replacing it with an opt-out solution and 195 in favor of removing it completely. As a direct reaction to these results, a new tool – Deep User Inspector – was programmed to provide aggregated user data across projects without giving users a chance to object. Alongside basic numbers of contributions, the tool also provides statistics on, for example, the times on weekdays when a user was active, lists of voting behavior, or a map showing the location of subjects on which the user has edited articles. This aggregation of data allows simple inferences to be made about each individual user. A cluster of edits on articles relating to a certain region, for example, makes it possible to deduce where the user most probably lives.

Problems

Every user knows that user data is recorded every time something is edited. However, there is a significant difference between a single data set and the aggregated presentation of this data. Aggregated data means that the user's right to anonymity can be reduced, or, in the worst case, lost altogether. Here are some examples:

- A list of the times that a user edits often allows a deduction to be made as to the time zone where he or she lives.
- From the coordinates of articles that a user has edited, it is generally possible to determine the user's location even more precisely. It would be rare for people to solely edit area X, when in fact they came from area Y.
- The most precise deductions can be made by analyzing the coordinates of a photo location, as it stands to reason that the user must have been physically present to take the photo.
- Places of origin and photo locations can reveal information on the user's means of transport (e.g. whether someone owns a car), as well as on his or her routes and times of travel. This makes it possible to create movement profiles on users who upload a large number of photos.
- Time analyses of certain days of the year allow inferences to be drawn about a user's family status. It is probable, for example, that those who tend not to edit during the school holidays are students, parents or teachers.
- Assumptions on religious orientation can also be made if a user tends not to edit on particular religious holidays.
- Foreign photo locations either reveal information about a user's holiday destination, and therefore perhaps disclose something about his or her financial situation, or suggest that the user is a photographer.
- If users work in a country or a company where editing is prohibited during working hours, they are particularly vulnerable if the recorded time reveals that they have been editing during these hours. In the worst-case scenario, somebody who wishes to harm the user and knows extra information about his or her life (which is not unusual if someone has been an editor for several years) could pass this information on to the user's employer. Disputes within Wikipedia would thus be carried over into real life.

Suggestions

Wikipedia is the fifth most visited website in the world. The way it treats its users therefore serves as an important example to others. It would be illogical and ridiculous to increase user protection on the one

~~PROTECTED FOIA Confidential Treatment Request~~

hand but, on the other hand, to allow users' right to anonymity to be eroded. The most important asset that Wikipedia, Commons and other projects have is their users. They create the content that has ensured these projects' success. But users are not content, and we should make sure that we protect them. The Wikimedia Foundation should commit to making the protection of its registered users a higher priority and should take the necessary steps to achieve this. Similarly to the regulations for the Toolserver, it should first require an opt-in for all the tools on its own servers that compile detailed aggregations of user data. Users could do this via their personal settings, for example. Since Wikipedia was founded in 2001, the project has grown without any urgent need for these kinds of tools, and at present there seems to be no reason why this should change in the future. By creating free content, the community enables Wikimedia to collect the donations needed to run WikiLabs. That this should lead to users loosing their right of anonymity, although the majority opposes this, is absurd. To ensure that user data are not evaluated on non-Wikimedia servers, the Foundation is asked to take the following steps:

- Wikipedia dumps should no longer contain any detailed user information. The license only requires the name of the author and not the time or the day when they edited.
- There should only be limited access to user data on the API.
- It might be worth considering whether or not it is necessary or consistent with project targets to store and display the IP addresses of registered users (if they are stored), as well as precise timestamps that are accurate to the minute of all their actions. The time limit here could be how long it reasonably takes CheckUsers to make a query. After all, data that are not available cannot be misused for other purposes.

submitted by Silke WMDE (talk) 16:21, 20 December 2013 (UTC)

~~PROTECTED FOIA Confidential Treatment Request~~ WIKI0001478

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

Plaintiff's Exhibit 13

WIKIMEDIA META-WIKI

Main page
Wikimedia News
Translations
Recent changes
Random page
Help
Babel

Community

Wikimedia Resource Center
Wikimedia Forum
Mailing lists
Requests
Babylon
Reports
Research
Planet Wikimedia

Beyond the Web

Meet Wikimedians
Events
Movement affiliates
Donate

Print/export

Create a book
Download as PDF
Printable version

Tools

What links here
Related changes
Special pages
Permanent link
Page information
Link by ID

Talk:PRISM

*The following discussion is closed. **Please do not modify it.** Subsequent comments should be made in a new section. A summary of the conclusions reached follows.*

Based on the discussion below, the WMF legal team feels that there is general support for some PRISM-related action. However, we feel that the current proposals are either not strongly supported, or there are genuine concerns or reservations about them. The team will therefore continue to monitor the situation. In particular, in keeping with the consultation below, we will look for opportunities for action and collaboration that are:

- **Focused on the movement's mission and values - for example, actions focused on ensuring reader privacy, or on protecting WMF's right to be transparent with the community**
- **Consistent with our international nature - in other words, actions that do not not privilege one country's citizens over another**

We also recognize the questions and concerns raised here about privacy, and urge interested community members to continue that discussion as part of our larger privacy policy call for input.

Thanks to everyone who participated in the consultation. We encourage further discussion, including suggestion of potential actions, either through the new section at the end of this page, or through the advocacy-advisors list.

LVilla (WMF) (talk) 21:34, 11 July 2013 (UTC)

Contents [hide]

1 What wasn't said
2 Better supporting anonymous contributions
3 What types of logs does the Wikimedia Foundation keep, for how long and in what level of detail?
4 Thirty day rule?
5 June 21
6 Community Feedback
7 On establishing servers in other countries
8 Should we join with these organizations in their public statements and efforts as they relate to the Wikimedia community's values and mission?
8.1 Update
9 Stop logging IP addresses
10 "law-enforcement agency or a court or equivalent government body"
11 A U.S. issue?

12 Comments copied from Blog
13 PRISM concerns Trust, Trust concerns Wikipedia
14 Snowden as Wikimanias keynote speaker
15 Historical Background
16 Call for input on WMF privacy policy
17 Universal Declaration of Human Rights
18 and now?
19 PRISM in not everthing
20 Wikimedia may be lying
21 Further feedback and suggestions
21.1 Copied from above
21.2 Followup blog post
22 We should sign the global Principles on Surveillance guidelines
23 Meu temor(como brasileiro):

What wasn't said [edit]

This statement appears to carefully avoid speaking to the ongoing surveillance and traffic interception which Wikimedia has specific knowledge of but which itself is not actually an active party to, I think this is unfortunate and misleading.

I also note that the claims that Wikimedia has 'not “changed” our systems to make government surveillance easier' is, in my well informed opinion, basically a lie by omission: By failing to move all reader traffic to SSL wikimedia has failed to change its systems in order to limit the ongoing traffic observation and manipulation which it is specifically aware of (and, generally, to also protect against additional surveillance which Wikimedia may not be aware of). Because the traffic is unencrypted there would be little reason for any government to seek out Wikimedia's cooperation. With no active involvement required Wikimedia would have no opportunity to oppose blanket surveillance in a court of law. Evening ignoring the fact that Wikimedia is already aware that its traffic is being intercepted the use of SSL is a best practice which is already employed by default for all users on many popular websites.

It is my personal experience that in the past Wikimedia has not considered the privacy of its readers to be a high priority. I have never quite been able to understand why: My view has always been that to many people Wikipedia is an extension of their mind and their access patterns betray some of their most personal and intimate thoughts. But whatever the reason, adopting best practices to protect reader privacy has simply not been a priority and I've accepted that although I did not agree with it. But now I'm confused with the manner in which this post fails to acknowledge this past indifference while simultaneously claiming to care deeply. I would be delighted to hear that there was a change in priorities here, but considering the history it seems like this is simply a politically expedient response to a fad issue which will soon be forgotten. --Gmaxwell (talk) 00:45, 15 June 2013 (UTC)

> This certainly seems like a fad issue. While I'm not sure I'd characterize the lack of forced SSL in the same way you do, I think working on documents such as User:Sue Gardner/Wikimedia Foundation Guiding Principles is a much better use of time and other resources. This allows us to define what we stand for and what we believe, rather than

simply denouncing whatever the latest government abuse (or potential future abuse) happens to be in the news at the moment (SOPA, PRISM, etc.).

For what it's worth, bugzilla:47832 is the relevant bug about enabling HTTPS for all users. I doubt we'll see this happen this year or next, though.

And, at some level, there is a reasonable argument that some level of user responsibility is warranted. That is, stable HTTPS access (using pretty URLs) is currently available to anyone interested in using it. --MZMcBride (talk) 04:01, 15 June 2013 (UTC)

> well ssl is important, and I wish it was on all the time, i don't think it quite provides the protection you think it does. People can still do fingerprinting based on size of things requested. If you edit, the exact timestamp is recorded, which if the government is monitoring all the inbound ssl trafic should be enough to match you up to who you are. (Ssl only protects the content of the message. Not who sent it or that a message was sent. In the context of wikimedia where the message is already known or is public (usually), this isnt a lot of protection. (The biggest benefit in our context is protection against shared session attacks).Bawolff (talk) 15:27, 15 June 2013 (UTC)

SSL or TLS ? Which versions are supported, which one are deprecated and its support should be removed ? verdy_p (talk) 16:33, 15 June 2013 (UTC)

> Well this conversation is talking about encrypting http in general. Which version of SSL/TLS and if it is secure, is an implementation detail (An important implementation detail no doubt, but still off topic). Wikipedia apparently supports SSL3 and TLS1.0 according to https://www.ssllabs.com/ssltest/analyze.html?d=en.wikipedia.org Bawolff (talk) 19:07, 15 June 2013 (UTC)

Hello Greg, can you say more about this surveillance and interception? Are you talking about datacenter-level or backbone-level surveillance?

And yes, let's finish enabling HTTPS by default for everyone. I don't see anyone suggesting obstacles to making that happen, other the observation that it hasn't happened yet. The comments on the relevant bugs seem to be ideas or positive reactions. And speeding the transition to SSL-only serviceis one effective way we can swiftly increase reader privacy, regardless of what is in our public statements of principle. –SJ talk 23:48, 15 June 2013 (UTC)

Even having https by default it would not be efficient for most of people: if users use a navigator which collect data. In this case, the software send statistics with "listening" on the input and output data, even with a SSL layer. Information are sent encrypted to the developper company. I espescially think to google chrome and it's HTTPs everywhere feature: "Nobody" can sniff data; except google. It is probaly the same with IE; safari etc... It is possible to think that they can send passwords if the user choose to record them

The use of some add-on can create the same problem.

Some Os (espescially mobile one) send data by simply check-in a develloper company server. I think to android which do things like time tracking per application. This make difficult to understand why nobody tried to create a build with stat funtion removed from android source code. Apple doesn't seems to collect data with OSx. It dosen't prevent to do this with

IOS.

So instoring encryption by default aiming at spying programs would only have the effect to slow down connection with SSL headers, most of the time. It is useless until users of such software or OS recieve a warning banner. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 01:02, 16 June 2013 (UTC)

- **Comment** SSL is good for concealing stuff like passwords, but it's of no help for keeping private what articles people are reading, since the message lengths are usually enough to identify articles even if the packets are encrypted. Adding some random padding to each message before encryption can fuzz this up a litle bit, but not enough to matter. Also, Firefox 20 (I haven't tested other browsers) sends an OCSP request to Digicert (iirc) whenever you view an article on the secure site. That means Digicert gets the IP address of everyone who reads Wikipedia through SSL, which doesn't seem so great, although OCSP in general is a good idea. 50.0.136.106 07:21, 20 June 2013 (UTC)

  The OCSP request is not very helpful to determine what you are reading. In fact, since we have now SUL activated by default, the secure connection can be proxied from a random site owned by the WMF, and unrelated to the wiki you are actually reading (that secure proxy can then be used to visit all Wikimedia sites, and for a limited time, it could be used to navigate to other sites, within a secure frame, and for a limited set of protocols, only HTTP sites; to vicite external HTTPS sites, the proxy will not be used, that proxy will cache these external visits in a Squid server, for a limited time : one hour max, isolating the sessions as much as possible, but this proxy won't support external cookies very well, except temporary session cookies so this may limit the interactions with these external sites).

  For the user's browser, all will appear as if they were visiting the randomized proxy as the main site, and the HTTPS session will appear being originating from of a visit of this WMF proxying site. Digicert won't be able to determine which Wikimedia project you're actually visiting with HTTPS connected to that random proxy (With SUL, the session is identified and communicated to other actual projects using internal security tokens, and a single session is established for all wikis. In fact the proxies are located directly on the existing farm of Squid servers for any WMF project. verdy_p (talk) 23:47, 20 June 2013 (UTC)

- **Comment** Why not making wkimedia domains availaible with the .onion extension in more than SSL. It would be a message that this extension is not only used by bandits. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 13:20, 3 July 2013 (UTC)

Better supporting anonymous contributions [edit]

I repeat my comment: SSL or TLS ? And this is NOT off-topic, because you always use **SSL** when in fact you should speak about **HTTPS**.

SSL is deprecated (and too much unsecure if we think about what developers PRISM can do) ! What I mean is that the level of security needed in HTTPS and supported by Wikimedia sites should be specified. The strongest algorithms should be used, and users should be warned if their connection configuration do not support it. Otherwise they will

feel falsely protected if they just see "https:" or the security icon in their address bar or status bar !

In other words, **Wikimedia sites should display the current security level of their connection. It should also allow evaluating the security of their local account** (user password, inspection of the email confirmation : users can copy-paste the MIME headers of the confirmation email they recieved, or the MIME headers of the last mail sent to Wikimedia for posting images, or the informations added in HTTP headers by some browser plugins, or inspection of their version and known defects, suggesting upgrades or removal of these unsecure plugins), even before they create a local account, or when creating it by evaluating the strength of their password, because the local account will be the only protection they'll have for their pricay, by hiding to others their connection IP.

If an account is stolen or spied (by an intruder that broke the security algorithms), it should still not allow inspecting the connection history. And may be it should even hide to users the email address that they have registered, by encypting it once the email has been confirmed (the only thing that a user will be able to do is to change the email address, or reconfirming what they think is their own address).

All registered users should be notified immediately at their old email address to confirm the change of email address (to avoid it to be replaced by another proxying and spying email address). As the email address will now be invisible in the user's preferences to the user as well as to any possible spier, it will be impossible to know who really owns that account (this should be kept by Wikimedia sites in a secure database (so all subscribed notifications will be sent to an address that no spier should know.

And Wikimedia should also monitor the security of its mailservers for its outgoing emails going to the email address of a registered user (this means securing its DNS server, asserting the DNS entries, using all possible antispoofind technics, verifying mail server secure signatures...), because these emails are the main tool by which a user could still be identified, even if they are IP-connected via an anonymizing proxy.

But of course, users that want to communicate with Wikimedia sites on *politically sensitive subjects*, should avoid revealing their own identity online in their talk pages or when discussing in any public spaces or on talk pages of other users.

Instead, they should create a new specific (and unrelated) account for these activities, using an alternate email for registering it. Then they should use tools offered in their User's preferences page to assert the securoty of this new account.

Another idea:

If users fear their account on Wikimedia has been compromized, they should immediately ask the deletion of this registered account, for possibly creating a new one (the contributions will be kept, but will be anonymized using a user name like "anonymous-<random-hexadecimal-id>" in the history, the old account will be locked and no longer accessible to anyone.

All users should be offered an oppotunity to create an "**publicly anonymous secondary account**" : if they have one, and make any contribution on Wikimedia using their normal non-anonymous account, then Wikimedia should ask them if they intended to use the anonymous account instead: they can confirm it each time or instruct Wikimedia to stop

asking it for the next hour. If they want to use the secondary account, Wikimedia will present them a secure logon screen asking for the secondary password. As this account is anonymous, it should not need to be working under SUL (each wiki will use its own local database of anonymous user accounts). One they are connected to the two accounts, two icons are shown at top of page : their regular user name, and the "anonymous" account name, they can click on one of them to select which one to use (if they use the anonymous account, Wikimedia will not ask them to confirm their edits. If the anonymous session is idle for more than one hour, it will be automatically logged out (the session cookie should not last for more than one hour), and the anonymous icon will be shown in its disconnected state, even if they are still connected on their regular account (and Wikimedia will restart asking them if they want to use their anonymous account for their edits).

The secondary anonymous account may inherit immediately, at creation time, of some privileges from the primary regular account (notably the autoconfirmed status, but NOT any admin privileges). Users may also opt for creating an anonymous account directly, without any associated regular account (but then they'll start with no privileges, like all other newly registered regular users): in fact this should be the best solution for supporting anonymous users, we should encourage them to do so, instead of using their IP-only connection, logged in public histories (they can still register their email with it, and be sure that they'll be ale to reuse this same account on later connections): even if they are logged on, these anonymous users with a personal account should be kept logged on for a maximum of 1-hour of idle time (regular accounts may continue staying connected for 1 month). And even if they only have an anonymous account, they can also be offered the option to create a primary regular account, like other users (for their non-sensitive editing or reading sessions; in that case Wikmedia wil also ask them every hour if they should not use their existing anonymous account when accessing one page). Some pages should also not be warned by Wikimedia: the anonymous account may specify a ist of pages, or categories, or namespaces, where Wikiemdia will not ask them if they wish to use their anonymous account instead.

Registered anonymous users should also be allowed to participate to secured community polls (they will be able to vote only once), if this account is associated with a regular account (the vote will be visible to others as coming from a registered anonymous account, but then they won't be able to vote with their regular account as well). The secure vote server will check internally the status of the anonymous account, and will be able to see if the regular account has already participated or if another past anonymous account has voted (if so, users won't be able to vote again or will or change their vote, unless they ask to Wikimedia server to delete their old anonymous vote; this vote deletion will be performed securely).

Only one active (undeleted) anonymous account may be associated at any time to a regular account (this will limit abuses, notably with spammers, even if the CheckUser admin team may see with which regular account the anonymous account is associated. Some abusers may also be restricted (by spamfighters) from using their anonymous account for some time and informed. This event may be logged in their regular account that thay may continue to use).

This will also be useful when contributing in some subjects with the regular account, when there are personal conflicts (this could calm others, avoiding personal wars or personal defamation).

The list of past (deleted) anonymous accounts, as well as the current active anonymous account will be kept in the regular user account history, for a limited time, only to help fighting spammers; this should not exceed 1 month).

Creating and activating a publicly anonymous account should be a two click action (including for generating the password: users need to copy the generated strnig password, because it will later be encrypted and never shown again to anyone (including the user), but the user can request the deletion of this account and creation of a new one with a newly generatef password (overridable by the user typing a password of his choice and confirming it).

Even for regular (publicly non-anonymous) registered accounts, this should be simple, and Wikimedia should immediately propose a strong password before the user overrides it. All accounts (anonymous and non-anymous, should have a one-click button in their preference page, to generate a new string password and fill the two input boxes where they can change and confirm it (when the user types his own pawwsord, it is hidden by default, when the user clicks the "generate strong password", it will be shown and stay on screen, it will be used only if the user accepts it by confirming the preferences; but for accessibility reasons, there should still be a checkbox to hide/show the content of the password input and password confirmation box). verdy_p (talk) 23:29, 20 June 2013 (UTC)

What types of logs does the Wikimedia Foundation keep, for how long and in what level of detail? [edit]

Before we can start to consider actions by the Foundation, I think it's appropriate for us to look at our own logs and how PRISM could affect us. There was a thread brought up on Wikimedia-l about this topic this week. I didn't have a chance to read it fully but from a brief skim of it, I believe it's unclear exactly what information the Foundation keeps, and for how long. There was a link to a mailing list post by Domas from 2010 saying it's a 1/1000 sample, but other comments referred to a full access log for the past 30 days. Therefore, please can we get the relevant technical details from **all** teams with access to logs of what data is stored and for how long? I don't know the full details, but a few ideas would include asking the Analytics team (who use the new Kraken machine), whoever is using the raw data to produce http://reportcard.wmflabs.org/, general reader access logs, error logs etc. **Thehelpfulone** 00:28, 15 June 2013 (UTC)

Yes please. We should assume any record we keep might be accessed one day so the best preparation for this is to minimise the records we keep. If we don't have them then they can't be accessed. Filceolaire (talk) 00:43, 15 June 2013 (UTC)

- Well, these are the things we know they have per browser operation and Help:CheckUser#Information returned; article accessed, date/time of access, referer, username, IP address, user agent (browser, operating system, blah, blah, blah) and XFF headers. Depending on who you talk to, this info is supposedly purged after 30, 60 or 90

days. But it has been acknowledged that some of this information is copied to the checkuser wiki, arb wiki, etc. where it is kept permanently. 64.40.54.96 05:35, 15 June 2013 (UTC)

> This shouldn't be a "depending on who you talk to" situation. We're pretty open about it - the data is purged after 90 days. Data on long-term abusers *may* be copied to the Checkuser wiki for later use in analysis to determine whether future vandalism is related to a long term abuser, but that's incredibly rare, when viewed as a percentage of the whole. Philippe (WMF) (talk) 07:53, 15 June 2013 (UTC)
>
> > I think the original comment was about access logs for readers, not authors who edit. For how long is the access log kept for readers and is there an access log for all readers or just a 1/1000 sample? --Tobias talk · contrib 08:00, 15 June 2013 (UTC)
> >
> > > I have no idea. Deferring to those who know. :) Philippe (WMF) (talk) 09:55, 15 June 2013 (UTC)

I second that question. A EU citizen myself, and even though Wikimedia might not own or borrow servers in the European Union, how close are the Wikimedia servers from the requirements of the EU law ? It was alleged here, in 2011 that *EU legislation, (...) requires search engines to purge all data relating to end users after a six month period.* User:Philippe (WMF) says above : "data is purged after 90 days". I am afraid that as long as this is not clearly written in http://wikimediafoundation.org/wiki/Privacy_policy , there is no guarantee that the Wikimedia Foundation is intending to enforce this kind of regulation and serious about it. Is there anything that can guarantee that the Wikimedia Foundation cannot change the present "90 days" of today into "90 years" tomorrow without warning and consultation with the community and sufficient warning of the end user as regards the "terms and conditions" ? Teofilo (talk) 18:49, 15 June 2013 (UTC)
Agreed: this should be part of our privacy policy. –SJ talk 23:48, 15 June 2013 (UTC)
I had always had the impression that logs of editing operations were kept around for a while, but access logs were not--and in particular that CU couldn't tell what articles people were reading. If they can, I find that scary and invasive, but potentially useful in sock investigations. I would urge getting rid of all logging of read-only accesses, including aggregated logging such as viewcounts on articles and geolocations. There could be some very limited exceptions for dealing with ops problems (DDOS origins, etc) but any such info (about human readers, I'm less concerned about automated clients especially malicious oens) should never be disclosed. 50.0.136.106 07:28, 21 June 2013 (UTC)

Thirty day rule? [edit]

I thought there was some thirty day rule comment period related to proposals of this nature. Maybe I'm thinking of something else.

I suppose the Wikimedia Foundation could sign, but that wouldn't necessarily be representative of Wikimedia signing. --MZMcBride (talk) 00:55, 15 June 2013 (UTC)

> I assume you're talking about these policies? It doesn't look like there is a deadline (both a 'if times permits' clause to allow exceptions and no actual expectation of a deadline

spelled out) or do you mean something else? JAlexander (talk) 02:01, 15 June 2013 (UTC)

MZMcBride, that was for changes to the terms of use, I think. I'm not sure if the privacy policy is a subset of the terms of use, or if it's a separate contract. --NaBUru38 (talk) 20:21, 18 June 2013 (UTC)

June 21 [edit]

What happens on June 21 that makes that day the final day of community consultations? Don't you think that it's at least eyebrow–raising that it took the WMF 8 days (since the news first broke out on June 6) to write a blog post, and you only give the community 7 days to comment on it? How are you planning to get the wider community to comment on this? Are there any plans for CentralNotice/Watchlist campaigns asking people to comment, or are you perhaps planning to use EdwardsBot to send a notice to the village pumps? odder (talk) 00:57, 15 June 2013 (UTC)

Hi, Odder - the blog post came out today, but we asked for comment on wikimedia-l and advocacy-advisors on June 11th (and have been following the conversation on both of those lists). That said, if the community thinks the correct answer is "take more time" we're open to that too; our main interest in speed is because the earlier we move, the greater the opportunity to actually impact the discussion. - LVilla (WMF) (talk) 01:59, 15 June 2013 (UTC)

Thanks for the explanation, Luis—I was mostly afraid that 7 days might not be enough time for the wider Wikimedia community to comment on this proposal. Your answer clears this up, so thanks again. odder (talk) 13:47, 15 June 2013 (UTC)

Community Feedback [edit]

"It's important for Wikimedia to be a voice of opinion in these matters, but joining a group to back the opposition of PRISM doesn't seem like the most successful avenue to me. I think whenever an association is made with another organization or group of organizations it is easier for the whole group to find itself with potential liability. One company can never be completely sure of another company's origin, path and trajectory - take Invisible Children as an example - and the risk of being jointly discredited for something possibly inconsequential could affect the momentum of the movement at large. I think that many orangizations taking individual stances on the issue weighs heavier than a conglomerate doing the same." —Glenn Sorrentino

Hi, Glenn- Many of the organizations behind stopwatching.us have extremely long track records of doing the right thing: EFF, FSF, and CDT have all been doing rights advocacy for around 20 years, and while Mozilla is relatively new to direct activism, it also has a long track record of having strong values like ours. That said, if you feel we should have a voice, just not through stopwatching.us, what other suggestions would you make about how we should advance our views? — LVilla (WMF) (talk) 16:11, 15 June 2013 (UTC)

Some might have a "long track record of doing the right thing" but some of their fellow

travelers are, shall we say, controversial. Snowden was photographed with an EFF sticker on his laptop, suggesting he supports these "strong values." Yet Snowden's particular version of what he presumably considers to be "strong values" led him to seek employment with his latest employer with the advance purpose of getting access to secrets that he could then reveal without authorization. This is controversial, to say the least. If it wasn't controversial, surely a country with a better track record on Internet freedom than China or Russia would be sheltering him. I am amazed at how the WMF keeps finding the bad guys in the form of large numbers of U.S. Congressmen as opposed to somewhere else (first with SOPA/PIPA and now with PRISM which Congress has long been aware of).--Brian Dell (talk) 17:29, 25 June 2013 (UTC)

On establishing servers in other countries [edit]

At Meta:Babel#Wikimedia_servers_and_NSA_wiretapping I started a discussion on the possibility of the foundation establishing other servers in other countries partly so individual connections are less likely to be wiretapped.

Please read Stefan2's comments on that page.

So far Wikimedia has servers in Tampa, FL, Ashburn, VA, and Amsterdam. Considering that data usually takes the cheapest route rather than the most direct, where else should the foundation get servers? We have to take in consideration money that the WMF has and the political inclinations of the countries where the new Wikimedia servers are set up. For specific locations, would anyone like to evaluate the following locations? Singapore, Hong Kong, Brazil, South Africa... and I am not sure if the political climate in Dubai would support a WMF server there.

The idea is that, say, if an individual in Pakistan wants to connect to Wikimedia projects, he/she can connect to servers in Dubai, or if a person in Malaysia wants to connect, he/she can connect to servers in Singapore.

WhisperToMe (talk) 04:27, 15 June 2013 (UTC)

I'm not an expert on this, but it seems to me that increasing the potential number of jurisdictions that servers live in actually increases the risk of wiretapping, not decreases it, right? I mean, any of those countries could order a wiretap on a server, and all of a sudden we're up from one potential governmental player to several. Philippe (WMF) (talk) 07:57, 15 June 2013 (UTC)

We have a server in the Netherlands, so that's two government players so far. WhisperToMe (talk) 14:38, 15 June 2013 (UTC)

{{citation needed}}, please. odder (talk) 16:12, 15 June 2013 (UTC)

Wikimedia servers#Hosting says "As of June 2010, we have four colocation facilities:" with two in Tampa and two in the Netherlands, and "As of 2012 there are also servers in Ashburn, Virginia (eqiad)" WhisperToMe (talk) 17:11, 15 June 2013 (UTC)

You wrote we had *a server* in the Netherlands, which is not true. Additionally, I would also suggest that you check what are the roles of the

NL servers before jumping to any conclusions. Odder (talk) 17:16, 15 June 2013 (UTC)

Okay, so I should have said two servers or one location. Nonetheless the point was that we also have facilities in the Netherlands. Anyway I followed the link to "Server roles" on Wikitech from the Wikimedia servers#Hosting page, and the page is blank. However I found wikitech:Category:Servers (should I redirect "Server roles" to that page?). Each of those pages don't have information on geographical locations, but I found wikitech:Amsterdam cluster WhisperToMe (talk) 17:24, 15 June 2013 (UTC)

Doing further digging the Amsterdam cluster is a part of wikitech:Category:Esams cluster. I'm going to file through wikitech:Category:Clusters to get a count of geographical locations. WhisperToMe (talk) 17:30, 15 June 2013 (UTC)

Aside from the Esams cluster: wikitech:Category:Eqiad cluster -> Ashburn, VA. wikitech:Category:Knams cluster -> wikitech:Kennisnet cluster (Amsterdam). Lopar cluster seems to be in (Tampa) Florida (wikitech:Lopar cluster mentions caching out of Florida). Pmtpa cluster -> Tampa, Florida (wikitech:Tampa cluster). The page on the Ulsfo cluster (wikitech:Ulsfo) is blank. WhisperToMe (talk) 17:34, 15 June 2013 (UTC)

Okay, I found a page on the network design: Wikitech:Network design - It goes over the US network and the European network WhisperToMe (talk) 17:41, 15 June 2013 (UTC)

Notes some of the pages at wikitech are rather outdated. (For example, Isn't lopar long gone?). Perhaps looking through the lists of server types at ganglia would give you a better idea. My understanding [**which could be wrong**. Don't trust me. I do not know what I'm talking about] is that most of the "real" servers are in US, with esams (netherlands) having squid/varnish caching servers, that just forwards requests (other then anons who aren't editing) to the backend servers in ~~Vagina~~Virginia [Bad auto-spelling correct]. Bawolff (talk) 18:10, 15 June 2013 (UTC)

You mean Virginia, right? :) WhisperToMe (talk) 18:29, 15 June 2013 (UTC)

For our readers having multiple countries with servers may give some comfort, especially if there was some way to choose which server to connect to. I'm not convinced things work so well for editors, if you have more than one copy of a database open for editing you will get synchronisation issues. WereSpielChequers (talk) 14:56, 15 June 2013 (UTC)

That's a good point. Who are the WMF board members or officials who know the most about this? Based on the PRISM charts it may mean that Latin America & Caribbean and the Asia Pacific Regions may be the best place to establish Wikimedia

servers (it seems like those in Africa can connect to European servers). So I think the WMF should study Hong Kong, Singapore, Brazil, and/or Panama (or another Central American country which can be neutral) as ideas for server locations. WhisperToMe (talk) 15:32, 15 June 2013 (UTC)

It is useless, according to the end of this film about the NSA wiretraping program (NSA - L'agence de l'Ombre) (author: James Bamford and C Scott Willis) (2008), the NSA is also watching all strategic point of internet accross the world, with subprograms affilieted indirectly to PRISM. So it is not limited to the US. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 21:40, 15 June 2013 (UTC)

Does the film say where these end points are? WhisperToMe (talk) 00:17, 16 June 2013 (UTC)

No, they don't list all of them.The film say there are sattelite communication sniffing. I can also say that certain under sea cable landing have optical splittering circuits. The film give only details (to show an example) about Moro Bay in California: It give a full explaination about where the data is collected. You can find some part of the example at cryptome, but you won't understand many things with this web page.

The film is based on a book : The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America.

You have a lot of more information on those parts with the film rather than the PRISM leaks.

The orignal language is in english, but as I saw the film on the TV, all was translated, including the title. I can't find the original one.

2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 03:10, 16 June 2013 (UTC)

Thank you for the info! I'm going to try to find this book and get as much information about NSA wiretapping locations (now we will assume whatever Bamford says is true) as possible and perhaps the WMF can find information on how best to avoid this wiretapping. Locations for new WMF servers can be based on this information. Also it may be good to have backup servers in "neutral" countries in case the possibility of war comes. I would hate to see all of our hard work wiped out. I have been working on Wikimedia projects for almost ten years, so I'm sure you understand how I feel about this. WhisperToMe (talk) 02:56, 17 June 2013 (UTC)

2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA: I saw a video on YouTube which seems to be what you watched.

- Bamford's message was routed from en:Kuala Lumpur, to en:Mersing, Malaysia where it entered an undersea cable along the South China Sea to through en:Shantou, China, and then in an undersea cable to an area near en:Morro Bay, California, to a building near en:San Luis Obispo (80% of all communications from Asia to the US enter through this building, but under new NSA orders they don't tap in here), and then to the AT&T Regional Switching Center in en:San Francisco (this is where the NSA taps into the connection) -- So, if I am correct, if the reader traffic in East/Southeast Asia goes to Singapore or Hong Kong and it doesn't go via satellite, it will avoid

the NSA tap in San Francisco

I'll check if the NSA book has more information

WhisperToMe (talk) 06:10, 17 June 2013 (UTC)

I won't have a static ip this week. If you want to know which routers is used by a request, I suggest you the **tracepath6(article)** command. tracepath give you generally more details (more hops) than traceroute. Here is an example of a traceroute6 result from Dalas:

```
hop      rtt      rtt      rtt        ip address              fully
qualified domain name
1        7        7        6          2001:470:1f0e:513::1
hexillion-2.tunnel.tserv8.dal1.ipv6.he.net
2        8        1        1          2001:470:0:78::1        gige-g2-
14.core1.dal1.he.net
3        29       25       24         2001:470:0:1b6::2
10gigabitethernet5-4.core1.atl1.he.net
4        33       41       34         2001:470:0:1b5::1
10gigabitethernet16-5.core1.ash1.he.net
5        39       38       58         2001:470:0:299::2
100gigabitethernet7-1.core1.nyc4.he.net
6        108      107      116        2001:470:0:128::2
10gigabitethernet1-2.core1.lon1.he.net
7        118      115      138        2001:470:0:3f::21
10gigabitethernet1-1.core1.ams1.he.net
8        117      117      117        2001:7f8:1::a504:8539:1
9        120      125      124        2a00:d10:1144:61::468
vlan61.br.en1.oxilion.net
10       121      121      121        2a00:d10:1144:62::731
vlan62.n5k-a.en1.oxilion.net
11       116      116      116        2a00:d10:101::11:1
ergens.org
```

```
dal=Dalas
atl=Atlas
I don't know for ash
nyc=New York City
lon=London
ams=Amsterdam
```

If you want a good answer for server location: The best place for data center is everywhere in the world.

Let me explain: There is a technique originally created to reduce load on the public network. Instead of creating a big server in one place (wikmedia use also separate severs in Europe), you choose to have "medium" data centers divided all over the world. Each place contain a copy of the whole webs sites. With a same host name, the list of ip address you get will varies according to servers workload and your geographic location.

This technique of geographical web placement has a name, (which I forgot) and probably a wikipedia article. It is used by big firms like Google. You can make the test on companies like these: If you launch a tracepath, the number hops will be always fewer than most sites, and independently from the place you are located.

2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 02:19, 18 June 2013 (UTC)

> I'm in the US myself, but this would be fun to try! According to your vision, do you have cities in mind which would be good places for these medium data servers? How many such medium servers would you establish per continent? WhisperToMe (talk) 05:27, 18 June 2013 (UTC)
>
> > Sorry, I've been busy since last time. I'm afraid that I don't have a real answer. This is just something I learned when I was studying DNS. I know google have serveral location in europe, but if I do a host on yahoo...
>
> ```
> root@sysresccd /root % host www.yahoo.com
> www.yahoo.com is an alias for fd-fp3.wg1.b.yahoo.com.
> fd-fp3.wg1.b.yahoo.com is an alias for ds-fp3.wg1.b.yahoo.com.
> ds-fp3.wg1.b.yahoo.com is an alias for ds-eu-fp3-
> lfb.wa1.b.yahoo.com.
> ds-eu-fp3-lfb.wa1.b.yahoo.com is an alias for ds-eu-
> fp3.wa1.b.yahoo.com.
> ds-eu-fp3.wa1.b.yahoo.com has address 87.248.112.181
> ds-eu-fp3.wa1.b.yahoo.com has address 87.248.122.122
> ds-eu-fp3.wa1.b.yahoo.com has IPv6 address
> 2a00:1288:f00e:1fe::3000
> ds-eu-fp3.wa1.b.yahoo.com has IPv6 address
> 2a00:1288:f00e:1fe::3001
> ds-eu-fp3.wa1.b.yahoo.com has IPv6 address
> 2a00:1288:f006:1fe::3001
> ds-eu-fp3.wa1.b.yahoo.com has IPv6 address
> 2a00:1288:f006:1fe::3000
> ```
>
> > there are alias which contains eu. It make think yahoo have only one point for the whole european union. You probably won't have the same density in south corea as in Sahara. I must say that I know absolutely nothing about the synchronisation thecniques that are used, and i don't realy know sor dns too.
> > With the high number of law voted in US & eu for alowing thing this, I don't understand why peoples warm only now. If you think to the number of contries where drones work. You can realize most of peoples are safe.
> > For the rest of the world the main risk is unemployment, but it is not linked to any government. 2A02:8422:1191:6E00:56E6:FCFF:FEDB:2BBA 14:08, 3 July 2013 (UTC)

Should we join with these organizations in their public statements and efforts as they relate to the Wikimedia community's values and mission? [edit]

- Yes, please. Kellerkind (talk) 08:35, 15 June 2013 (UTC) (Hello, NSA!)
  - +1 --Isderion (talk) 13:54, 15 June 2013 (UTC)
- Should Wikimedia join in decrying PRISM? No.

  It was OK when Wikimedia decided to make a stand on SOPA, b/c SOPA legislation had clear and obvious detrimental consequences on the functioning of Wikimedia.

  It is not clear or obvious how PRISM or FISA has negative consequences on Wikimedia. In my view, the Foundation seems to have adopted the role of an internet freedom fighter, wanting to take a stand against anything perceived to threaten web users' privacy and freedoms. Now, that might be an admirable position, but it's also to some extent a political position and one that clashes with the foundation's longstanding principle of remaining neutral on such issues. moved from blog, comment by Nicholas Sammons : 2013/06/14 at 7:59 UTC by Jalexander (talk) 10:11, 15 June 2013 (UTC)

  > To be neutral about the knowledge inside Wikipedia and being neutral about the way internet works are not the same thing. If we want a neutral point of view inside Wikipedia, we need to protect free use of internet for dissident opinions to be able to exist. I think the Wikimedia Foundation should fight for the freedom of internet. Lionel Allorge (talk) 11:03, 15 June 2013 (UTC)

  Staying neutral in the face of a global wiretapping action by the US isn't neutral. Silence means saying "Yes" to this actions. We shouldn't do that. It is pretty clear how Wikimedia is affected by PRISM. It is about trust in internet use at all which then includes the never to be answered question about the tracking of your own search habits on Wikimedia projects.
  So I vote Yes for at least joining the public statements and efforts according to the role Wikimedia can do relating to its community's value and mission. --Jensbest (talk) 13:26, 15 June 2013 (UTC)

  > Then I guess we would all appreciate if you let us know *how exactly* Wikimedia is affected by PRISM and how is it involved in the scandal that broke around it if you think it's *pretty clear*. For me it isn't, so I would welcome an explanation. odder (talk) 13:46, 15 June 2013 (UTC)
  >
  > > You can't look on Wikimedia without reflecting on its digital environment. If the web as a whole is monitored by a state, Wikimedia, with Wikipedia being one of the biggest websites in this web, must take a stand according to its values and long-term practices. It isn't about the question if there is any Wikimedia-Staff forced to lie to us because of secret judge rulings and gag orders, it is about the fundamental question if there can be a free, not-state-monitored encyclopedia in a non-free, state-monitored web. The actions of the US-government spreading massive distrust all over the web. Distrust is endangering the emanzipatory and participatory culture of the web which is also an important foundation of all Wikimedia-projects. --Jensbest (talk) 18:28, 15 June 2013 (UTC)
  > >
  > > > Certainly Wikimedia does not have to do anything. It is the Foundation's (or rather the community's) choice whether to take any action, which is precisely what is being debated here. There is no information whether any

government monitors the whole web, PRISM is only about one government monitoring services of a couple of companies (however big they are). However, it's common knowledge that the Web, or some parts of it, has been monitored and censored for a long time (take China, Qatar, Egypt, Syria, and now Turkey as examples), and the Wikimedia movement did not protest against that. odder (talk) 18:57, 15 June 2013 (UTC)

> Certainly Wikimedia has to do something when the country in which most of its servers are hosted is convicted doing massive secret global webwide monitoring. You are wrong on how PRISM works. It is sweeping the web at a whole AND is using direct access to thousands of companies. Therefore my point made above is very relevant - there is no good web use inside a corrupted system, there is no free and anonymous use when the leading country of the so-called free webworld is doing massive global secret surveillance. The other "argument" that the web is partially state-monitored anyway and therefore any action would be useless is definitely the most fatalistic and irresponsible opinion on freedom I've heard for a long time. --Jensbest (talk) 20:52, 15 June 2013 (UTC)

> > How do you know that? As far as the media report the situation, PRISM is related to a small number of Internet service providers, if you take the global picture into consideration. Plus, I've never said that Wikimedia shouldn't act — I only said that it *did* not act when there were reports on how Chinese, Syrian, Egyptian and now Turkish governments monitored and censored the Web. We have millions of readers in those countries, and yet there wasn't any suggestion for the WMF to join the local initiatives for a free and unmonitored Internet — if we're acting now, then I'd think it be just fair for the WMF to react whenever there are reports on monitoring Internet users in countries reached by our projects. odder (talk) 21:09, 15 June 2013 (UTC)

> > > I agree with you that it is a question of how to balance decisions on taking action. Maybe Wikimedia should have a more fundamental permanent stance on the subject, but being based on the idea of openness and collaboration Wikimedia has to stick to the more complicated and sometimes tedious decision-finding process by asking the community. This doesn't make us as effective and "punchy" as other digital NGOs more focused on fighting for digital rights like EFF etc. - But then again, if this "big ship" Wikimedia is moving it means something for more people even beyond the digital filterbubble. - According to your question about the broadness and depth of Prism and related state-surveillance activities I don't wanna spam you with articles, so just one for some sunday lecture: a longer overview-article by AP. --Jensbest (talk) 22:23, 15 June 2013 (UTC)

one potential argument: Wikimedia relies on editors being able to edit freely without real world retalation. This is one reason things like no legal threats is a policy. If editors fear retalation by gov for the things they do on wikimedia, they wont do things that might piss off gov. Amount of systemic bias in Wikimedia could sky rocket. Obviously we arent at full survalience/police state yet, but things like that happen one small step at a time. This is a large step. Bawolff (talk) 15:17, 15 June 2013 (UTC)

- Yes we should decry PRISM, unless that is the US government announces that it wasn't monitoring Wikimedia traffic. If they give an assurance that they weren't snooping on us then Wikimedia should revert to neutrality as that would be consistent with only reacting to direct threats. Decrying is much less drastic an action than a blackout, and I think that it would be an appropriate level of action. WereSpielChequers (talk) 15:01, 15 June 2013 (UTC)
- That's definitely compliant with Wikimedian values and long-term practices: Wiki contributions are based on the premise that we are not forced to disclose our *real* identity. Alexander Doria (talk) 16:07, 15 June 2013 (UTC)
- I applaud the Wikimedia foundation for taking action.

  It is to my knowledge that the "collection" of data from those internet companies mentioned in the leaks are not done willingly, but unknowingly through a massive collection of packets that travel to and from their data centers (very similar to the upstream method found here http://en.wikipedia.org/wiki/Room_641A).

  If this is true, the only preventative way of circumventing such "prism" taps would entail allocating your data centers, specifically for North America, outside of United States jurisdiction — to Canada and Mexico, for example. However, user packets that are sent to and from Wikipedia are still very vulnerable as they will traverse private ISPs in the U.S., those of which are supposedly already under surveillance.

  An immediate response would be implementing a secure SSL connection for users inside the United States.

  I hope the Wikimedia foundation, along with other key organizations, continue to fight for a free, open and secure internet.

  I thank you all for your efforts. moved from blog, comment by Mark B : 2013/06/15 at 21:47 UTC by Jalexander (talk) 01:07, 16 June 2013 (UTC)
- Yes, the WMF should join with these organizations and support efforts to protect internet privacy from warrant-less removal. - Amgine/meta wikt wnews blog wmf-blog goog news 16:35, 16 June 2013 (UTC)
- ⊕ **Support** – We should stand with the Internet and against government spying. --Michaeldsuarez (talk) 23:11, 17 June 2013 (UTC)
- The WMF board should feel free to make a statement, if there is consensus for one, and individual board members should feel free to campaign as individuals as much as they wish, but I would be firmly opposed to a PRISM blackout in the style of the SOPA blackout. While I understand the temptation to wield political power, the project as a whole should not be a political actor, but remain neutral. Andreas JN466 10:32, 18 June

2013 (UTC)

- **Oppose** Per Andreas. --Anthonyhcole (talk) 12:37, 18 June 2013 (UTC)
- **Oppose** - I believe it's already been acknowledged by the Feds that to the extent that info is being collected beyond that pursuant to a particularized request, it's because they are data mining and data mining more or less by definition means the queries are not particularized. I don't think people fully understand just how different this is from prying eyes reading your personal email. On the other hand, were the WMF to gain media attention for its activism here, in my view it would provide some evidence for my claims at the the time of the SOPA/PIPA activism that the WMF feels compelled to weigh in on civil liberties issues that are of dubious if any connection to the development of Wikimania projects.--Brian Dell (talk) 18:44, 19 June 2013 (UTC)
- **Comment**. WMF needs to find out, in detail, whether any of these programs **potentially** affect Wikipedia, which is a different question from whether information has been delivered so far. My assumption is that potentially yes, they could be served up a NSL tomorrow demanding data on everybody who reads w:Acetone peroxide, etc. Indeed, it seems too tempting a resource for me to be entirely credulous that the NSA has passed it up so far - surely there were a few days a while back when they would have wanted every possible means to know who looked up anything about pressure cooker bombs from an IP address in Boston. In opposing this, we oppose what seems like a very sensible police tactic, and we have to do so on the basis of weighing the mild harm against the vast multitude against the chance of preventing grievous harm to a few - and in an age of locking down a whole city, there are clearly some authorities making the wrong decisions about things like that. We'll need more transparency about how search warrants/subpoenas for such things are *legally* delivered, and what protections there are there. What we need here isn't a vague feeling, but a well-constructed ideological fortress. We just need a lot better data and thought about all the issues involved. It is unfortunately likely that, far from being on the offensive, Wikipedia will find itself trying to argue against *mandated* data retention policies that have been promulgated in many contexts, trying to preserve what it has now. Wnt (talk) 21:48, 19 June 2013 (UTC)
- **Support** Prism (according to some people) presumptively examines all Wikipedia traffic (along with all other internet traffic) from Room 641A and similar locations. Therefore its operators monitor everything everyone is reading (even if only metadata is logged, that is enough to deduce the content being read, from message sizes). This has potentially major consequences for readers and therefore is a matter of serious concern for Wikipedia. Even if the allegations turn out to be false, they are plausible enough to have a chilling effect in their own right, so Wikipedia should intervene either way. I personally support major changes in Wikipedia operations and practices to deal with this, but that's beyond the scope of this immediate question. 50.0.136.106 07:14, 20 June 2013 (UTC)
- **Support**. I don't fear US where I'm located in France. Though I still fear blanket cooperation of France with US to provide everything that US requests. But I would need to violate French laws. I don't fear the consequences of my opinion and I'm free for reading everything I want. But I stil think that users around us are in severe troubles, and US action will create a precedent that will be followed by other countries (notably in

China, and in all Islamic countries, as well as Russia, against their political opponents; LGBT people for example are in severe troubles now almost everywhere in Africa, Russia, Central and Southern Asia, Indonesia, only by the fact they may read about these topics or give their opinion, or present the facts about what happens in their country, or translate articles about their country originating from foreign countries into their national language : this is even more critical for languages that are not major, like Azeri, Uzbek, Burmese, Persian, Urdu, Indonesian/Malaysian, Javanese... and most African languages, because there's not a very active and protected community abroad using these languages on Wikimedia projects... If people in these countries cannot read major foreign languages, they will be presented a skewed view. This view will be skewed (NPOV) even in Wikimedia sites edited mostly by other national residents of their country). verdy_p (talk) 00:26, 21 June 2013 (UTC)

Update [edit]

Hello all, thank you to everyone who shared their feedback above. Based on this consultation, there is limited support for advocacy about government surveillance, such as PRISM. We are currently evaluating possible advocacy options that are consistent with this feedback. Particularly, we are looking for options that are focused on government surveillance from an international perspective. You are welcome to continue to leave feedback and suggestions, and I will keep you updated. Thanks again, Stephen LaPorte (WMF) (talk) 18:52, 5 July 2013 (UTC)

15 threads, 10 support, 1 comment, 4 oppose (66.7%, 6.7%, 26.7%) - Amgine/meta wikt wnews blog wmf-blog goog news 17:28, 8 July 2013 (UTC)

But also a fair amount of negative feedback in other parts of the discussion (e.g., "US Issue" below, some of the blog comments), so my sense is that a pure count of the (very small) numbers does not mean much. Honestly open to persuasion/discussion on that point, though. LVilla (WMF) (talk) 17:39, 8 July 2013 (UTC)

Actually, I took the liberty of examining the remainder of this page. Not one thread did I find which stated opposition to action on this topic. There were questions about whether this is a a solely US topic (which, in a manner of speaking, it is, as it's the US NSA whose actions are being discussed.) There were discussions which suggested this is diversionary. But none opposed acting on it. Perhaps you're referring to discussions elsewhere and ascribing them locally as none expressed opposition to acting on this topic as far as I could discern. - Amgine/meta wikt wnews blog wmf-blog goog news 07:03, 9 July 2013 (UTC)

If we feel that "stopwatching.us" is too US-centric, I think it would be appropriate for us to post a similar statement of our own, framed more globally:

- Indicating that we will support regional or national efforts to keep this aspect of the web open, because of its impact on the free exchange of knowledge.
- Listing the national/regional initiatives we are aware of, which we may or may not have expressly signed on to.
- Listing and amplifying the participation of Chapters and other regional Wikimedia groups who have supported those regional initiatives.

- Encouraging the global Wikimedia community to help keep the web open in this fashion.

–SJ talk 18:34, 8 July 2013 (UTC)

Stop logging IP addresses [edit]

Currently and as far as I'm aware for the life of the project, edits by IPs have been publicly and permanently logged by full IP address on our databases. For me as a Brit that has never been an issue, and I even linked a couple of IP addresses I'd used in one of my RFAs. But to others it is an ongoing issue, I gather that much of our oversighting relates to accidentally disclosed IPs. IPs present a real security risk, for example an IP editor in a totalitarian country might not be aware of what irritates the regime, might be unaware that their IP is so easily tracked to them, might be caught out by an unexpected change of regime or may simply lose their temper and say something that puts them in trouble. We could fairly easily reduce these risks this by assigning temporary codes to IPs that edit. Unless there were a block in place, the codes could be reset every few months. Checkusers would still be able to look at recent full IP addresses. Other editors could still see which other edits had been made by the same IP during a period of months. But once the codes changed even the checkusers would only be able to link the IP addresses of last few months edits to defunct temporary codes, much as is the situation with logged in editors. Arguably the US would be the Government least affected by this security measure. But a boost to the security of an oft neglected part of our community would be a reassuring response to PRISM.
WereSpielChequers (talk) 15:41, 15 June 2013 (UTC)

> Stopping logging IP's will be a problem for the fight against spammers. But a solution is would be to transfer all logs outside US in a safe haven, in compressed batches, leaving just the minimum logs needed for performance, on a short timeframe.
> However the US law may still already require that service providers keep a minium amount of logs for inspection. In all cases, these logs must be severely restricted from random accesses, kept on servers in encrypted forms. And most probably, there should no longer be any user with CheckUser capability ni US or acting under US law.
> Note that many other countries already have such laws requiring keeping a minimum amount of logs for judiciary requests. In some countries this could be just a couple of months, in some others the requirements may extend to several years. For very visited sites, this means a cost not only for the storage, but also to ensure that it will be correctly backed up and saved from severe crashes, so that they remain readable (this implies additional maintenance costs for these backups, possibly offsite, or could require transfering these logs to a legally approved legal escrow, that will also want to be paid for this service... or directly to a governmental department).
> For now the WMF is locating most of its servers in Florida and has to comply to the laws of US and Florida (some servers for tools or for proxies are also located in Europe : proxies also may need to keep these connection logs.
> In some countries, users already can only to Wikimedia sites by using mandatory national proxies). Most users accessing to WMF sites via mobile Internet accesses are also using proxies maintained by their ISP, which will keep these logs (in addition to restricting the protocols, for example only HTTP, or HTTPS only for authentification and

data signatures for securing commercial/bank transactions, but not strong encryption!).

But the scope of PRISM is not just about connection logs to help tracking network paths and identify the senders. It is really in inspecting the contents sent, and getting access to the full user profiles maintained by websites (for example the full list of emails sent and received with their content and metadata, and precisce timing of user interactions with any online service : this includes the Internet, as well as GSM networks or any other electronic transport path).

The solution would be transmit data hidden within analog signals or strong random noise fields with steganographic technics (those that are used by militaries that can hide their transmission within the mediums used by regular commercial channels, by slightly modifying it in an invisible way (a way that does not break the existing protocols, or that just generates a small amount of random errors that these networks tolerate.) But Wikimedia is not a military organization, and these technics are very costly (they constantly need to be adapted, this implies huge unamortized development costs). verdy_p (talk) 16:29, 15 June 2013 (UTC)

> Note, one has to be careful when designing such a system, as it is shockingly easy to design something like that poorly, and have it be no more private then just putting the IPs of anons everywhere. Historically, if you go back far enough (aka during phase 1 time), we actually blanked out the last 3 digits of the IP address so it was just xxx. (AFAIK we stopped because this didn't actually provide any "real" privacy). A second problem is that each IP address is not an independent number, they are related. If we replaced each IP with some sort of hash of the IP, we wouldn't be able to as effectively investigate vandalism that comes from different IPs from the same network. Range blocks also would be a thing of the past. Bawolff (talk) 18:16, 15 June 2013 (UTC)
>
> > Good points, yes a careful redesign would be needed, and we still need to retain the ability to rangeblock. I think it is time for a major review of this area, both for privacy and to reduce collateral damage. For example range blocks are notorious for effecting lots of innocent parties, *smart rangeblocks* would only block edits by people with the same hardware and and browser configuration as the problematic editor. WereSpielChequers (talk) 23:55, 15 June 2013 (UTC)
> >
> > > I'm inclined to agree with WSC about this, but honestly -- I always assumed the reason why Wikipedia lists the IP addresses openly was to spare government agents the trouble of coming in and requesting them (and themselves the trouble of giving them out). Wikipedia's structure has in many ways seemed like a reaction to long-term spying, where so little is kept that is *not* public that the spies barely have an advantage over anybody else, which may be the best anyone can achieve now. Wnt (talk) 21:51, 19 June 2013 (UTC)
> > >
> > > > We have no longterm need for most IP data, and the spies can't request what no longer exists. OK there are some scenarios where this would be of little use, but what about where governments change and a new government wants to know things that one could have trusted the old government not to ask? WereSpielChequers (talk) 12:13, 30 June 2013

(UTC)

"law-enforcement agency or a court or equivalent government body" [edit]

http://wikimediafoundation.org/wiki/Privacy_policy uses "law-enforcement agency or a court or equivalent government body" language. Does that include the en:National Security Agency ? Teofilo (talk) 18:56, 15 June 2013 (UTC)

A U.S. issue? [edit]

The fact that WMF is concerned about privacy-eroding actions by the U.S. government is commendable, and I completely agree with ALA's statement quoted in the blog post: "rights of privacy are necessary for intellectual freedom". I also agree with the statement that "the global nature of internet traffic, and the alleged sharing of surveillance information between governments, means that Internet users around the world are potentially affected". However, as far as the issue has been handled by the organisations in the *StopWatchingUs* coalition up to now, the matter falsely seems to be only affecting U.S. citizens. We, non-U.S. citizens, have been ever treated as second-class humans in U.S. law: the safeguards against illegal wiretapping in FISA and PATRIOT act only apply to U.S. citizens. And despite the fact that the alleged surveillance potentially affects hundreds of millions of people around the world, the *StopWatchingUs* coalition is calling to "*Enact reform this Congress to Section 215 of the USA PATRIOT Act, the state secrets privilege, and the FISA Amendments Act to make clear that blanket surveillance of the Internet activity and phone records of any person residing in the U.S. is prohibited by law and that violations can be reviewed in adversarial proceedings before a public court*". That would surely be a good step forward for U.S. citizens, but still leaves out in the cold us. By "us", I mean the people *from abroad the U.S.* that access the Internet *from abroad the U.S.* to send contents to or retrieve them from *abroad the U.S.* and whose packets are routed through the U.S. (as 60 % of Internet traffic does). If WMF intends to push a less U.S.-centric approach in this issue, please count with all my support. But, please (and perhaps once in a lifetime), please stop seeing U.S. as the very center of the Universe. Thanks, Cinabrium (talk) 23:10, 15 June 2013 (UTC)

> Blanket surveillance of the use of US servers is a global issue. The language of this page does not suggest otherwise. We should focus on the underlying principles of privacy, which are universal. –SJ talk 23:48, 15 June 2013 (UTC)
>
> > @Sj But the letter by StopWatchingUs does *not* focus on "underlying principles" but on some aspects of US law only affecting US citizens. That was Cinabrium's point. --Chricho (talk) 01:15, 16 June 2013 (UTC)
> >
> > > Exactly. Thanks, Chricho. Wikimedia projects house a huge international community, which is affected by U.S. surveillance policies (and in a non trivial number of cases, by those of their home countries too). If WMF's actions on this issue will be limited to endorse the *StopWatchingUs* letter, then nothing would have changed for those member of the community out of the U.S. Furthermore, while demanding transparency and respect for privacy from the U.S. government,

and taking into consideration the transnational nature of the community, WMF should engage in similar actions wherever privacy and freedom of expression are harmed by sevretive laws and Star Chamber procedures. Canada, Sweden, Italy and India are just examples of legal frameworks allowing forms of surveillance even more invasive that those in the U.S. I'm not opposing actions with regard to NSA's PRISM scandal (I would add BLARNEY, NUCLEON, and many other questionable systems). I'm just saying that WMF's actions should be directed to protect some fundamental rights of the whole Wikimedia community, wherever those rights may be at risk. Cinabrium (talk) 08:56, 16 June 2013 (UTC)

Hello, Alex Fowler here from Mozilla, one of the sponsoring organizations behind the StopWatching.Us campaign. We are also a community made up of thousands of contributors from around the world. Starting this week, we've broadened the campaign site to be inclusive of citizens outside of the US. More is underway to broaden input and dialogue from around the world. We'd benefit greatly from this community's participation and ideas on other ways to globalize campaign messages and actions.

Hello, Alex! Endorsing this statement (and convincing other organizations to do the same) could be a good starting point for globalizing the campaign. Cinabrium (talk) 17:38, 19 June 2013 (UTC)

I agree with Cinabrium's and Chricho's remarks. --NaBUru38 (talk) 20:34, 18 June 2013 (UTC)

Comments copied from Blog [edit]

- The united states government is only trolling the very low hanging fruit. Any serious netherios group knows the ways to circumvent detection. Its reminiscent of “weapons of mass destruction” and will be lapped up by the chattering classes on the net. Anonymous. Copied from blog; Comment by Anonymous 2013/06/15 at 00:37 UTC by Jalexander (talk) 07:57, 16 June 2013 (UTC)
- What people want to know is this:
  “When I read Wikipedia is the government reading over my shoulder, logging my activity, and potentially inferring my politics and values?”

  But they cannot find the answer to this simple question in your post. Allow me to help you with a frank answer:

  For some users the answer is unequivocally yes: Wikimedia has _specific_ knowledge of authorities in some countries intercepting and monitoring traffic to Wikipedia.

  For users who are concerned about observation by the US government the frank answer is “We probably couldn’t tell you if it were so, so asking us is pointless.”— if Wikimedia was ordered to lie by the United States government it would lie. It might fight such an order but it would lie until it won. Furthermore, individual members Wikimedia staff may also be acting under the influence of the US or other government without Wikimedia’s knowledge. It is difficult to be sure of the absence of surveillance.

  Wikimedia also currently keeps detailed access logs which may be subpoenad (or stolen)

at some time in the future and used to look for people (by IP address) were reading particular articles or which articles a particular IP address has read. Similar data— in the form of search engine logs— has been used in US courts in the past to prosecute people.

Fortunately the readers of Wikipedia aren't helpless and don't have to trade privacy for knowledge:

- If you use the https-everywhere browser add-on (https://www.eff.org/https-everywhere) the identify of the specific articles you read are hidden from any party who does not have Wikimedia's cooperation.
- If you browse using Tor (https://www.torproject.org/) then your Wikipedia reading habits will be kept more private even if Wikimedia is cooperating with parties conducting surveillance, and the fact that you are using Wikipedia at all will be hidden.
- For smaller Wikipedia languages it is feasible to download the entire Wikipedia and read it offline at your leisure (http://en.wikipedia.org/wiki/Wikipedia:Database_download)

You can also limit your Wikipedia browsing to public wifi networks, although many keep logs, and libraries systems where no identification is required.

These actions can keep your reading private regardless of the specific surveillance program of concern or Wikimedia's level of (non)-participation. Copied from blog; Comment by Greg Maxwell 2013/06/15 at 01:21 UTC by Jalexander (talk) 07:57, 16 June 2013 (UTC)

- The US government doesn't believe in humans, their values. So the PRISM happened. Copied from blog; Comment by arun 2013/06/15 at 03:59 UTC by Jalexander (talk) 07:57, 16 June 2013 (UTC)
- About note 2: it has been revealed that the alleged minor limits on the scope of surveillance only applies to US nationals living in US, but in fact this is only determined by a fuzzy reasonnable conviction that the location and nationality Internet user is not really very well determined. These fuzzy limits imply that more than half of US citizens will be spiable independantly of these limits.
  The limitations of budgets for the US agency means that they will in fact just scope some keywords to determine this.

  In addition this minor limitation of sope also means that US citizens located abroad, or accessing the Internet via foreign networks will be spied without knowing it. As well, the world trafic from abroad that can reach a US network is tremendous, due to the many third-parties involved in delivering Internet services in the world. So anyone in the world will not be subject to these limitation of scope, and can have their personal data or opinion gathered, stored, and searched in the US agency "Big Data" systems, and kept for unlimited time.

  There's absoutely no limits on the usage that will be done about these data, and it may be used to exercise pressures against people around the world, only for their political, social or economical views or actions, even if these actions are perfectly legal in these countries (and rules there by laws protecting their privacy). This could then be used not

just for fighting against terrorism or international criminality (this is already allowed within international cooperations of law enforcement polices, under the scrutiny of national justice systems), but for any concern that the US government judges will be useful to protect its own economical interests, such as limiting the capability of saling things to US, or threatening them of nex taxes, or harassing their contacts in US that still work there in full compliance with US laws (for example refusing to contract with them, without having to justify why).

We've already seen people denied access to US when boarding a plane or only when they put their first foot on a US airport, for many false (unverified) allegations of links with terrorists, or international criminals, or their providers, only because they had a name similar to a growing list of people created in a multi-level web where those people have never had any contact or nay reason to believe that they were in contact with these seeked people. Every month now, this costs a lot of money to travel agencies around the world (or in US), and people are held in custody temporarily and ejected back to their country, based on false allegations or suspiscions. And legal contracts are broken unilaterally by the US governement? All these actions are made without any compensation (people may only defend their case in a US court, but they cannot go there and the only mean for them would be to pay a very costly US attorney, acting alone with very limited informations collected : only rich people can pay these services, without any warranty that false allegations or suspiscions will be removed from the databases, and new difficulties will reappear later, even if the initial allegations were proven completely wrong).

On the opposite, the US in fact does not collaborate with the same scale to fight against some US criminals, and offers a passive protection in many cases, not really limiting their actions (notably in cases of financial abuses and Internet abuses).

It is wellknown that US even pays them to act abroad, and will protect them by offering them immediate asylum in US in case of problems, and that legal threats against them abroad will be alerted to them, to limit the legal actions or embarass the investigators (using private information collected illegally from them, without them having any action in US, or against US, or being aware that this may impact some US politics or interests, other than fair and legal competition protected by international treaties and conventions).

This system of Internet surveillance is very unbalanced when we measure how the Internet is controlled from US, or its services are hosted in US for most critical operations, as well as a broad cloud of third-part providers of services (and of proprietary softwares, hardwares and very important technologies such as encryption, DRM systems, the PKI... and even HTTPS itself). The US detains the power-off button to cut any one at any moment from most parts of the Internet (even on services made abroad and not intended really to be used in US). The core infrastructure of the Internet cannot work without US control (or it can only work in a very limited subnetwork, but not on the "open" Internet we use everyday via our foreign ISPs, that are often liable themselves in US where they have some subsidiaries, and via international stock markets controling their corporate governance).

For these reasons, your note #2 tends to reduce the severity of the effective impact of

this surveillance. Probably only about 100 millions of US citizens will be protected, within a world of 7 billions people (this is about 98.5% of the world population that will be under possible US scrutiny of their legal private life, at any time and for no reason at all at the time of this surveillance, but who will become some years laters to difficulties or personnal harassment...) Moved from blog comment by Verdy_p on 2013/06/15 at 09:45 (UTC) by Jalexander (talk) 01:20, 16 June 2013 (UTC)

PRISM concerns Trust, Trust concerns Wikipedia [edit]

I strongly support any steps by the Wikimedia movement (including WMF) to openly oppose PRISM and similar spy programs. Though currently there is little certainty about what exactly is happening, it is clear to me that NSA spying has the *potential* to violate privacy rights of our users on a massive scale. As a main source for unbiased and quality information on the web, there is every reason to believe that Wikipedia is a potential target. Among the billions and billions of harmless requests, there are without doubt some interesting ones, to filter out which is the NSA's specialty. Someone from the middle east is acquiring chemistry knowledge on Wikipedia that could be helpful in making bombs? A French author writes elaborate articles about military radio stations? The simple fact that most of what is accessed is harmless does not mean that everything is.

As a result, the privacy of our users is in jeopardy. Even if you don't agree with this, certainly the *belief in privacy* is in jeopardy. If users can't or won't trust us anymore to distribute uncensored information in a privacy-respecting manner, this is a huge loss. It is our responsibility to make sure that users can and will keep trusting and that their trust is well-founded by doing everything in our power to make sure our user's rights are respected. --Tobias talk · contrib 23:00, 16 June 2013 (UTC) Ps.: The big Internet companies are busy finding sneaky wordings that dodge the question of whether violated user privacy. With SOPA and PIPA there was a broad alliance. With PRISM, much more depends on our voice.

> Saying Wikimedia ought to take a stand whenever "the *belief in privacy* is in jeopardy" would seem to place an extraordinary burden on the foundation. One could point to a whole slew of legislation/government practices which potentially threaten the *belief in privacy*. Is Wikimedia's role that of some kind of privacy warrior akin the ACLU? NickCT (talk) 14:46, 17 June 2013 (UTC)
>
> > Sorry, I should have been more precise. I'm talking about privacy *when accessing Wikipedia*. Facebook and Google doesn't respect user privacy, that much is well known and it shouldn't be a great concern to Wikipedia/Wikimedia. Similarly, if the government decides to install more CCTVs, it doesn't impact Wikipedia directly. But with PRISM and other governmental spying activities, privacy not only of our users in general, but *while browsing Wikipedia* is at stake. --Tobias talk · contrib 18:48, 17 June 2013 (UTC)

Snowden as Wikimanias keynote speaker [edit]

In August we will have Wikimania in Hong Kong and I would like to hear Snowden. (If it is secure for


Wikimania or Blue Lagoon?

him.) This would be also a good statement, beside joining stopwatchingus. So please invite him. --Kolossos (talk) 18:39, 17 June 2013 (UTC)

+1 --Kellerkind (talk) 19:00, 17 June 2013 (UTC)

+1 --Tobias talk · contrib 19:46, 17 June 2013 (UTC)

+1 --Manastirile (talk) 20:14, 17 June 2013 (UTC)

+1 -- TheOriginalSoni (talk) 04:20, 18 June 2013 (UTC)

+1 but not billed as a "keynote speaker". That's too big a statement, and I'd be very uncomfortable pinning our public face to this issue. While it's relevant, important, appropriate and will surely catch the media, our core Wikimedia priorities include our own affairs - Wikipedia Zero, global south, editor rates, Wikimedia community, Visual editor, and chapter and foundation highlights of the year. If we include a prominent but not keynote session with him, that doesn't dominate our core issues, that would come across better and more maturely - and not like bandwagon jumping. It won't go un-noticed for low-keying it. FT2 *(Talk | email)* 13:32, 18 June 2013 (UTC)

I don't imagine this will be possible. It seems as though Mr. Snowden is currently in hiding. I imagine by August he'll be in a U.S. prison or dead. --MZMcBride (talk) 16:50, 18 June 2013 (UTC)

...or in Iceland at the Blue Lagoon <:o) --Kellerkind (talk) 18:34, 18 June 2013 (UTC)

If it's unsafe for him to come personally, can he give a speech through Skype or something Ypnypn (talk) 22:26, 18 June 2013 (UTC)

+1, A dedicated speech will be more than enough. Chenxiaoqino (talk) 13:00, 19 June 2013 (UTC)

+1. I would suggest that he should be strongly encouraged to spend at least *some* time talking about how NSA surveillance affects Wikimedia projects in particular. In this way, such a talk can be viewed not solely as a political statement but as a technical consultation, and if an honorarium is required it would be more feasible to justify the spending on that basis. Wnt (talk) 21:23, 19 June 2013 (UTC)

- Though I should emphasize about the above that some good lawyers had better check over everything carefully - we would not want Wikimedia to end up with Assange-like charges of actually paying for/conspiring in *new* releases of classified information. Wnt (talk) 21:33, 19 June 2013 (UTC)

Historical Background [edit]

See also w:Cabinet noir. One of the best things Wikipedians can do about this issue is to provide professional, serious, published knowledge about this issue in its articles. Teofilo (talk) 22:00, 17 June 2013 (UTC)

[edit]

Call for input on WMF privacy policy

Not the same topic but related in many ways so I wanted to drop a note here pointing to the new Call for input on WMF privacy policy (also posted as a blog post) and it's associated discussion page. Jalexander (talk) 09:41, 19 June 2013 (UTC)

Universal Declaration of Human Rights [edit]

> « *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.* » (article 12).

Does anybody remember the Declaration of the Independence of Cyberspace? It was in 1996. Twenty years later, non-free software providers let governments to read everybody's emails, phone calls, web access… This is not only an attack against human rights, but also a threat to the knowledge society. Privacy is a pillar of liberty, a need on Internet. And without freedom, no free software. Mediawiki is free software, and our free encyclopedia is online.

We have to support our allies. (GENIUM) 21:48, 20 June 2013 (UTC)

and now? [edit]

A decision should be reached on the 21th June, now is the 25... Any news on the subject? --Isderion (talk) 01:38, 25 June 2013 (UTC)

> Hello Isderion, we are reviewing the above comments, and we will share an update soon. Many thanks, Stephen LaPorte (WMF) (talk) 16:23, 25 June 2013 (UTC)
>
> > Soon? --Kellerkind (talk) 14:12, 2 July 2013 (UTC) P.S. If you don't like to do something, that's ok, but say something.
> >
> > > This is getting frustrating. You give the community one week to comment, the community participates to a small degree and then you need more than 2 weeks for reviewing the comments and reaching a decision. In the meantime you give no information to the community. This is not my understanding of a professional community liaison. --Isderion (talk) 23:14, 4 July 2013 (UTC)
> > >
> > > > Is there anything I can do to help here? I also haven't heard any update but, as I noted more generally here, I feel it is important to our community and to our long-term mission for us to take a stand beside like-minded organizations. I would like to help the WMF take a more public stance on the matter. –SJ talk 20:55, 7 July 2013 (UTC)
> > > >
> > > > > Thanks for the offer (and btw. congrats for the board seat), but the WMF posted an update 2 days ago, though it is a little bit hidden in the middle of the page (see Talk:PRISM#Update). It seems that this topic is rather low priority for the WMF, but I appreciate that they are going to focus on an international perspective, now that it becomes more and more clear that most governments spy on each others citizens and sometimes also their own. Maybe Noam Chomsky is right when he says that Governments will use whatever technology is available to combat their primary enemy – their

own population. (→Isderion (talk) 22:24, 7 July 2013 (UTC))

PRISM in not everthing [edit]

Now we have also a problem with British GCHQ so the problem comes to europe. And there are also articles about surveillance of public social media http://www.wired.co.uk/news/archive/2013-06/26/socmint and other stuff. So should we have different pages, should we have a more generally page or should we still concentrate on US-GOV and PRISM? --Kolossos (talk) 22:02, 26 June 2013 (UTC)

Government surveillance? --Kellerkind (talk) 11:52, 27 June 2013 (UTC)

Wikimedia may be lying [edit]

It is of knowledge of everyone that US authorities have, nowadays, power enough to make secret subpoenas, that means, request user's informations without user's knowledge, and without and order from a judge. The holder of the information may be arrested and suffer bitter consequences from revealing information about the subpoena to the targeted user. That said, subpoenas may have been sent to Wikimedia Foundation, and if it is forbidden to reveal any cooperation with US authorities, it's completely useless to simply state that it did NOT cooperate with them. Useless, and senseless, for the simple fact that it would be a crime to admit the oposite. That said, it is clear for me that it is **NOT** safe to trust in ANY organization, foundation or enterprise located in the US, or owned by any US organization, foundation or enterprise. US has become a state of exception, and the most realistically measure to be taken would be moving not only servers, but also capital, staff and headquarters to places where freedom of expression still has some meanning.

- AFAIK with open source software it's harder to hide secret measures to record information than with closed source software. The Wikimedia software on this site is open source. It's why hackers didn't trust Michael Domscheit-Berg when he refused to release the source code for his "en:OpenLeaks" website. WhisperToMe (talk) 15:02, 6 July 2013 (UTC)
  - It is possible for certain requests (*national security letters*, which are different than a subpoena) to include a demand that you not tell anyone you have received one. However it does not compel you to lie; you can simply say you "cannot answer" when asked whether you have received one. In contrast, until an organization has received such a request, it can say clearly that it **has not** received such a request. Wikimedia's head counsel stated clearly on the blog, "*We have not received any National Security Letters*." (Caveat: as a Board member, I would not be notified if such an NSL had been received by the Foundation, so I have no direct knowledge.) –SJ talk 20:55, 7 July 2013 (UTC)

*The above discussion is preserved as an archive. **Please do not modify it.** Subsequent comments should be made in a new section.*

Further feedback and suggestions [edit]

Copied from above [edit]

Hello all, thank you to everyone who shared their feedback above. Based on this consultation, there is limited support for advocacy about government surveillance, such as PRISM. We are currently evaluating possible advocacy options that are consistent with this feedback. Particularly, we are looking for options that are focused on government surveillance from an international perspective. You are welcome to continue to leave feedback and suggestions, and I will keep you updated. Thanks again, Stephen LaPorte (WMF) (talk) 18:52, 5 July 2013 (UTC)

> 15 threads, 10 support, 1 comment, 4 oppose (66.7%, 6.7%, 26.7%) - Amgine/meta wikt wnews blog wmf-blog goog news 17:28, 8 July 2013 (UTC)
>
> > But also a fair amount of negative feedback in other parts of the discussion (e.g., "US Issue" below, some of the blog comments), so my sense is that a pure count of the (very small) numbers does not mean much. Honestly open to persuasion/discussion on that point, though. LVilla (WMF) (talk) 17:39, 8 July 2013 (UTC)
> >
> > > Actually, I took the liberty of examining the remainder of this page. Not one thread did I find which stated opposition to action on this topic. There were questions about whether this is a a solely US topic (which, in a manner of speaking, it is, as it's the US NSA whose actions are being discussed.) There were discussions which suggested this is diversionary. But none opposed acting on it. Perhaps you're referring to discussions elsewhere and ascribing them locally as none expressed opposition to acting on this topic as far as I could discern. - Amgine/meta wikt wnews blog wmf-blog goog news 07:03, 9 July 2013 (UTC)
> > >
> > > As one of the first commenters on this page, I said:
> > >
> > > > "This certainly seems like a fad issue. [...] I think working on documents such as User:Sue Gardner/Wikimedia Foundation Guiding Principles is a much better use of time and other resources. This allows us to define what we stand for and what we believe, rather than simply denouncing whatever the latest government abuse (or potential future abuse) happens to be in the news at the moment (SOPA, PRISM, etc.)."
> > >
> > > If this isn't explicit enough to rise to the level of stated opposition to action on this topic, let me know and I can rephrase.
> > >
> > > Another comment copied over to this page reads:
> > >
> > > > "Should Wikimedia join in decrying PRISM? No."
> > >
> > > Given comments like these, I'm not sure what opposition to action would look like to you.
> > >
> > > It would be helpful if you could describe specifically what actions you feel the Wikimedia Foundation should take and how you feel those actions would further the Wikimedia Foundation's mission. I think most Wikimedians strongly disagree with secret government surveillance programs such as PRISM. But what of it? Wikimedia is in the business of providing free educational content to the world, not acting as a freedom fighter or political advocate. --MZMcBride (talk) 19:43, 10 July 2013 (UTC)

If we feel that "stopwatching.us" is too US-centric, I think it would be appropriate for us to post a

similar statement of our own, framed more globally.

- Indicating that we will support regional or national efforts to keep this aspect of the web open, because of its impact on the free exchange of knowledge.
- Listing the national/regional initiatives we are aware of, which we may or may not have expressly signed on to.
- Listing and amplifying the participation of Chapters and other regional Wikimedia groups who have supported those regional initiatives.
- Encouraging the global Wikimedia community to help keep the Web open in this fashion.

–SJ talk 18:34, 8 July 2013 (UTC)

I think making a public statement that is less US-centric is fine as well and more in line with our global mission. --Tobias talk · contrib 11:31, 13 July 2013 (UTC)

Followup blog post [edit]

FYI, the Foundation/LCA wrote and posted a followup post on this topic on July 18.

We should sign the global Principles on Surveillance guidelines [edit]

A coalition of global groups, called "Necessary and Proportionate", formulated a beautiful and non-nation-specific set of guidelines for how to apply human rights principles to surveillance.

It is called the "**International Principles on the Application of Human Rights to Communications Surveillance**", and has been signed by hundreds of organizations, including human rights, internet, legal, policy, and knowledge organizations. This would be an excellent and appropriate statement for us to sign.

We would be the largest website to sign on to date; but dozens of major global organizations and foundations that we rely on and work with have already done so. –SJ talk 00:56, 7 November 2013 (UTC)

I am very supportive of this suggestion. How can we learn what is the status of the Foundation's decision-making on this suggestion? - Amgine/meta wikt wnews blog wmf-blog goog news 04:57, 6 December 2013 (UTC)

Meu temor(como brasileiro): [edit | Add topic]

- Eu acho que o governo americano podem invadir conta de administradores da wiki e destruir este projeto. Por isso defendo que sites como o nosso tenham o sistema de segurança EV-SSL. João bonomo (talk) 17:13, 19 July 2013 (UTC)
- I think the U.S. government can invade the wiki administrators account and destroy this project. therefore argue that sites like ours have the security system EV-SSL. João bonomo (talk) 17:13, 19 July 2013 (UTC)

This page was last edited on 6 December 2013, at 04:57.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. See Terms of

Use for details

Privacy policy About Meta Disclaimers Developers Cookie statement Mobile view

a WIKIMEDIA project Powered by MediaWiki

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

Plaintiff's Exhibit 14

USCA4 Appeal: 20-1191 Doc: 18-4 Filed: 07/01/2020 Pg: 57 of 549

TECHNICAL STATISTICS FOR 2017 TO 2018 RESPONSIVE TO ODNI INTERROGATORY NO. 19						
Protocol	**Volume**	**Date Range**	**Foreign Countries, Regions, Territories**	**IP Addresses**	**Encryption Status**	**Additional Notes**
ODNI Interrogatory 19(a)	*ODNI Interrogatory 19(b)*		*ODNI Interrogatory 19(c)*	*ODNI Interrogatory 19(e)*	*ODNI Interrogatory 19(d)*	*ODNI Interrogatory 19 (d)*
Category 1 Wikimedia communications with its community members, who read and contribute to Wikimedia's Projects and webpages, and who use the Projects and webpages to interact with each other						
Total HTTP & HTTPS requests: foreign users to WMF US servers	381,655,849,279	Aug. 1, 2017, to Jan. 31, 2018 (six months)	List of countries for HTTPS (Exhibit A)	198.35.26.0/23, 208.80.152.0/22, 2620:0:860::/48, 2620:0:861::/48, 2620:0:863::/48	HTTPS: 373,045,851,598	For clarity, these HTTPS and HTTP requests use the same IP addresses.
			List of countries for HTTP (Exhibit B)		HTTP: 8,609,997,681	
Total HTTP & HTTPS requests: US users to WMF foreign servers	2,812,819,460	Aug. 1, 2017, to Jan. 31, 2018 (six months)	Netherlands	91.198.174.0/24, 2620:0:862::/48	HTTPS: 2,479,014,613	For clarity, these HTTPS and HTTP requests use the same IP addresses.
					HTTP: 333,804,847	
SMTP communications: foreign users to WMF US servers	Unknown		Unknown	208.80.152.0/22, 2620:0:860::/48, 2620:0:861::/48	Unknown	
Category 2 Wikimedia's internal log communications						
Apache Kafka log communications transmitted from WMF foreign servers to WMF US servers	736,045,377,450	Aug. 1, 2017, to Jan. 31, 2018 (six months)	Netherlands	10.0 0 0/8, 2620:0:860: /46	736,045,377,450 log communications encrypted using IPSec	
Category 3 Communications by Wikimedia staff						
Logged international TCP connections using WMF Office Network or WMF VPN	4,948,011	Mar. 1, 2017 to Feb. 28, 2018 (one year)	List of countries for non-VPN (Exhibit C); List of countries for VPN (Exhibit D)	The WMF Office Network IP range is 198.73.209 0/24, with the WMF VPN operating on IP address 198.73.209 25	All 791 connections encrypted using OpenVPN (SSL/TLS protocol)	Other than the VPN connections, Wikimedia itself does not systematically encrypt connections to and from the office network router and it would not be practical for it to do so. However, individuals who use the office network router may establish encrypted connections based on the particular communications services they use at any given time. Because Wikimedia's office network router does not log application-layer protocol information, Wikimedia does not know with certainty the extent to which the data transmitted over these non-VPN connections is encrypted. The logs do contain, however, the source and destination ports of connections, which in certain cases may shed light on the encryption status of connections, such as those that use port 443 or port 22.

Logged international UDP connections using WMF Office Network or WMF VPN	2,207,771	Mar. 1, 2017 to Feb. 28, 2018 (one year)	List of countries for non-VPN (Exhibit E); List of countries for VPN (Exhibit F)	The WMF Office Network IP range is 198.73.209 0/24, with the WMF VPN operating on IP address 198.73.209 25	All 19,709 connections encrypted using OpenVPN (SSL/TLS protocol)	Same response.
Logged international ICMP connections using WMF Office Network or WMF VPN	51,301	Mar. 1, 2017 to Feb. 28, 2018 (one year)	List of countries for non-VPN (Exhibit G)	The WMF Office Network IP range is 198.73.209 0/24, with the WMF VPN operating on IP address 198.73.209 25	0 connections encrypted using VPN	Same response.

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

USCA4 Appeal: 20-1191 Doc: 18-4 Filed: 07/01/2020 Pg: 58 of 549

EXHIBIT A

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with HTTPS Requests to Wikimedia Servers in United States from August 1, 2017 to January 31, 2018

1.	Afghanistan
2.	Åland
3.	Albania
4.	Algeria
5.	Andorra
6.	Angola
7.	Anguilla
8.	Antigua and Barbuda
9.	Argentina
10.	Armenia
11.	Aruba
12.	Australia
13.	Austria
14.	Azerbaijan
15.	Bahamas
16.	Bahrain
17.	Bangladesh
18.	Barbados
19.	Belarus
20.	Belgium
21.	Belize
22.	Benin
23.	Bermuda
24.	Bhutan
25.	Bolivia
26.	Bonaire, Sint Eustatius, and Saba
27.	Bosnia and Herzegovina
28.	Botswana
29.	Brazil
30.	British Indian Ocean Territory
31.	British Virgin Islands
32.	Brunei
33.	Bulgaria
34.	Burkina Faso
35.	Burundi
36.	Cabo Verde
37.	Cambodia
38.	Cameroon
39.	Canada
40.	Cayman Islands

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

41.	Central African Republic
42.	Chad
43.	Chile
44.	China
45.	Christmas Island
46.	Cocos [Keeling] Islands
47.	Colombia
48.	Comoros
49.	Congo
50.	Cook Islands
51.	Costa Rica
52.	Croatia
53.	Cuba
54.	Curaçao
55.	Cyprus
56.	Czechia
57.	Denmark
58.	Djibouti
59.	Dominica
60.	Dominican Republic
61.	East Timor
62.	Ecuador
63.	Egypt
64.	El Salvador
65.	Equatorial Guinea
66.	Eritrea
67.	Estonia
68.	Ethiopia
69.	Falkland Islands
70.	Faroe Islands
71.	Federated States of Micronesia
72.	Fiji
73.	Finland
74.	France
75.	French Guiana
76.	French Polynesia
77.	French Southern Territories
78.	Gabon
79.	Gambia
80.	Georgia
81.	Germany
82.	Ghana
83.	Gibraltar

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

84.	Greece
85.	Greenland
86.	Grenada
87.	Guadeloupe
88.	Guatemala
89.	Guernsey
90.	Guinea
91.	Guinea-Bissau
92.	Guyana
93.	Haiti
94.	Hashemite Kingdom of Jordan
95.	Honduras
96.	Hong Kong
97.	Hungary
98.	Iceland
99.	India
100.	Indonesia
101.	Iran
102.	Iraq
103.	Ireland
104.	Isle of Man
105.	Israel
106.	Italy
107.	Ivory Coast
108.	Jamaica
109.	Japan
110.	Jersey
111.	Kazakhstan
112.	Kenya
113.	Kiribati
114.	Kosovo
115.	Kuwait
116.	Kyrgyzstan
117.	Laos
118.	Latvia
119.	Lebanon
120.	Lesotho
121.	Liberia
122.	Libya
123.	Liechtenstein
124.	Luxembourg
125.	Macao
126.	Macedonia

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

127.	Madagascar
128.	Malawi
129.	Malaysia
130.	Maldives
131.	Mali
132.	Malta
133.	Marshall Islands
134.	Martinique
135.	Mauritania
136.	Mauritius
137.	Mayotte
138.	Mexico
139.	Monaco
140.	Mongolia
141.	Montenegro
142.	Montserrat
143.	Morocco
144.	Mozambique
145.	Myanmar [Burma]
146.	Namibia
147.	Nauru
148.	Nepal
149.	Netherlands
150.	New Caledonia
151.	New Zealand
152.	Nicaragua
153.	Niger
154.	Nigeria
155.	Niue
156.	Norfolk Island
157.	North Korea
158.	Norway
159.	Oman
160.	Pakistan
161.	Palau
162.	Palestine
163.	Panama
164.	Papua New Guinea
165.	Paraguay
166.	Peru
167.	Philippines
168.	Pitcairn Islands
169.	Poland

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

170.	Portugal
171.	Qatar
172.	Republic of Korea
173.	Republic of Lithuania
174.	Republic of Moldova
175.	Republic of the Congo
176.	Romania
177.	Russia
178.	Rwanda
179.	Réunion
180.	Saint Helena
181.	Saint Kitts and Nevis
182.	Saint Lucia
183.	Saint Martin
184.	Saint Pierre and Miquelon
185.	Saint Vincent and the Grenadines
186.	Saint Barthélemy
187.	Samoa
188.	San Marino
189.	Saudi Arabia
190.	Senegal
191.	Serbia
192.	Seychelles
193.	Sierra Leone
194.	Singapore
195.	Sint Maarten
196.	Slovak Republic
197.	Slovakia
198.	Slovenia
199.	Solomon Islands
200.	Somalia
201.	South Africa
202.	South Georgia and the South Sandwich Islands
203.	South Sudan
204.	Spain
205.	Sri Lanka
206.	St Kitts and Nevis
207.	Sudan
208.	Suriname
209.	Svalbard and Jan Mayen
210.	Swaziland
211.	Sweden

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

212.	Switzerland
213.	Syria
214.	São Tomé and Príncipe
215.	Taiwan
216.	Tajikistan
217.	Tanzania
218.	Thailand
219.	Togo
220.	Tokelau
221.	Tonga
222.	Trinidad and Tobago
223.	Tunisia
224.	Turkey
225.	Turkmenistan
226.	Turks and Caicos Islands
227.	Tuvalu
228.	Uganda
229.	Ukraine
230.	United Arab Emirates
231.	United Kingdom
232.	Uruguay
233.	Uzbekistan
234.	Vanuatu
235.	Vatican City
236.	Venezuela
237.	Vietnam
238.	Wallis and Futuna
239.	Western Sahara
240.	Yemen
241.	Zambia
242.	Zimbabwe

EXHIBIT B

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with HTTP Requests to Wikimedia Servers in United States from August 1, 2017 to January 31, 2018

1.	Afghanistan
2.	Åland
3.	Albania
4.	Algeria
5.	Andorra
6.	Angola
7.	Anguilla
8.	Antigua and Barbuda
9.	Argentina
10.	Armenia
11.	Aruba
12.	Australia
13.	Austria
14.	Azerbaijan
15.	Bahamas
16.	Bahrain
17.	Bangladesh
18.	Barbados
19.	Belarus
20.	Belgium
21.	Belize
22.	Benin
23.	Bermuda
24.	Bhutan
25.	Bolivia
26.	Bonaire, Sint Eustatius, and Saba
27.	Bosnia and Herzegovina
28.	Botswana
29.	Brazil
30.	British Indian Ocean Territory
31.	British Virgin Islands
32.	Brunei
33.	Bulgaria
34.	Burkina Faso
35.	Burundi
36.	Cabo Verde
37.	Cambodia
38.	Cameroon
39.	Canada
40.	Cayman Islands

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

41.	Central African Republic
42.	Chad
43.	Chile
44.	China
45.	Christmas Island
46.	Cocos [Keeling] Islands
47.	Colombia
48.	Comoros
49.	Congo
50.	Cook Islands
51.	Costa Rica
52.	Croatia
53.	Cuba
54.	Curaçao
55.	Cyprus
56.	Czechia
57.	Denmark
58.	Djibouti
59.	Dominica
60.	Dominican Republic
61.	East Timor
62.	Ecuador
63.	Egypt
64.	El Salvador
65.	Equatorial Guinea
66.	Eritrea
67.	Estonia
68.	Ethiopia
69.	Falkland Islands
70.	Faroe Islands
71.	Federated States of Micronesia
72.	Fiji
73.	Finland
74.	France
75.	French Guiana
76.	French Polynesia
77.	French Southern Territories
78.	Gabon
79.	Gambia
80.	Georgia
81.	Germany
82.	Ghana
83.	Gibraltar

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

84.	Greece
85.	Greenland
86.	Grenada
87.	Guadeloupe
88.	Guatemala
89.	Guernsey
90.	Guinea
91.	Guinea-Bissau
92.	Guyana
93.	Haiti
94.	Hashemite Kingdom of Jordan
95.	Honduras
96.	Hong Kong
97.	Hungary
98.	Iceland
99.	India
100.	Indonesia
101.	Iran
102.	Iraq
103.	Ireland
104.	Isle of Man
105.	Israel
106.	Italy
107.	Ivory Coast
108.	Jamaica
109.	Japan
110.	Jersey
111.	Kazakhstan
112.	Kenya
113.	Kiribati
114.	Kosovo
115.	Kuwait
116.	Kyrgyzstan
117.	Laos
118.	Latvia
119.	Lebanon
120.	Lesotho
121.	Liberia
122.	Libya
123.	Liechtenstein
124.	Luxembourg
125.	Macao
126.	Macedonia

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

127.	Madagascar
128.	Malawi
129.	Malaysia
130.	Maldives
131.	Mali
132.	Malta
133.	Marshall Islands
134.	Martinique
135.	Mauritania
136.	Mauritius
137.	Mayotte
138.	Mexico
139.	Monaco
140.	Mongolia
141.	Montenegro
142.	Montserrat
143.	Morocco
144.	Mozambique
145.	Myanmar [Burma]
146.	Namibia
147.	Nauru
148.	Nepal
149.	Netherlands
150.	New Caledonia
151.	New Zealand
152.	Nicaragua
153.	Niger
154.	Nigeria
155.	Niue
156.	Norfolk Island
157.	North Korea
158.	Norway
159.	Oman
160.	Pakistan
161.	Palau
162.	Palestine
163.	Panama
164.	Papua New Guinea
165.	Paraguay
166.	Peru
167.	Philippines
168.	Pitcairn Islands
169.	Poland

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

170.	Portugal
171.	Qatar
172.	Republic of Korea
173.	Republic of Lithuania
174.	Republic of Moldova
175.	Republic of the Congo
176.	Romania
177.	Russia
178.	Rwanda
179.	Réunion
180.	Saint Helena
181.	Saint Kitts and Nevis
182.	Saint Lucia
183.	Saint Martin
184.	Saint Pierre and Miquelon
185.	Saint Vincent and the Grenadines
186.	Saint Barthélemy
187.	Samoa
188.	San Marino
189.	Saudi Arabia
190.	Senegal
191.	Serbia
192.	Seychelles
193.	Sierra Leone
194.	Singapore
195.	Sint Maarten
196.	Slovak Republic
197.	Slovakia
198.	Slovenia
199.	Solomon Islands
200.	Somalia
201.	South Africa
202.	South Georgia and the South Sandwich Islands
203.	South Sudan
204.	Spain
205.	Sri Lanka
206.	St Kitts and Nevis
207.	Sudan
208.	Suriname
209.	Svalbard and Jan Mayen
210.	Swaziland
211.	Sweden

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

212.	Switzerland
213.	Syria
214.	São Tomé and Príncipe
215.	Taiwan
216.	Tajikistan
217.	Tanzania
218.	Thailand
219.	Togo
220.	Tokelau
221.	Tonga
222.	Trinidad and Tobago
223.	Tunisia
224.	Turkey
225.	Turkmenistan
226.	Turks and Caicos Islands
227.	Tuvalu
228.	Uganda
229.	Ukraine
230.	United Arab Emirates
231.	United Kingdom
232.	Uruguay
233.	Uzbekistan
234.	Vanuatu
235.	Vatican City
236.	Venezuela
237.	Vietnam
238.	Wallis and Futuna
239.	Western Sahara
240.	Yemen
241.	Zambia
242.	Zimbabwe

EXHIBIT C

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with Logged non-VPN TCP Connections to Wikimedia Office Router in United States from March 1, 2017 to February 28, 2018

1.	Andorra
2.	United Arab Emirates
3.	Afghanistan
4.	Antigua and Barbuda
5.	Albania
6.	Armenia
7.	Angola
8.	Antarctica
9.	Argentina
10.	Austria
11.	Australia
12.	Aruba
13.	Aland Islands
14.	Azerbaijan
15.	Bosnia and Herzegovina
16.	Barbados
17.	Bangladesh
18.	Belgium
19.	Burkina Faso
20.	Bulgaria
21.	Bahrain
22.	Burundi
23.	Benin
24.	Saint Bartelemey
25.	Bermuda
26.	Brunei Darussalam
27.	Bolivia
28.	Bonaire, Saint Eustatius and Saba
29.	Brazil
30.	Bahamas
31.	Bhutan
32.	Botswana
33.	Belarus
34.	Belize
35.	Canada
36.	Congo, The Democratic Republic of the
37.	Central African Republic
38.	Congo
39.	Switzerland
40.	Cote d'Ivoire

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

41.	Cook Islands
42.	Chile
43.	Cameroon
44.	China
45.	Colombia
46.	Costa Rica
47.	Cuba
48.	Cape Verde
49.	Curacao
50.	Christmas Island
51.	Cyprus
52.	Czech Republic
53.	Germany
54.	Djibouti
55.	Denmark
56.	Dominica
57.	Dominican Republic
58.	Algeria
59.	Ecuador
60.	Estonia
61.	Egypt
62.	Eritrea
63.	Spain
64.	Ethiopia
65.	Europe
66.	Finland
67.	Fiji
68.	France
69.	Gabon
70.	United Kingdom
71.	Grenada
72.	Georgia
73.	French Guiana
74.	Guernsey
75.	Ghana
76.	Gibraltar
77.	Greenland
78.	Gambia
79.	Guadeloupe
80.	Equatorial Guinea
81.	Greece
82.	Guatemala
83.	Guam

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

84.	Guyana
85.	Hong Kong
86.	Honduras
87.	Croatia
88.	Haiti
89.	Hungary
90.	Indonesia
91.	Ireland
92.	Israel
93.	Isle of Man
94.	India
95.	Iraq
96.	Iran, Islamic Republic of
97.	Iceland
98.	Italy
99.	Jersey
100.	Jamaica
101.	Jordan
102.	Japan
103.	Kenya
104.	Kyrgyzstan
105.	Cambodia
106.	Kiribati
107.	Comoros
108.	Saint Kitts and Nevis
109.	Korea, Democratic People's Republic of
110.	Korea, Republic of
111.	Kuwait
112.	Cayman Islands
113.	Kazakhstan
114.	Lao People's Democratic Republic
115.	Lebanon
116.	Saint Lucia
117.	Liechtenstein
118.	Sri Lanka
119.	Liberia
120.	Lesotho
121.	Lithuania
122.	Luxembourg
123.	Latvia
124.	Libyan Arab Jamahiriya
125.	Morocco
126.	Monaco

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

127.	Moldova, Republic of
128.	Montenegro
129.	Saint Martin
130.	Madagascar
131.	Marshall Islands
132.	Macedonia
133.	Mali
134.	Myanmar
135.	Mongolia
136.	Macao
137.	Northern Mariana Islands
138.	Martinique
139.	Mauritania
140.	Malta
141.	Mauritius
142.	Maldives
143.	Malawi
144.	Mexico
145.	Malaysia
146.	Mozambique
147.	Namibia
148.	New Caledonia
149.	Niger
150.	Nigeria
151.	Nicaragua
152.	Netherlands
153.	Norway
154.	Nepal
155.	New Zealand
156.	Oman
157.	Panama
158.	Peru
159.	French Polynesia
160.	Papua New Guinea
161.	Philippines
162.	Pakistan
163.	Poland
164.	Puerto Rico
165.	Palestinian Territory
166.	Portugal
167.	Palau
168.	Paraguay
169.	Qatar

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

170.	Reunion
171.	Romania
172.	Serbia
173.	Russian Federation
174.	Rwanda
175.	Saudi Arabia
176.	Solomon Islands
177.	Seychelles
178.	Sudan
179.	Sweden
180.	Singapore
181.	Slovenia
182.	Slovakia
183.	Sierra Leone
184.	Senegal
185.	Somalia
186.	Suriname
187.	South Sudan
188.	Sao Tome and Principe
189.	El Salvador
190.	Sint Maarten
191.	Syrian Arab Republic
192.	Swaziland
193.	Turks and Caicos Islands
194.	Chad
195.	Togo
196.	Thailand
197.	Tajikistan
198.	Turkmenistan
199.	Tunisia
200.	Tonga
201.	Turkey
202.	Trinidad and Tobago
203.	Taiwan
204.	Tanzania, United Republic of
205.	Ukraine
206.	Uganda
207.	Uruguay
208.	Uzbekistan
209.	Holy See (Vatican City State)
210.	Saint Vincent and the Grenadines
211.	Venezuela
212.	Virgin Islands, British

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

213.	Virgin Islands, U.S.
214.	Vietnam
215.	Vanuatu
216.	Samoa
217.	Kosovo
218.	Yemen
219.	South Africa
220.	Zambia
221.	Zimbabwe

EXHIBIT D

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with Logged VPN TCP Connections to Wikimedia Office Router in United States from March 1, 2017 to February 28, 2018

1.	United Arab Emirates
2.	Bulgaria
3.	Brazil
4.	Canada
5.	Switzerland
6.	China
7.	Colombia
8.	Germany
9.	Spain
10.	France
11.	United Kingdom
12.	Greece
13.	Hong Kong
14.	Ireland
15.	Iceland
16.	Japan
17.	Korea, Republic of
18.	Latvia
19.	Moldova, Republic of
20.	Mongolia
21.	Nigeria
22.	Netherlands
23.	Portugal
24.	Romania
25.	Russian Federation
26.	Seychelles
27.	Singapore
28.	Ukraine
29.	Uzbekistan

EXHIBIT E

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with Logged non-VPN UDP Connections to Wikimedia Office Router in United States from March 1, 2017 to February 28, 2018

1.	United Arab Emirates
2.	Antigua and Barbuda
3.	Anguilla
4.	Albania
5.	Armenia
6.	Angola
7.	Antarctica
8.	Argentina
9.	Austria
10.	Australia
11.	Aruba
12.	Aland Islands
13.	Azerbaijan
14.	Bosnia and Herzegovina
15.	Barbados
16.	Bangladesh
17.	Belgium
18.	Burkina Faso
19.	Bulgaria
20.	Bahrain
21.	Burundi
22.	Benin
23.	Bermuda
24.	Brunei Darussalam
25.	Bolivia
26.	Bonaire, Saint Eustatius and Saba
27.	Brazil
28.	Bahamas
29.	Bhutan
30.	Botswana
31.	Belarus
32.	Belize
33.	Canada
34.	Switzerland
35.	Cote d'Ivoire
36.	Cook Islands
37.	Chile
38.	Cameroon
39.	China
40.	Colombia

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

41.	Costa Rica
42.	Cuba
43.	Cape Verde
44.	Curacao
45.	Cyprus
46.	Czech Republic
47.	Germany
48.	Denmark
49.	Dominica
50.	Dominican Republic
51.	Algeria
52.	Ecuador
53.	Estonia
54.	Egypt
55.	Spain
56.	Ethiopia
57.	Europe
58.	Finland
59.	Fiji
60.	France
61.	Gabon
62.	United Kingdom
63.	Grenada
64.	Georgia
65.	French Guiana
66.	Guernsey
67.	Ghana
68.	Gibraltar
69.	Greenland
70.	Guinea
71.	Guadeloupe
72.	Greece
73.	Guatemala
74.	Guam
75.	Guyana
76.	Hong Kong
77.	Honduras
78.	Croatia
79.	Hungary
80.	Indonesia
81.	Ireland
82.	Israel
83.	Isle of Man

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

84.	India
85.	Iraq
86.	Iran, Islamic Republic of
87.	Iceland
88.	Italy
89.	Jersey
90.	Jamaica
91.	Jordan
92.	Japan
93.	Kenya
94.	Kyrgyzstan
95.	Cambodia
96.	Comoros
97.	Saint Kitts and Nevis
98.	Korea, Democratic People's Republic of
99.	Korea, Republic of
100.	Kuwait
101.	Cayman Islands
102.	Kazakhstan
103.	Lao People's Democratic Republic
104.	Lebanon
105.	Saint Lucia
106.	Liechtenstein
107.	Sri Lanka
108.	Lithuania
109.	Luxembourg
110.	Latvia
111.	Libyan Arab Jamahiriya
112.	Morocco
113.	Monaco
114.	Moldova, Republic of
115.	Montenegro
116.	Saint Martin
117.	Madagascar
118.	Macedonia
119.	Myanmar
120.	Mongolia
121.	Macao
122.	Martinique
123.	Mauritania
124.	Montserrat
125.	Malta
126.	Mauritius

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

127.	Maldives
128.	Malawi
129.	Mexico
130.	Malaysia
131.	Mozambique
132.	Namibia
133.	New Caledonia
134.	Niger
135.	Nigeria
136.	Nicaragua
137.	Netherlands
138.	Norway
139.	Nepal
140.	Nauru
141.	New Zealand
142.	Oman
143.	Panama
144.	Peru
145.	French Polynesia
146.	Philippines
147.	Pakistan
148.	Poland
149.	Puerto Rico
150.	Palestinian Territory
151.	Portugal
152.	Paraguay
153.	Qatar
154.	Reunion
155.	Romania
156.	Serbia
157.	Russian Federation
158.	Rwanda
159.	Saudi Arabia
160.	Seychelles
161.	Sudan
162.	Sweden
163.	Singapore
164.	Slovenia
165.	Slovakia
166.	Sierra Leone
167.	San Marino
168.	Senegal
169.	Somalia

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

170.	Suriname
171.	El Salvador
172.	Sint Maarten
173.	Syrian Arab Republic
174.	Swaziland
175.	Turks and Caicos Islands
176.	Chad
177.	Togo
178.	Thailand
179.	Tajikistan
180.	Tokelau
181.	Turkmenistan
182.	Tunisia
183.	Turkey
184.	Trinidad and Tobago
185.	Taiwan
186.	Tanzania, United Republic of
187.	Ukraine
188.	Uganda
189.	Uruguay
190.	Uzbekistan
191.	Holy See (Vatican City State)
192.	Saint Vincent and the Grenadines
193.	Venezuela
194.	Virgin Islands, British
195.	Virgin Islands, U.S.
196.	Vietnam
197.	Vanuatu
198.	Kosovo
199.	Yemen
200.	Mayotte
201.	South Africa
202.	Zambia
203.	Zimbabwe

EXHIBIT F

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with Logged VPN UDP Connections to Wikimedia Office Router in United States from March 1, 2017 to February 28, 2018

1.	Argentina
2.	Austria
3.	Australia
4.	Canada
5.	China
6.	Colombia
7.	Czech Republic
8.	Germany
9.	Denmark
10.	Egypt
11.	Spain
12.	France
13.	United Kingdom
14.	Greece
15.	Hungary
16.	Iran, Islamic Republic of
17.	Jordan
18.	Mexico
19.	Netherlands
20.	New Zealand
21.	Peru
22.	Poland
23.	Russian Federation
24.	Seychelles
25.	Sweden
26.	Turkey
27.	Uzbekistan

EXHIBIT G

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

List of Countries with Logged non-VPN ICMP Connections to Wikimedia Office Router in United States from August 1, 2017 to January 31, 2018

1.	United Arab Emirates
2.	Albania
3.	Armenia
4.	Argentina
5.	Austria
6.	Australia
7.	Azerbaijan
8.	Bosnia and Herzegovina
9.	Bangladesh
10.	Belgium
11.	Bulgaria
12.	Bolivia
13.	Brazil
14.	Belarus
15.	Canada
16.	Switzerland
17.	Chile
18.	China
19.	Colombia
20.	Costa Rica
21.	Czech Republic
22.	Germany
23.	Denmark
24.	Dominican Republic
25.	Ecuador
26.	Estonia
27.	Egypt
28.	Spain
29.	Europe
30.	Finland
31.	France
32.	United Kingdom
33.	Georgia
34.	Ghana
35.	Greece
36.	Guatemala
37.	Hong Kong
38.	Croatia
39.	Hungary
40.	Indonesia

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

41.	Ireland
42.	Israel
43.	India
44.	Iran, Islamic Republic of
45.	Iceland
46.	Italy
47.	Jordan
48.	Japan
49.	Kenya
50.	Kyrgyzstan
51.	Cambodia
52.	Korea, Republic of
53.	Kuwait
54.	Kazakhstan
55.	Lao People's Democratic Republic
56.	Lebanon
57.	Sri Lanka
58.	Lithuania
59.	Luxembourg
60.	Latvia
61.	Morocco
62.	Moldova, Republic of
63.	Macedonia
64.	Mongolia
65.	Mauritius
66.	Mexico
67.	Malaysia
68.	Mozambique
69.	New Caledonia
70.	Netherlands
71.	Norway
72.	Nepal
73.	New Zealand
74.	Peru
75.	French Polynesia
76.	Philippines
77.	Pakistan
78.	Poland
79.	Portugal
80.	Romania
81.	Serbia
82.	Russian Federation
83.	Rwanda

~~HIGHLY PROTECTED – ATTORNEYS' EYES ONLY~~
~~FOIA Confidential Treatment Request~~

84.	Saudi Arabia
85.	Seychelles
86.	Sudan
87.	Sweden
88.	Singapore
89.	Slovenia
90.	Slovakia
91.	El Salvador
92.	Thailand
93.	Tunisia
94.	Turkey
95.	Taiwan
96.	Tanzania, United Republic of
97.	Ukraine
98.	Uruguay
99.	Uzbekistan
100.	Venezuela
101.	Vietnam
102.	Vanuatu
103.	Kosovo
104.	South Africa
105.	Zimbabwe

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

Plaintiff's Exhibit 15

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.

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

Plaintiff's Exhibit 16

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.



MEMORANDUM OPINION

These matters are before the Foreign Intelligence Surveillance Court ("FISC" or "Court") on: (1) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications

[redacted], which was filed on April 20, 2011; (2) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [redacted], which was filed on April 22, 2011; and (3) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [redacted], which was also filed on April 22, 2011.[1]

Through these submissions, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA" or the "Act"), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth below, the government's requests for approval are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the "upstream collection" of Internet transactions containing multiple communications – is, in some respects, deficient on statutory and constitutional grounds.

[1] For ease of reference, the Court will refer to these three filings collectively as the "April 2011 Submissions."

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

I. BACKGROUND

A. The Certifications and Amendments

The April 2011 Submissions include DNI/AG 702(g) Certification [redacted] [redacted], all of which were executed by the Attorney General and the Director of National Intelligence ("DNI") pursuant to Section 702. [redacted] previous certifications have been submitted by the government and approved by the Court pursuant to Section 702. [redacted] (collectively, the "Prior 702 Dockets"). Each of the April 2011 Submissions also includes supporting affidavits by the Director or Acting Director of the National Security Agency ("NSA"), the Director of the Federal Bureau of Investigation ("FBI"), and the Director of the Central Intelligence Agency ("CIA"); two sets of targeting procedures, for use by NSA and FBI respectively; and three sets of minimization procedures, for use by NSA, FBI, and CIA, respectively.[2]

Like the acquisitions approved by the Court in the eight Prior 702 Dockets, collection

[2] The targeting and minimization procedures accompanying Certification [redacted] are identical to those accompanying [redacted] As discussed below, the NSA targeting procedures and FBI minimization procedures accompanying Certifications [redacted] also are identical to the NSA targeting procedures and FBI minimization procedures that were submitted by the government and approved by the Court for use in connection with Certifications [redacted]. The FBI targeting procedures and the NSA and CIA minimization procedures that accompany the April 2011 Submissions differ in several respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications [redacted].

under Certifications [redacted] is limited to "the targeting of non-United States persons reasonably believed to be located outside the United States." Certification [redacted]

The April 2011 Submissions also include amendments to certifications that have been submitted by the government and approved by the Court in the Prior 702 Dockets. The amendments, which have been authorized by the Attorney General and the DNI, provide that information collected under the certifications in the Prior 702 Dockets will, effective upon the Court's approval of Certifications [redacted], be handled subject to the same

revised NSA and CIA minimization procedures that have been submitted for use in connection with Certifications [redacted].

B. The May 2 "Clarification" Letter

On May 2, 2011, the government filed with the Court a letter pursuant to FISC Rule 13(a) titled "Clarification of National Security Agency's Upstream Collection Pursuant to Section 702 of FISA" ("May 2 Letter"). The May 2 Letter disclosed to the Court for the first time that NSA's "upstream collection"[3] of Internet communications includes the acquisition of entire "transaction[s]" (b) (1) (A) [redacted][4] According to the May 2 Letter, such transactions may contain data that is wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection. See id. at 2-3. The letter noted that NSA uses [redacted] to ensure that "the person from whom it seeks to obtain foreign intelligence information is located overseas," but suggested that the government might lack confidence in the effectiveness of such measures as applied to Internet transactions. See id. at 3 (citation omitted).

---

[3] The term "upstream collection" refers to NSA's interception of Internet communications as they transit (b) (1) (A) [redacted], rather than to acquisitions directly from Internet service providers such as [redacted].

[4] The concept of "Internet transactions" is discussed more fully below. See infra, pages 27-41 and note 23.

C. The Government's First Motion for Extensions of Time

On May 5, 2011, the government filed a motion seeking to extend until July 22, 2011, the 30-day periods in which the Court must otherwise complete its review of Certifications [redacted], and the amendments to the certifications in the Prior 702 Dockets. See Motion for an Order Extending Time Limit Pursuant to 50 U.S.C. § 1881a(j)(2) at 1 ("May Motion"). The period for FISC review of Certification [redacted] was then set to expire on May 20, 2011, and the period for review of the other pending certifications and amendments was set to expire on May 22, 2011. Id. at 6.[5]

The government noted in the May Motion that its efforts to address the issues raised in the May 2 Letter were still ongoing and that it intended to "supplement the record . . . in a manner that will aid the Court in its review" of the certifications and amendments and in making the determinations required under Section 702. Id. at 7. According to the May Motion, however, the government would "not be in a position to supplement the record until after the statutory time limits for such review have expired." Id. The government further asserted that granting the requested extension of time would be consistent with national security, because, by operation of

[5] 50 U.S.C. § 1881a(i)(1)(B) requires the Court to complete its review of the certification and accompanying targeting and minimization procedures and issue an order under subsection 1881a(i)(3) not later than 30 days after the date on which the certification and procedures are submitted. Pursuant to subsection 1881a(i)(1)(C), the same time limit applies to review of an amended certification or amended procedures. However, 50 U.S.C. § 1881a(j)(2) permits the Court, by order for reasons stated, to extend "as necessary for good cause in a manner consistent with national security," the time limit for the Court to complete its review and issue an order under Section 1881a(i)(3).

statute, the government's acquisition of foreign intelligence information under Certifications [redacted] could continue pending completion of the Court's review. See id. at 9-10.

On May 9, 2011, the Court entered orders granting the government's May Motion. Based upon the representations in the motion, the Court found that there was good cause to extend the time limit for its review of the certifications to July 22, 2011, and that the extensions were consistent with national security. May 9, 2011 Orders at 4.

D. The May 9 Briefing Order

Because it appeared to the Court that the acquisitions described in the May 2 Letter exceeded the scope of collection previously disclosed by the government and approved by the Court, and might, in part, fall outside the scope of Section 702, the Court issued a Briefing Order on May 9, 2011 ("Briefing Order"), in which it directed the government to answer a number of questions in writing. Briefing Order at 3-5. On June 1, 2011, the United States filed the "Government's Response to the Court's Briefing Order of May 9, 2011" ("June 1 Submission"). After reviewing the June 1 Submission, the Court, through its staff, directed the government to answer a number of follow-up questions. On June 28, 2011, the government submitted its written responses to the Court's follow-up questions in the "Government's Response to the Court's Follow-Up Questions of June 17, 2011" ("June 28 Submission").

E. The Government's Second Motion for Extensions of Time

The Court met with senior officials of the Department of Justice on July 8, 2011, to

discuss the information provided by the government in the June 1 and June 28 Submissions. During the meeting, the Court informed the government that it still had serious concerns regarding NSA's acquisition of Internet transactions and, in particular, whether the Court could make the findings necessary to approve the acquisition of such transactions pursuant to Section 702. The Court also noted its willingness to entertain any additional filings that the government might choose to make in an effort to address those concerns.

On July 14, 2011, the government filed a motion seeking additional sixty-day extensions of the periods in which the Court must complete its review of DNI/AG 702(g) Certifications [redacted], and the amendments to the certifications in the Prior 702 Dockets. Motion for Orders Extending Time Limits Pursuant to 50 U.S.C. § 1881a(j)(2) ("July Motion").[6]

In its July Motion, the government indicated that it was in the process of compiling additional information regarding the nature and scope of NSA's upstream collection, and that it was "examining whether enhancements to NSA's systems or processes could be made to further ensure that information acquired through NSA's upstream collection is handled in accordance with the requirements of the Act." Id. at 8. Because additional time would be needed to supplement the record, however, the government represented that a 60-day extension would be necessary. Id. at 8, 11. The government argued that granting the request for an additional extension of time would be consistent with national security, because, by operation of statute, the

---

[6] As discussed above, by operation of the Court's order of May 9, 2011, pursuant to 50 U.S.C. § 1881a(j)(2), the Court was required to complete its review of, and issue orders under 50 U.S.C.§ 1881a(i)(3) concerning, DNI/AG 702(g) Certifications [redacted] and the amendments to the certifications in the Prior 702 Dockets, by July 22, 2011. Id. at 6.

government's acquisition of foreign intelligence information under Certifications [redacted] could continue pending completion of the Court's review. Id. at 9-10.

On July 14, 2011, the Court entered orders granting the government's motion. Based upon the representations in the motion, the Court found that there was good cause to extend the time limit for its review of the certifications to September 20, 2011, and that the extensions were consistent with national security. July 14, 2011 Orders at 4.

F. The August 16 and August 30 Submissions

On August 16, 2011, the government filed a supplement to the June 1 and June 28 Submissions ("August 16 Submission"). In the August 16 Submission, the government described the results of "a manual review by [NSA] of a statistically representative sample of the nature and scope of the Internet communications acquired through NSA's . . . Section 702 upstream collection during a six-month period." Notice of Filing of Aug. 16 Submission at 2. Following a meeting between the Court staff and representatives of the Department of Justice on August 22, 2011, the government submitted a further filing on August 30, 2011 ("August 30 Submission").

G. The Hearing and the Government's Final Written Submission

Following review of the August 30 Submission, the Court held a hearing on September 7, 2011, to ask additional questions of NSA and the Department of Justice regarding the government's statistical analysis and the implications of that analysis. The government made its

final written submissions on September 9, 2011, and September 13, 2011 ("September 9 Submission" and "September 13 Submission," respectively).

H. The Final Extension of Time

On September 14, 2011, the Court entered orders further extending the deadline for its completion of the review of the certifications and amendments filed as part of the April Submissions. The Court explained that "[g]iven the complexity of the issues presented in these matters coupled with the Court's need to fully analyze the supplemental information provided by the government in recent filings, the last of which was submitted to the Court on September 13, 2011, the Court will not be able to complete its review of, and issue orders . . . concerning [the certifications and amendments] by September 20, 2011." [redacted] The Court further explained that although it had originally intended to extend the deadline by only one week, the government had advised the Court that "for technical reasons, such a brief extension would compromise the government's ability to ensure a seamless transition from one Certification to the next." [redacted] Accordingly, the Court extended the deadline to October 10, 2011. [redacted]

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

II. REVIEW OF CERTIFICATIONS [redacted]

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

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

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

(3) as required by 50 U.S.C. § 1881a(g)(2)(B), each of the certifications is accompanied by the applicable targeting procedures[7] and minimization procedures;[8]

(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);[9] and

(5) each of the certifications includes an effective date for the authorization in compliance

---

[7] See April 2011 Submissions, NSA Targeting Procedures and FBI Targeting Procedures (attached to Certifications [redacted]).

[8] See April 2011 Submissions, NSA Minimization Procedures, FBI Minimization Procedures, and CIA Minimization Procedures (attached to Certifications [redacted].

[9] See April 2011 Submissions, Affidavits of John C. Inglis, Acting Director, NSA (attached to Certifications [redacted]); Affidavit of Gen. Keith B. Alexander, U.S. Army, Director, NSA (attached to Certification [redacted]); Affidavits of Robert S. Mueller, III, Director, FBI (attached to Certifications [redacted]); Affidavits of Leon E. Panetta, Director, CIA [redacted]

with 50 U.S.C. § 1881a(g)(2)(D), see Certification [redacted].[10]

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

III. REVIEW OF THE AMENDMENTS TO THE CERTIFICATIONS IN THE PRIOR DOCKETS.

Under the judicial review procedures that apply to amendments by virtue of Section 1881a(i)(1)(C), the Court must review each of the amended certifications "to determine whether the certification contains all the required elements." 50 U.S.C. § 1881a(i)(2)(A). The Court has previously determined that the certifications in each of the Prior 702 Dockets, as originally submitted to the Court and previously amended, contained all the required elements.[11] Like the prior certifications and amendments, the amendments now before the Court were executed under oath by the Attorney General and the DNI, as required by 50 U.S.C. § 1881a(g)(1)(A), and submitted to the Court within the time allowed under 50 U.S.C. § 1881a(i)(1)(C). See

---

[10] 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).

[11] [redacted]

Certification [redacted][12] Pursuant to Section 1881a(g)(2)(A)(ii), the latest amendments include the attestations of the Attorney General and the DNI that the accompanying NSA and CIA minimization procedures meet the statutory definition of minimization procedures, are consistent with the requirements of the Fourth Amendment, and will be submitted to the Court for approval. Certification [redacted]. The latest amendments also include effective dates that comply with 50 U.S.C. § 1881a(g)(2)(D) and § 1881a(i)(1). Certification [redacted] All other aspects of the certifications in the Prior 702 Dockets – including the further attestations made therein in accordance with § 1881a(g)(2)(A), the NSA targeting procedures and FBI minimization procedures submitted therewith in accordance with § 1881a(g)(2)(B),[13] and the affidavits executed in support thereof in accordance with § 1881a(g)(2)(C) – are unaltered by the latest amendments.

In light of the foregoing, the Court finds that the certifications in the Prior 702 Dockets, as amended, each contain all the required elements. 50 U.S.C. § 1881a(i)(2)(A).

---

[12] The amendments to the certifications in the Prior 702 Dockets were approved by the Attorney General on April 11, 2011, and by the DNI on April 13, 2011. See Certification [redacted]

[13] Of course, targeting under the certifications filed in the Prior 702 Dockets will no longer be permitted following the Court's issuance of an order on Certifications [redacted]

IV. REVIEW OF THE TARGETING AND MINIMIZATION PROCEDURES

The Court is required 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). See 50 U.S.C. § 1881a(i)(2)(B) and (C); see also 50 U.S.C. § 1881a(i)(1)(C) (providing that amended procedures must be reviewed under the same standard). Section 1881a(d)(1) provides that the targeting procedures must be "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." Section 1881a(e)(1) requires that the minimization procedures "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4) . . . ." Most notably, that definition requires "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." 50 U.S.C. §§ 1801(h) & 1821(4). Finally, the Court must determine whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A).

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

A. The Effect of the Government's Disclosures Regarding NSA's Acquisition of Internet Transactions on the Court's Review of the Targeting and Minimization Procedures

The Court's review of the targeting and minimization procedures submitted with the April 2011 Submissions is complicated by the government's recent revelation that NSA's acquisition of Internet communications through its upstream collection under Section 702 is accomplished by acquiring Internet "transactions," which may contain a single, discrete communication, or multiple discrete communications, including communications that are neither to, from, nor about targeted facilities. June 1 Submission at 1-2. That revelation fundamentally alters the Court's understanding of the scope of the collection conducted pursuant to Section 702 and requires careful reexamination of many of the assessments and presumptions underlying its prior approvals.

In the first Section 702 docket, [redacted], the government disclosed that its Section 702 collection would include both telephone and Internet communications. According to the government, the acquisition of telephonic communications would be limited to "to/from" communications – i.e., communications to or from a tasked facility. The government explained, however, that the Internet communications acquired would include both to/from communications and "about" communications – i.e., communications containing a reference to the name of the tasked account. See [redacted]. Based upon the government's descriptions of the proposed collection, the Court understood that the acquisition of Internet communications under Section 702 would be limited to discrete "to/from" communications between or among individual account users and to "about"

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

communications falling within [redacted] specific categories that had been first described to the Court in prior proceedings. [redacted] Declaration of Director of NSA at 20-22. The Court's analysis and ultimate approval of the targeting and minimization procedures in Docket No. [redacted], and in the other [redacted] Prior 702 Dockets, depended upon the government's representations regarding the scope of the collection. In conducting its review and granting those approvals, the Court did not take into account NSA's acquisition of Internet transactions, which now materially and fundamentally alters the statutory and constitutional analysis.[14]

---

[14] The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.

In March, 2009, the Court concluded that its authorization of NSA's bulk acquisition of telephone call detail records from [redacted] in the so-called "big business records" matter "ha[d] been premised on a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." Docket No. BR 08-13, March 2, 2009 Order at 10-11. Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying. The Court concluded that this requirement had been "so frequently and systemically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively." Id.

Shortly thereafter, the government made a similar disclosure regarding NSA's bulk acquisition of metadata regarding Internet communications in the so-called "big pen register" matter. In [redacted] the government reported that, from the time of the initial Court authorization in 2004, NSA had been continually collecting various forms of data falling outside the scope of the Court's orders, and that "'[v]irtually every PR/TT record' generated by this program included some data that had not been authorized for collection." Docket No. PR/TT [redacted] Mem. Op. at 20-21. This long-running and systemic overcollection had

(continued...)

The government's submissions make clear not only that NSA has been acquiring Internet transactions since before the Court's approval of the first Section 702 certification in 2008,[15] but also that NSA seeks to continue the collection of Internet transactions. Because NSA's acquisition of Internet transactions presents difficult questions, the Court will conduct its review in two stages. Consistent with the approach it has followed in past reviews of Section 702 certifications and amendments, the Court will first consider the targeting and minimization procedures as applied to the acquisition of communications other than Internet transactions – i.e., to the discrete communications between or among the users of telephone and Internet communications facilities that are to or from a facility tasked for collection.[16] The Court will

---

[14](...continued)
occurred despite the government's repeated assurances over the course of nearly [redacted] years that [redacted] authorizations granted by docket number PR/TT [redacted] and previous docket numbers only collect, or collected, authorized metadata." Id. at 20. The overcollection was not detected by NSA until after an "end-to-end review" of the PR/TT metadata program that had been completed by the agency on August 11, 2009. Id.

[15] The government's revelations regarding the scope of NSA's upstream collection implicate 50 U.S.C. § 1809(a), which makes it a crime (1) to "engage[] in electronic surveillance under color of law except as authorized" by statute or (2) to "disclose[] or use[] 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 statute. See [redacted] (concluding that Section 1809(a)(2) precluded the Court from approving the government's proposed use of, among other things, certain data acquired by NSA without statutory authority through its "upstream collection"). The Court will address Section 1809(a) and related issues in a separate order.

[16] As noted, the Court previously authorized the acquisition of [redacted] categories of "about" communications. The Court now understands that all "about" communications are acquired by means of NSA's acquisition of Internet transactions through its upstream collection. See June 1 Submission at 1-2, see also Sept. 7, 2011 Hearing Tr. at 76. Accordingly, the Court considers the (continued...)

then assess the effect of the recent disclosures regarding NSA's collection of Internet transactions on its ability to make the findings necessary to approve the certifications and the NSA targeting and minimization procedures.[17]

B. The Unmodified Procedures

The government represents that the NSA targeting procedures and the FBI minimization procedures filed with the April 2011 Submissions are identical to the corresponding procedures that were submitted to the Court in Docket Nos. [redacted][18] The Court has reviewed each of these sets of procedures and confirmed that is the case. In fact, the NSA targeting procedures and FBI minimization procedures now before the Court are copies

---

[16](...continued)
[redacted]categories of "about" communications to be a subset of the Internet transactions that NSA acquires. The Court's discussion of the manner in which the government proposes to apply its targeting and minimization procedures to Internet transactions generally also applies to the [redacted] categories of "about" communications. See infra, pages 41-79.

[17] The FBI and the CIA do not receive unminimized communications that have been acquired through NSA's upstream collection of Internet communications. Sept. 7, 2011 Hearing Tr. at 61-62. Accordingly, the discussion of Internet transactions that appears below does not affect the Court's conclusions that the FBI targeting procedures, the CIA minimization procedures, and the FBI minimization procedures meet the statutory and constitutional requirements.

[18] See Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [redacted]; Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [redacted]; Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications for DNI/AG 702(g) Certifications [redacted].

of the procedures that were initially filed on July 29, 2009, in Docket No. [redacted][19] The Court found in those prior dockets that the targeting and minimization procedures were consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment. See Docket No. [redacted] The Court is prepared to renew its past findings that the NSA targeting procedures (as applied to forms of to/from communications that have previously been described to the Court) and the FBI minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.[20]

C. The Amended Procedures

As noted above, the FBI targeting procedures and the NSA and CIA minimization procedures submitted with the April 2011 Submissions differ in a number of respects from the corresponding procedures that were submitted by the government and approved by the Court in connection with Certifications [redacted]. For the reasons that follow, the Court finds that, as applied to the previously authorized collection of discrete communications to or from a tasked facility, the amended FBI targeting procedures and the amended NSA and CIA

---

[19] Copies of those same procedures were also submitted in Docket Nos. [redacted]

[20] The Court notes that the FBI minimization procedures are not "set forth in a clear and self-contained manner, without resort to cross-referencing," as required by FISC Rule 12, which became effective on November 1, 2010. The Court expects that future submissions by the government will comport with this requirement.

minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(d)-(e) and with the Fourth Amendment.

1. The Amended FBI Targeting Procedures

The government has made three changes to the FBI targeting procedures, all of which involve Section I.4. That provision requires the FBI, [redacted]

The new language proposed by the government would allow the FBI to [redacted] The government has advised the Court that this change was prompted by the fact that [redacted] Nevertheless, the current procedures require the FBI to [redacted]. The change is intended to eliminate the requirement of [redacted].

The second change, reflected in subparagraph (a) of Section I.4, would allow the FBI, under certain circumstances, to [redacted]

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

[redacted]

The above-described changes to the FBI targeting procedures pose no obstacle to a finding by the Court that the FBI targeting procedures are "reasonably designed" to "ensure that any acquisition authorized . . . is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). [redacted]

[redacted]

Furthermore, as the Court has previously noted, before the FBI targeting procedures are applied, NSA will have followed its own targeting procedures in determining that the user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States. See Docket No. [redacted]. The FBI targeting procedures apply in addition to the NSA targeting procedures, [redacted] Id. The Court has previously found that the NSA targeting procedures proposed for use in connection with Certifications [redacted] are reasonably designed to ensure that the users of tasked selectors are non-United States persons reasonably believed to be located outside the United States and also consistent with the Fourth Amendment. See Docket No. [redacted]. It therefore follows that the amended FBI targeting procedures, which provide additional assurance that the users of tasked accounts are non-United States persons located outside the United States, also pass muster.

2. The Amended NSA Minimization Procedures

The most significant change to the NSA minimization procedures regards the rules for querying the data that NSA acquires pursuant to Section 702. The procedures previously approved by the Court effectively impose a wholesale bar on queries using United States-Person identifiers. The government has broadened Section 3(b)(5) to allow NSA to query the vast majority of its Section 702 collection using United States-Person identifiers, subject to approval

pursuant to internal NSA procedures and oversight by the Department of Justice.[21] Like all other NSA queries of the Section 702 collection, queries using United States-person identifiers would be limited to those reasonably likely to yield foreign intelligence information. NSA Minimization Procedures § 3(b)(5). The Department of Justice and the Office of the DNI would be required to conduct oversight regarding NSA's use of United States-person identifiers in such queries. See id.

This relaxation of the querying rules does not alter the Court's prior conclusion that NSA minimization procedures meet the statutory definition of minimization procedures. The Standard Minimization Procedures for FBI Electronic Surveillance and Physical Search Conducted Under the Foreign Intelligence Surveillance Act ("FBI SMPs") contain an analogous provision allowing queries of unminimized FISA-acquired information using identifiers – including United States-person identifiers – when such queries are designed to yield foreign intelligence information. See FBI SMPs § III.D. In granting hundreds of applications for electronic surveillance or physical search since 2008, including applications targeting United States persons and persons in the United States, the Court has found that the FBI SMPs meet the definitions of minimization procedures at 50 U.S.C. §§ 1801(h) and 1821(4). It follows that the substantially-similar

---

[21] The government is still in the process of developing its internal procedures and will not permit NSA analysts to begin using United States-person identifiers as selection terms until those procedures are completed. June 28 Submission at 4 n.3. In addition, the government has clarified that United States-person identifiers will not be used to query the fruits of NSA's upstream collection. Aug. 30 Submission at 11. NSA's upstream collection acquires approximately 9% of the total Internet communications acquired by NSA under Section 702. Aug. 16 Submission at 2.

querying provision found at Section 3(b)(5) of the amended NSA minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons.

A second change to the NSA minimization procedures is the addition of language specifying that the five-year retention period for communications that are not subject to earlier destruction runs from the expiration date of the certification authorizing the collection. See NSA Minimization Procedures, §§ 3(b)(1), 3(c), 5(3)(b), and 6(a)(1)(b). The NSA minimization procedures that were previously approved by the Court included a retention period of five years, but those procedures do not specify when the five-year period begins to run. The change proposed here harmonizes the procedures with the corresponding provision of the FBI minimization procedures for Section 702 that has already been approved by the Court. See FBI Minimization Procedures at 3 (¶ j).

The two remaining changes to the NSA minimization procedures are intended to clarify the scope of the existing procedures. The government has added language to Section 1 to make explicit that the procedures apply not only to NSA employees, but also to any other persons engaged in Section 702-related activities that are conducted under the direction, authority or control of the Director of NSA. NSA Minimization Procedures at 1. According to the government, this new language is intended to clarify that Central Security Service personnel conducting signals intelligence operations authorized by Section 702 are bound by the procedures, even when they are deployed with a military unit and subject to the military chain of

command. The second clarifying amendment is a change to the definition of "identification of a United States person" in Section 2. The new language eliminates a potential ambiguity that might have resulted in the inappropriate treatment of the name, unique title, or address of a United States person as non-identifying information in certain circumstances. Id. at 2. These amendments, which resolve any arguable ambiguity in favor of broader application of the protections found in the procedures, raise no concerns.

3. The Amended CIA Minimization Procedures

The CIA minimization procedures include a new querying provision similar to the provision that the government proposes to add to the NSA minimization procedures and that is discussed above. CIA Minimization Procedures § 4. The new language would allow the CIA to conduct queries of Section 702-acquired information using United States-person identifiers. All CIA queries of the Section 702 collection would be subject to review by the Department of Justice and the Office of the DNI. See id. For the reasons stated above with respect to the relaxed querying provision in the amended NSA minimization procedures, the addition of the new CIA querying provision does not preclude the Court from concluding that the amended CIA minimization procedures satisfy the statutory definition of minimization procedures and comply with the Fourth Amendment.[22]

The amended CIA minimization procedures include a definition of "United States person identity," a term that is not defined in the current version of the procedures. CIA Minimization

---

[22] The Court understands that NSA does not share its upstream collection in unminimized form with the CIA. [redacted]

Procedures § 1.b. The proposed definition closely tracks the revised definition of "identification of a United States person" that is included in the amended NSA minimization procedures and discussed above. For the same reasons, the addition of this definition, which clarifies the range of protected information, raises no concerns in the context of the CIA minimization procedures.

Another new provision of the CIA minimization procedures prescribes the manner in which the CIA must store unminimized Section 702-acquired communications. See CIA Minimization Procedures § 2. The same provision establishes a default retention period for unminimized communications that do not qualify for longer retention under one of three separate provisions. See id. Absent an extension by the Director of the National Clandestine Service or one of his superiors, that default retention period is five years from the date of the expiration of the certification authorizing the collection. Id. As noted above, this is the same default retention period that appears in the FBI minimization procedures that have previously been approved by the Court. See FBI Minimization Procedures at 3 (¶ j).

The government also has added new language to the CIA minimization procedures to clarify that United States person information deemed to qualify for retention based on its public availability or on the consent of the person to whom it pertains may be kept indefinitely and stored separately from the unminimized information subject to the default storage and retention rules set forth in new Section 2, which is discussed above. CIA Minimization Procedures § 2. Because FISA's minimization requirements are limited to the acquisition, retention, and dissemination of "nonpublicly available information concerning unconsenting United States persons," this provision raises no statutory concern. See 50 U.S.C. §§ 1801(h)(1), 1821(4)(A)

(emphasis added). It likewise raises no Fourth Amendment problem. See Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.").

Finally, a new provision would expressly allow the CIA to retain information acquired pursuant to Section 702 in emergency backup systems that may be used to restore data in the event of a system failure. CIA Minimization Procedures § 6(e). Only non-analyst technical personnel will have access to data stored in data backup systems. Id. Further, in the event that such systems are used to restore lost, destroyed, or inaccessible data, the CIA must apply its minimization procedures to the transferred data. Id. The FBI minimization procedures that have previously been approved by the Court contemplate the storage of Section 702 collection in emergency backup systems that are not accessible to analysts, subject to similar restrictions. See FBI Minimization Procedures at 2 (¶ e.3). The Court likewise sees no problem with the addition of Section 6(e) to the CIA minimization procedures.

D. The Effect of the Government's Disclosures Regarding NSA's Acquisition of Internet Transactions

Based on the government's prior representations, the Court has previously analyzed NSA's targeting and minimization procedures only in the context of NSA acquiring discrete communications. Now, however, in light of the government's revelations as to the manner in which NSA acquires Internet communications, it is clear that NSA acquires "Internet

transactions,"[23] including transactions that contain a single discrete communication ("Single Communication Transactions" or "SCTs"), and transactions that contain multiple discrete communications ("Multi-[C]ommunication Transactions" or "MCTs"), see Aug. 16 Submission at 1.

The Court has repeatedly noted that the government's targeting and minimization procedures must be considered in light of the communications actually acquired. See Docket No. [redacted] ("Substantial 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."), see also Docket No. [redacted] Until now, the Court had a singular understanding of the nature of NSA's acquisitions under Section 702. Accordingly, analysis of the implementation of the procedures focused on whether NSA's procedures were applied effectively in that context and whether the procedures adequately addressed over-collections that occurred. But, for the first time, the government has now advised the Court that the volume and nature of the information it has been collecting is fundamentally different from what the Court had been led to believe. Therefore, the Court must, as a matter of first impression, consider whether, in view of NSA's acquisition of Internet transactions, the targeting and minimization procedures satisfy the statutory standards and comport with the

[23] 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." June 1 Submission at 1.

Fourth Amendment.

For the reasons set forth below, the Court finds that NSA's targeting procedures, as the government proposes to implement them in connection with MCTs, are consistent with the requirements of 50 U.S.C. §1881a(d)(1). However, the Court is unable to find that NSA's minimization procedures, as the government proposes to apply them in connection with MCTs, 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." 50 U.S.C. §§ 1801(h)(1) &1821(4)(A). The Court is also unable to find that NSA's targeting and minimization procedures, as the government proposes to implement them in connection with MCTs, are consistent with the Fourth Amendment.

1. The Scope of NSA's Upstream Collection

NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702, but the vast majority of these communications are obtained from Internet service providers and are not at issue here.[24] Sept. 9 Submission at 1; Aug. 16 Submission at Appendix A. Indeed, NSA's upstream collection constitutes only approximately

[24] In addition to its upstream collection, NSA acquires discrete Internet communications from Internet service providers such as [redacted] Aug. 16 Submission at 2; Aug. 30 Submission at 11; see also Sept. 7, 2011 Hearing Tr. at 75-77. NSA refers to this non-upstream collection as its "PRISM collection." Aug. 30 Submission at 11. The Court understands that NSA does not acquire "Internet transactions" through its PRISM collection. See Aug. 16 Submission at 1.

9% of the total Internet communications being acquired by NSA under Section 702. Sept. 9 Submission at 1; Aug. 16 Submission at 2.

Although small in relative terms, NSA's upstream collection is significant for three reasons. First, NSA's upstream collection is "uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information."[25] Docket No. [redacted]. Second, the Court now understands that, in order to collect those targeted Internet communications, NSA's upstream collection devices acquire Internet transactions, and NSA acquires millions of such transactions each year.[26] Third, the government has acknowledged that, due to the technological challenges associated with acquiring Internet transactions, NSA is unable to exclude certain Internet transactions from its upstream collection. See June 1 Submission at 3-12.

In its June 1 Submission, the government explained that NSA's upstream collection devices have technological limitations that significantly affect the scope of collection. [redacted]

[25] [redacted]

[26] NSA acquired more than 13.25 million Internet transactions through its upstream collection between January 1, 2011, and June 30, 2011. See Aug. 16 Submission at 2; see also Sept. 9 Submission at 1-2.

[redacted]. See id. at 7. Moreover, at the time of acquisition, 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 may be to, from, or about a tasked selector.[27] Id. at 2.

As a practical matter, this means that NSA's upstream collection devices acquire any Internet transaction transiting the device if the transaction contains a targeted selector anywhere within it, and:

[redacted]

See id. at 6.

The practical implications of NSA's acquisition of Internet transactions through its upstream collection for the Court's statutory and Fourth Amendment analyses are difficult to assess. The sheer volume of transactions acquired by NSA through its upstream collection is such that any meaningful review of the entire body of the transactions is not feasible. As a result, the Court cannot know for certain the exact number of wholly domestic communications acquired through this collection, nor can it know the number of non-target communications

[redacted]

acquired or the extent to which those communications are to or from United States persons or persons in the United States. Instead, NSA and the Court can only look at samples of the data and then draw whatever reasonable conclusions they can from those samples. Even if the Court accepts the validity of conclusions derived from statistical analyses, there are significant hurdles in assessing NSA's upstream collection. Internet service providers are constantly changing their protocols and the services they provide, and often give users the ability to customize how they use a particular service.[28] Id. at 24-25. As a result, it is impossible to define with any specificity the universe of transactions that will be acquired by NSA's upstream collection at any point in the future.

Recognizing that further revelations concerning what NSA has actually acquired through its 702 collection, together with the constant evolution of the Internet, may alter the Court's analysis at some point in the future, the Court must, nevertheless, consider whether NSA's targeting and minimization procedures are consistent with FISA and the Fourth Amendment based on the record now before it. In view of the revelations about how NSA is actually conducting its upstream collection, two fundamental underpinnings of the Court's prior assessments no longer hold true.

---

28 [redacted]

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

First, the Court previously understood that NSA's technical measures[29] would prevent the acquisition of any communication as to which the sender and all intended recipients were located in the United States ("wholly domestic communication") except for "theoretically possible" cases [redacted] The Court now understands, however, that NSA has acquired, is acquiring, and, if the certifications and procedures now before the Court are approved, will continue to acquire, tens of thousands of wholly domestic communications. NSA's manual review of a statistically representative sample drawn from its upstream collection[30] reveals that NSA acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication.[31] See Aug. 16 Submission at 9. In addition to these MCTs, NSA

[29] [redacted]

[30] In an effort to address the Court's concerns, NSA conducted a manual review of a random sample consisting of 50,440 Internet transactions taken from the more than 13.25 million Internet transactions acquired through NSA's upstream collection during a six month period. See generally Aug. 16 Submission (describing NSA's manual review and the conclusions NSA drew therefrom). The statistical conclusions reflected in this Memorandum Opinion are drawn from NSA's analysis of that random sample.

[31] Of the approximately 13.25 million Internet transactions acquired by NSA through its upstream collection during the six-month period, between 996 and 4,965 are MCTs that contain a wholly domestic communication not to, from, or about a tasked selector. Aug. 16 Submission at 9.

likely acquires tens of thousands more wholly domestic communications every year,[32] given that NSA's upstream collection devices will acquire a wholly domestic "about" SCT if it is routed internationally.[33] Moreover, the actual number of wholly domestic communications acquired

---

[32] NSA's manual review focused on examining the MCTs acquired through NSA's upstream collection in order to assess whether any contained wholly domestic communications. Sept. 7, 2011 Hearing Tr. at 13-14. As a result, once NSA determined that a transaction contained a single, discrete communication, no further analysis of that transaction was done. See Aug. 16 Submission at 3. After the Court expressed concern that this category of transactions might also contain wholly domestic communications, NSA conducted a further review. See Sept. 9 Submission at 4. NSA ultimately did not provide the Court with an estimate of the number of wholly domestic "about" SCTs that may be acquired through its upstream collection. Instead, NSA has concluded that "the probability of encountering wholly domestic communications in transactions that feature only a single, discrete communication should be smaller – and certainly no greater – than potentially encountering wholly domestic communications within MCTs." Sept. 13 Submission at 2.

The Court understands this to mean that the percentage of wholly domestic communications within the universe of SCTs acquired through NSA's upstream collection should not exceed the percentage of MCTs containing a wholly domestic communication that NSA found when it examined all of the MCTs within its statistical sample. Since NSA found 10 MCTs with wholly domestic communications within the 5,081 MCTs reviewed, the relevant percentage is .197% (10/5,081). Aug. 16 Submission at 5.

NSA's manual review found that approximately 90% of the 50,440 transactions in the sample were SCTs. Id. at 3. Ninety percent of the approximately 13.25 million total Internet transactions acquired by NSA through its upstream collection during the six-month period, works out to be approximately 11,925,000 transactions. Those 11,925,000 transactions would constitute the universe of SCTs acquired during the six-month period, and .197% of that universe would be approximately 23,000 wholly domestic SCTs. Thus, NSA may be acquiring as many as 46,000 wholly domestic "about" SCTs each year, in addition to the 2,000-10,000 MCTs referenced above.

[33] Internet communications are "nearly always transmitted from a sender to a recipient through multiple legs before reaching their final destination." June 1 Submission at 6. For example, an e-mail message sent from the user of [redacted] to the user of [redacted] will at the very least travel from the [redacted] user's own computer, to [redacted], to [redacted], and then to the computer of the [redacted] user. Id. Because the communication's route is made up of multiple legs, the transaction used to transmit the communication across any particular leg of the route need only identify the IP

(continued...)

may be still higher in view of NSA's inability conclusively to determine whether a significant portion of the MCTs within its sample contained wholly domestic communications.[34]

Second, the Court previously understood that NSA's upstream collection would only acquire the communication of a United States person or a person in the United States if: 1) that

---

[33](...continued)
addresses at either end of that leg in order to properly route the communication. Id. at 7. As a result, for each leg of the route, the transaction header will only contain the IP addresses at either end of that particular leg. Id. [redacted]

[34] During its manual review, NSA was unable to determine whether 224 of the 5,081 MCTs reviewed contained any wholly domestic communications, because the transactions lacked sufficient information for NSA to determine the location or identity of the "active user" (i.e., the individual using the electronic communications account/address/identifier to interact with his/her Internet service provider). Aug. 16 Submission at 7. NSA then conducted an intensive review of all available information for each of these MCTs, including examining the contents of each discrete communication contained within it, but was still unable to determine conclusively whether any of these MCTs contained wholly domestic communications. Sept. 9 Submission at 3. NSA asserts that "it is reasonable to presume that [the] 224 MCTs do not contain wholly domestic communications," but concedes that, due to the limitations of the technical means used to prevent the acquisition of wholly domestic communications, NSA may acquire wholly domestic communications. See Aug. 30 Submission at 7-8. The Court is prepared to accept that the number of wholly domestic communications acquired in this category of MCTs is relatively small, for the reasons stated in the government's August 30 Submission. However, when considering NSA's upstream collection as a whole, and the limitations of NSA's technical means, the Court is not prepared to presume that the number of wholly domestic communications contained within this category of communications will be zero. Accordingly, the Court concludes that this category of communications acquired through NSA's upstream collection may drive the total number of wholly domestic communications acquired slightly higher.

person was in direct contact with a targeted selector; 2) the communication referenced the targeted selector, and the communication fell into one of [redacted] specific categories of "about" communications; or 3) despite the operation of the targeting procedures, United States persons or persons inside the United States were mistakenly targeted. See Docket No. [redacted]. But the Court now understands that, in addition to these communications, NSA's upstream collection also acquires: a) the communications of United States persons and persons in the United States that are not to, from, or about a tasked selector and that are acquired solely because the communication is contained within an MCT that somewhere references a tasked selector [redacted] and b) any Internet transaction that references a targeted selector, regardless of whether the transaction falls within one of the [redacted] previously identified categories of "about communications," see June 1 Submission at 24-27. [redacted]

On the current record, it is difficult to assess how many MCTs acquired by NSA actually contain a communication of or concerning a United States person,[35] or a communication to or from a person in the United States. This is because NSA's manual review of its upstream collection focused primarily on wholly domestic communications – i.e., if one party to the

[35] NSA's minimization procedures define "[c]ommunications of a United States person" to include "all communications to which a United States person is a party." NSA Minimization Procedures § 2(c). "Communications concerning a United States person" include "all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person. Id. § 2(b).

communication was determined to be outside the United States, the communication was not further analyzed. Aug. 16 Submission at 1-2. Nevertheless, NSA's manual review did consider the location and identity of the active user for each MCT acquired, and this information – when considered together with certain presumptions – shows that NSA is likely acquiring tens of thousands of discrete communications of non-target United States persons and persons in the United States, by virtue of the fact that their communications are included in MCTs selected for acquisition by NSA's upstream collection devices.[36]

To illustrate, based upon NSA's analysis of the location and identity of the active user for the MCTs it reviewed, MCTs can be divided into four categories:

1. MCTs as to which the active user is the user of the tasked facility (i.e., the target of the acquisition) and is reasonably believed to be located outside the United States;[37]

2. MCTs as to which the active user is a non-target who is believed to be located inside the United States;

3. MCTs as to which the active user is a non-target who is believed to be located outside the United States; and

---

[36] Although there is some overlap between this category of communications and the tens of thousands of wholly domestic communications discussed above, the overlap is limited to MCTs containing wholly domestic communications. To the extent that the wholly domestic communications acquired are SCTs, they are excluded from the MCTs referenced here. Similarly, to the extent communications of non-target United States persons and persons in the United States that are contained within the tens of thousands of MCTs referenced here are not wholly domestic, they would not be included in the wholly domestic communications referenced above.

[37] Although it is possible for an active user target to be located in the United States, NSA's targeting procedures require NSA to terminate collection if it determines that a target has entered the United States. NSA Targeting Procedures at 7-8. Accordingly, the Court excludes this potential category from its analysis.

4. MCTs as to which the active user's identity or location cannot be determined.

Aug. 16 Submission at 4-8.

With regard to the first category, if 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 following categories because the communicants were in direct communication with a tasked facility, and the acquisition presumptively serves the foreign intelligence purpose of the collection. NSA acquires roughly 300-400 thousand such MCTs per year.[38]

For the second category, since the active user is a non-target who is located inside the United States, there is no reason to believe that all of the discrete communications contained within the MCTs will be to, from, or about the targeted selector (although there would need to be at least one such communication in order for NSA's upstream devices to acquire the transaction). Further, because the active user is in the United States, the Court presumes that the majority of that person's communications will be with other persons in the United States, many of whom will be United States persons. NSA acquires approximately 7,000-8,000 such MCTs per year, each of which likely contains one or more non-target discrete communications to or from other

---

[38] NSA acquired between 168,853 and 206,922 MCTs as to which the active user was the target over the six-month period covered by the sample. Aug. 16 Submission at 9.

persons in the United States.[39]

The third category is similar to the second in that the active user is a non-target. Therefore, there is no reason to believe that all of the communications within the MCTs will be to, from, or about the targeted selector (although there would need to be at least one such communication in order for NSA's upstream devices to acquire the transaction). However, because the active user is believed to be located outside the United States, the Court presumes that most of that persons's communications will be with other persons who are outside the United States, most of whom will be non-United States persons. That said, the Court notes that some of these MCTs are likely to contain non-target communications of or concerning United States persons, or that are to or from a person in the United States.[40] The Court has no way of knowing precisely how many such communications are acquired. Nevertheless, it appears that NSA acquires at least 1.3 million such MCTs each year,[41] so even if only 1% of these MCTs

---

[39] In its manual review, NSA identified ten MCTs as to which the active user was in the United States and that contained at least one wholly domestic communication. See Aug. 16 Submission at 5-7. NSA also identified seven additional MCTs as to which the active user was in the United States. Id. at 5. Although NSA determined that at least one party to each of the communications within the seven MCTs was reasonably believed to be located outside the United States, NSA did not indicate whether any of the communicants were United States persons or persons in the United States. Id. The Court sees no reason to treat these two categories of MCTs differently because the active users for both were in the United States. Seventeen MCTs constitutes .3% of the MCTs reviewed (5,081), and .3% of the 1.29-1.39 million MCTs NSA acquires every six months (see id. at 8) is 3,870- 4,170, or 7,740-8,340 every year.

[40] The government has acknowledged as much in its submissions. See June 28 Submission at 5.

[41] Based on its manual review, NSA assessed that 2668 of the 5,081 MCTs reviewed
(continued...)

contain a single non-target communication of or concerning a United States person, or that is to or from a person in the United States, NSA would be acquiring in excess of 10,000 additional discrete communications each year that are of or concerning United States persons, or that are to or from a person in the United States.

The fourth category is the most problematic, because without the identity of the active user – i.e., whether the user is the target or a non-target – or the active user's location, it is difficult to determine what presumptions to make about these MCTs. NSA acquires approximately 97,000-140,000 such MCTs each year.[42] In the context of wholly domestic communications, the government urges the Court to apply a series of presumptions that lead to the conclusion that this category would not contain any wholly domestic communications. Aug. 30 Submission at 4-8. The Court questions the validity of those presumptions, as applied to wholly domestic communications, but certainly is not inclined to apply them to assessing the likelihood that MCTs might contain communications of or concerning United States persons, or communications to or from persons in the United States. The active users for some of these

---

[41](...continued)
(approximately 52%) had a non-target active user who was reasonably believed to be located outside the United States. Aug. 16 Submission at 4-5. Fifty-two percent of the 1.29 to 1.39 million MCTs that NSA assessed were acquired through its upstream collection every six months would work out to 670,800 - 722,800 MCTs, or approximately 1.3-1.4 million MCTs per year that have a non-target active user believed to be located outside the United States.

[42] NSA determined that 224 MCTs of the 5,081 MCTs acquired during a six-month period (b) (1) (A) [redacted] From this, NSA concluded that it acquired between 48,609 and 70,168 such MCTs every six months through its upstream collection (or approximately 97,000-140,000 such MCTs each year). Id. at 9 n.27.

MCTs may be located in the United States, and, even if the active user is located overseas, the MCTs may contain non-target communications of or concerning United States persons or that are to or from persons in the United States. Accordingly, this "unknown" category likely adds substantially to the number of non-target communications of or concerning United States persons or that are to or from persons in the United States being acquired by NSA each year.

In sum, then, NSA's upstream collection is a small, but unique part of the government's overall collection under Section 702 of the FAA. NSA acquires valuable information through its upstream collection, but not without substantial intrusions on Fourth Amendment-protected interests. Indeed, the record before this Court establishes that NSA's acquisition of Internet transactions likely results in NSA acquiring annually tens of thousands of wholly domestic communications, and tens of thousands of non-target communications of persons who have little or no relationship to the target but who are protected under the Fourth Amendment. Both acquisitions raise questions as to whether NSA's targeting and minimization procedures comport with FISA and the Fourth Amendment.

2. NSA's Targeting Procedures

The Court will first consider whether NSA's acquisition of Internet transactions through its upstream collection, as described above, means that NSA's targeting procedures, as implemented, are not "reasonably designed" to: 1) "ensure that any acquisition authorized under [the certifications] is limited to targeting persons reasonably believed to be located outside the United States"; and 2) "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the

United States." 50 U.S.C. § 1881a(d)(1); id. § (i)(2)(B). The Court concludes that the manner in which NSA is currently implementing the targeting procedures does not prevent the Court from making the necessary findings, and hence NSA's targeting procedures do not offend FISA.

a. Targeting Persons Reasonably Believed to be Located Outside the United States

To the extent NSA is acquiring Internet transactions that contain a single discrete communication that is to, from, or about a tasked selector, the Court's previous analysis remains valid. As explained in greater detail in the Court's September 4, 2008 Memorandum Opinion, in this setting the person being targeted is the user of the tasked selector, and NSA's pre-targeting and post-targeting procedures ensure that NSA will only acquire such transactions so long as there is a reasonable belief that the target is located outside the United States. Docket No. [redacted].

But NSA's acquisition of MCTs complicates the Court's analysis somewhat. With regard to "about" communications, the Court previously found that the user of the tasked facility was the "target" of the acquisition, because the government's purpose in acquiring such communications is to obtain information about that user. See id. at 18. Moreover, the communication is not acquired because the government has any interest in the parties to the communication, other than their potential relationship to the user of the tasked facility, and the parties to an "about" communication do not become targets unless and until they are separately vetted under the targeting procedures. See id. at 18-19.

In the case of "about" MCTs – i.e., MCTs that are acquired because a targeted selector is referenced somewhere in the transaction – NSA acquires not only the discrete communication

that references the tasked selector, but also in many cases the contents of other discrete communications that do not reference the tasked selector and to which no target is a party. See May 2 Letter at 2-3 [redacted] By acquiring such MCTs, NSA likely acquires tens of thousands of additional communications of non-targets each year, many of whom have no relationship whatsoever with the user of the tasked selector. While the Court has concerns about NSA's acquisition of these non-target communications, the Court accepts the government's representation that the "sole reason [a non-target's MCT] 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." June 1 Submission at 4. Moreover, at the time of acquisition, NSA's upstream collection devices often lack the capability to determine whether a transaction contains a single communication or multiple communications, or to identify the parties to any particular communication within a transaction. See id. Therefore, the Court has no reason to believe that NSA, by acquiring Internet transactions containing multiple communications, is targeting anyone other than the user of the tasked selector. See United States v. Chemical Found., Inc., 272 U.S. 1, 14-15 (1926) ("The presumption of regularity supports the official acts of public officers, and, in the absence of clear evidence to the contrary, courts presume that they have properly discharged their official duties.").

b. Acquisition of Wholly Domestic Communications

NSA's acquisition of Internet transactions complicates the analysis required by Section 1881a(d)(1)(B), since the record shows that the government knowingly acquires tens of thousands of wholly domestic communications each year. At first blush, it might seem obvious

that targeting procedures that permit such acquisitions could not 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." 50 U.S.C. § 1881a(d)(1)(B). However, a closer examination of the language of the statute leads the Court to a different conclusion.

The government focuses primarily on the "intentional acquisition" language in Section 1881a(d)(1)(B). Specifically, the government argues that NSA is not "intentionally" acquiring wholly domestic communications because the government does not intend to acquire transactions containing communications that are wholly domestic and has implemented technical means to prevent the acquisition of such transactions. See June 28 Submission at 12. This argument fails for several reasons.

NSA targets a person under Section 702 certifications by acquiring communications to, from, or about a selector used by that person. Therefore, to the extent NSA's upstream collection devices acquire an Internet transaction containing a single, discrete communication that is to, from, or about a tasked selector, it can hardly be said that NSA's acquisition is "unintentional." In fact, the government has argued, and the Court has accepted, that the government intentionally acquires communications to and from a target, even when NSA reasonably – albeit mistakenly – believes that the target is located outside the United States. See Docket No. [redacted]

[redacted]

With respect to MCTs, the sole reason NSA acquires such transactions is the presence of a tasked selector within the transaction. Because it is technologically infeasible for NSA's

upstream collection devices to acquire only the discrete communication to, from, or about a tasked selector that may be contained within an MCT, however, the government argues that the only way to obtain the foreign intelligence information found within the discrete communication is to acquire the entire transaction in which it is contained. June 1 Submission at 21. As a result, the government intentionally acquires all discrete communications within an MCT, including those that are not to, from or about a tasked selector. See June 28 Submission at 12, 14; see also Sept. 7, 2011 Hearing Tr. at 33-34.

The fact that NSA's technical measures cannot prevent NSA from acquiring transactions containing wholly domestic communications under certain circumstances does not render NSA's acquisition of those transactions "unintentional." The government repeatedly characterizes such acquisitions as a "failure" of NSA's "technical means." June 28 Submission at 12; see also Sept. 7, 2011 Hearing Tr. at 35-36. However, there is nothing in the record to suggest that NSA's technical means are malfunctioning or otherwise failing to operate as designed. Indeed, the government readily concedes that NSA will acquire a wholly domestic "about" communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA or is routed through a foreign server. See June 1 Submission at 29. And in the case of MCTs containing wholly domestic communications that are not to, from, or about a tasked selector, NSA has no way to determine, at the time of acquisition, that a particular communication within an MCT is wholly domestic. See id. Furthermore, now that NSA's manual review of a sample of its upstream collection has confirmed that NSA likely acquires tens of thousands of wholly domestic communications each year, there is no question that the

government is knowingly acquiring Internet transactions that contain wholly domestic communications through its upstream collection.[43]

The government argues that an NSA analyst's post-acquisition discovery that a particular Internet transaction contains a wholly domestic communication should retroactively render NSA's acquisition of that transaction "unintentional." June 28 Submission at 12. That argument is unavailing. NSA's collection devices are set to acquire transactions that contain a reference to the targeted selector. When the collection device acquires such a transaction, it is functioning precisely as it is intended, even when the transaction includes a wholly domestic communication. The language of the statute makes clear that it is the government's intention at the time of acquisition that matters, and the government conceded as much at the hearing in this matter. Sept. 7, 2011 Hearing Tr. at 37-38.

Accordingly, the Court finds that NSA intentionally acquires Internet transactions that reference a tasked selector through its upstream collection with the knowledge that there are tens of thousands of wholly domestic communications contained within those transactions. But this is not the end of the analysis. To return to the language of the statute, NSA's 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

---

[43] It is generally settled that a person intends to produce a consequence either (a) when he acts with a purpose of producing that consequence or (b) when he acts knowing that the consequence is substantially certain to occur. Restatement (Third) of Torts § 1 (2010); see also United States v. Dyer, 589 F.3d 520, 528 (1st Cir. 2009) (in criminal law, "'intent' ordinarily requires only that the defendant reasonably knew the proscribed result would occur"), cert. denied, 130 S. Ct. 2422 (2010).

acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1)(B) (emphasis added). The underscored language requires an acquisition-by-acquisition inquiry. Thus, the Court must consider whether, at the time NSA intentionally acquires a transaction through its upstream collection, NSA will know that the sender and all intended recipients of any particular communication within that transaction are located in the United States.

Presently, it is not technically possible for NSA to configure its upstream collection devices (b) (1) (A) [redacted] the practical effect of this technological limitation is that NSA cannot know at the time it acquires an Internet transaction whether the sender and all intended recipients of any particular discrete communication contained within the transaction are located inside the United States.

[redacted]

[44] See supra, note 33.

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

[redacted]

Given that NSA's upstream collection devices lack the capacity to detect wholly domestic communications at the time an Internet transaction is acquired, the Court is inexorably led to the conclusion that the targeting procedures are "reasonably designed" to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. This is true despite the fact that NSA knows with certainty that the upstream collection, viewed as a whole, results in the acquisition of wholly domestic communications.

By expanding its Section 702 acquisitions to include the acquisition of Internet transactions through its upstream collection, NSA has, as a practical matter, circumvented the spirit of Section 1881a(b)(4) and (d)(1) with regard to that collection. NSA's knowing acquisition of tens of thousands of wholly domestic communications through its upstream collection is a cause of concern for the Court. But the meaning of the relevant statutory provision is clear and application to the facts before the Court does not lead to an impossible or absurd result. The Court's review does not end with the targeting procedures, however. The Court must

also consider whether NSA's minimization procedures are consistent with §1881a(e)(1) and whether NSA's targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.

3. NSA's Minimization Procedures, As Applied to MCTs in the Manner Proposed by the Government, Do Not Meet FISA's Definition of "Minimization Procedures"

The Court next considers whether NSA's minimization procedures, as the government proposes to apply them to Internet transactions, meet the statutory requirements. As noted above, 50 U.S.C. § 1881a(e)(1) requires that the minimization procedures "meet the definition of minimization procedures under [50 U.S.C. §§] 1801(h) or 1821(4) . . . ." That definition requires "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." 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A). For the reasons stated below, the Court concludes that NSA's minimization procedures, as applied to MCTs in the manner proposed by the government, do not meet the statutory definition in all respects.

a. The Minimization Framework

NSA's minimization procedures do not expressly contemplate the acquisition of MCTs, and the language of the procedures does not lend itself to straightforward application to MCTs. Most notably, various provisions of the NSA minimization procedures employ the term

"communication" as an operative term. As explained below, for instance, the rules governing retention, handling, and dissemination vary depending whether or not a communication is deemed to constitute a "domestic communication" instead of a "foreign communication," see NSA Minimization Procedures §§ 2(e), 5, 6, 7; a communication "of" or "concerning" a U.S. person, see id. §§ 2(b)-(c), 3(b)(1)-(2), 3(c); a "communication to, from, or about a target," id. § 3(b)(4); or a "communication . . . reasonably believed to contain foreign intelligence information or evidence of a crime," id. But MCTs can be fairly described as communications that contain several smaller communications. Applying the terms of the NSA minimization procedures to MCTs rather than discrete communications can produce very different results.

In a recent submission, the government explained how NSA proposes to apply its minimization procedures to MCTs. See Aug. 30 Submission at 8-11.[45] Before discussing the measures proposed by the government for handling MCTs, it is helpful to begin with a brief overview of the NSA minimization procedures themselves. The procedures require that all acquisitions "will be conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant to the authorized purpose of the collection." NSA

[45] Although NSA has been collecting MCTs since before the Court's approval of the first Section 702 certification in 2008, see June 1 Submission at 2, it has not, to date, applied the measures proposed here to the fruits of its upstream collection. Indeed, until NSA's manual review of a six-month sample of its upstream collection revealed the acquisition of wholly domestic communications, the government asserted that NSA had never found a wholly domestic communication in its upstream collection. See id.

Minimization Procedures § 3(a).[46] Following acquisition, the procedures require that, "[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime." Id. § 3(b)(4). "Foreign communication means a communication that has at least one communicant outside of the United States." Id. § 2(e). "All other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications." Id. In addition, domestic communications include "[a]ny communications acquired through the targeting of a person who at the time of targeting was reasonably believed to be located outside the United States but is in fact located inside the United States at the time such communications were acquired, and any communications acquired by targeting a person who at the time of the targeting was believed to be a non-United States person but was in fact a United States person . . . ." Id. § 3(d)(2). A domestic communication must be "promptly destroyed upon recognition unless the Director (or Acting Director) of NSA specifically determines, in writing, that" the communication contains foreign intelligence

[46] Of course, NSA's separate targeting procedures, discussed above, also govern the manner in which communications are acquired.

information or evidence of a crime, or that it falls into another narrow exception permitting retention. See id. § 5.[47]

Upon determining that a communication is a "foreign communication," NSA must decide whether the communication is "of" or "concerning" a United States person. Id. § 6. "Communications of a United States person include all communications to which a United States person is a party." Id. § 2(c). "Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly-available information about the person." Id. § 2(b).

A foreign communication that is of or concerning a United States person and that is determined to contain neither foreign intelligence information nor evidence of a crime must be destroyed "at the earliest practicable point in the processing cycle," and "may be retained no longer than five years from the expiration date of the certification in any event." Id. § 3(b)(1).[48]

---

[47] Once such a determination is made by the Director, the domestic communications at issue are effectively treated as "foreign communications" for purposes of the rules regarding retention and dissemination.

[48] Although Section 3(b)(1) by its terms applies only to "inadvertently acquired communications of or concerning a United States person," the government has informed the Court that this provision is intended to apply, and in practice is applied, to all foreign communications of or concerning United States persons that contain neither foreign intelligence information nor evidence of a crime. Docket No. 702(i)-08-01, Sept. 2, 2008 Notice of Clarification and Correction at 3-5. Moreover, Section 3(c) of the procedures separately provides that foreign communications that do not qualify for retention and that "are known to contain communications of or concerning United States persons will be destroyed upon recognition," and, like unreviewed communications, "may be retained no longer than five years from the

(continued...)

A foreign communication that is of or concerning a United States person may be retained indefinitely if the "dissemination of such communications with reference to such United States persons would be permitted" under the dissemination provisions that are discussed below, or if it contains evidence of a crime. Id. § 6(a)(2)-(3). If the retention of a foreign communication of or concerning a United States person is "necessary for the maintenance of technical databases," it may be retained for five years to allow for technical exploitation, or for longer than five years if more time is required for decryption or if the NSA Signals Intelligence Director "determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements." Id. § 6(a)(1).

As a general rule, "[a] report based on communications of or concerning a United States person may be disseminated" only "if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person." Id. § 6(b). A report including the identity of the United States person may be provided to a "recipient requiring the identity of such person for the performance of official duties," but only if at least one of eight requirements is also met – for instance, if "the identity of the United States person is necessary to understand foreign intelligence information or assess its importance," or if "information indicates the United States

---

[48](...continued)
expiration date of the certification authorizing the collection in any event."

person may be . . . an agent of a foreign power" or that he is "engaging in international terrorism activities." Id.[49]

b. Proposed Minimization Measures for MCTs

The government proposes that NSA's minimization procedures be applied to MCTs in the following manner. After acquisition, upstream acquisitions, including MCTs, will reside in NSA repositories until they are accessed (e.g., in response to a query) by an NSA analyst performing his or her day-to-day work. NSA proposes adding a "cautionary banner" to the tools its analysts use to view the content of communications acquired through upstream collection under Section 702. See Aug. 30 Submission at 9. The banner, which will be "broadly displayed on [such] tools," will "direct analysts to consult guidance on how to identify MCTs and how to handle them." Id. at 9 & n.6.[50] Analysts will be trained to identify MCTs and to recognize wholly domestic communications contained within MCTs. See id. at 8-9.

When an analyst identifies an upstream acquisition as an MCT, the analyst will decide whether or not he or she "seek[s] to use a discrete communication within [the] MCT,"

---

[49] The procedures also permit NSA to provide unminimized communications to the CIA and FBI (subject to their own minimization procedures), and to foreign governments for the limited purpose of obtaining "technical and linguistic assistance." NSA Minimization Procedures §§ 6(c), 8(b). Neither of these provisions has been used to share upstream acquisitions. Sept. 7, 2011 Hearing Tr. at 61-62.

[50] The banner will not be displayed for communications that "can be first identified through technical means where the active user is NSA's tasked selector or that contain only a single, discrete communication based on particular stable and well-known protocols." Aug. 30 Submission at 9 n.6. See infra, note 27, and supra, note 54.

presumably by reviewing some or all of the MCT's contents. Id. at 8.[51] "NSA analysts seeking to use a discrete communication contained in an MCT (for example, in a FISA application, intelligence report, or Section 702 targeting) will assess whether the discrete communication is to, from, or about a tasked selector." Id. The following framework will then be applied:

- If the discrete communication that the analyst seeks to use is to, from, or about a tasked selector, "any U.S. person information in that communication will be handled in accordance with the NSA minimization procedures." Id. Presumably, this means that the discrete communication will be treated as a "foreign communication" that is "of" or "concerning" a United States person, as described above. The MCT containing that communication remains available to analysts in NSA's repositories without any marking to indicate that it has been identified as an MCT or as a transaction containing United States person information.

- If the discrete communication sought to be used is not to, from, or about a tasked selector, and also not to or from an identifiable United States person, "that communication (including any U.S. person information therein) will be handled in accordance with the NSA minimization procedures." Id. at 8-9.[52] Presumably, this means that the discrete communication will be treated as a "foreign communication" or, if it contains information concerning a United States person, as a "foreign communication" "concerning a United States person," as described above. The MCT itself remains available to analysts in NSA's repositories without any marking to indicate that it has been identified as an MCT or that it contains one or more communications that are not to, from, or about a targeted selector.

---

[51] A transaction that is identified as an SCT rather than an MCT must be handled in accordance with the standard minimization procedures that are discussed above.

[52] The Court understands that absent contrary information, NSA treats the user of an account who appears to be located in the United States as "an identifiable U.S. person." See Aug. 30 Submission at 9 n.7 ("To help determine whether a discrete communication not to, from, or about a tasked selector is to or from a U.S. person, NSA would perform the same sort of technical analysis it would perform before tasking an electronic communications account/address/identifier in accordance with its section 702 targeting procedures.").

• A discrete communication that is not to, from, or about a tasked selector but that is to or from an identifiable United States person "cannot be used for any purpose other than to protect against an immediate threat to human life (e.g., force protection or hostage situations)." Id. at 9. Presumably, this is a reference to Section 1 of the minimization procedures, which allows NSA to deviate from the procedures in such narrow circumstances, subject to the requirement that prompt notice be given to the Office of the Director of National Intelligence, the Department of Justice, and the Court that the deviation has occurred. Regardless of whether or not the discrete communication is used for this limited purpose, the MCT itself remains in NSA's databases without any marking to indicate that it is an MCT, or that it contains at least one communication that is to or from an identifiable United States person. See id.; Sept. 7, 2011 Hearing Tr. at 61.

• If the discrete communication sought to be used by the analyst (or another discrete communication within the MCT) is recognized as being wholly domestic, the entire MCT will be purged from NSA's systems. See Aug. 30 Submission at 3.

c. Statutory Analysis

i. Acquisition

The Court first considers how NSA's proposed handling of MCTs bears on whether NSA's minimization procedures are "reasonably designed in light of the purpose and technique of the particular surveillance, 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." See 50 U.S.C. § 1801(h)(1) (emphasis added). Insofar as NSA likely acquires approximately 2,000-10,000 MCTs each year that contain at least one wholly domestic communication that is neither to, from, nor about a targeted selector,[53] and tens of thousands of communications of or

[53] As noted above, NSA's upstream collection also likely results in the acquisition of tens (continued...)

concerning United States persons with no direct connection to any target, the Court has serious concerns. The acquisition of such non-target communications, which are highly unlikely to have foreign intelligence value, obviously does not by itself serve the government's need to "obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. § 1801(h)(1).

The government submits, however, that the portions of MCTs that contain references to targeted selectors are likely to contain foreign intelligence information, and that it is not feasible for NSA to limit its collection only to the relevant portion or portions of each MCT – i.e., the particular discrete communications that are to, from, or about a targeted selector. The Court

---

[53](...continued)
of thousands of wholly domestic SCTs that contain references to targeted selectors. See supra, pages 33-34 & note 33 (discussing the limits [redacted] Although the collection of wholly domestic "about" SCTs is troubling, they do not raise the same minimization-related concerns as discrete, wholly domestic communications that are neither to, from, nor about targeted selectors, or as discrete communications of or concerning United States persons with no direct connection to any target, either of which may be contained within MCTs. The Court has effectively concluded that certain communications containing a reference to a targeted selector are reasonably likely to contain foreign intelligence information, including communications between non-target accounts that contain the name of the targeted facility in the body of the message. See Docket No. 07-449, May 31, 2007 Primary Order at 12 (finding probable cause to believe that certain "about" communications were "themselves being sent and/or received by one of the targeted foreign powers"). Insofar as the discrete, wholly domestic "about" communications at issue here are communications between non-target accounts that contain the name of the targeted facility, the same conclusion applies to them. Accordingly, in the language of FISA's definition of minimization procedures, the acquisition of wholly domestic communications about targeted selectors will generally be "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." See 50 U.S.C. 1801(h)(1). Nevertheless, the Court understands that in the event NSA identifies a discrete, wholly domestic "about" communication in its databases, the communication will be destroyed upon recognition. See NSA Minimization Procedures § 5.

accepts the government's assertion that the collection of MCTs yields valuable foreign intelligence information that by its nature cannot be acquired except through upstream collection. See Sept. 7, 2011 Hearing Tr. at 69-70, 74. For purposes of this discussion, the Court further accepts the government's assertion that it is not feasible for NSA to avoid the collection of MCTs as part of its upstream collection or to limit its collection only to the specific portion or portions of each transaction that contains the targeted selector. See id. at 48-50; June 1 Submission at 27.[54] The Court therefore concludes that NSA's minimization procedures are, given the current state of NSA's technical capability, 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.

[redacted]

In any event, it is incumbent upon NSA to continue working to enhance its capability to limit acquisitions only to targeted communications.

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

ii. Retention

The principal problem with the government's proposed handling of MCTs relates to what will occur, and what will not occur, following acquisition. As noted above, the NSA minimization procedures generally require that, "[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime," see NSA Minimization Procedures § 3(b)(4), so that it can be promptly afforded the appropriate treatment under the procedures. The measures proposed by the government for MCTs, however, largely dispense with the requirement of prompt disposition upon initial review by an analyst. Rather than attempting to identify and segregate information "not relevant to the authorized purpose of the acquisition" or to destroy such information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information, including information of or concerning United States persons with no direct connection to any target. See id. § 3(b)(1).

The proposed measures focus almost exclusively on the discrete communications within MCTs that analysts decide, after review, that they wish to use. See Aug. 30 Submission at 8-10. An analyst is not obligated to do anything with other portions of the MCT, including any wholly domestic discrete communications that are not immediately recognized as such, and communications of or concerning United States persons that have no direct connection to the targeted selector. See id.; Sept. 7, 2011 Hearing Tr. at 61. If, after reviewing the contents of an

entire MCT, the analyst decides that he or she does not wish to use any discrete communication contained therein, the analyst is not obligated to do anything unless it is immediately apparent to him or her that the MCT contains a wholly domestic communication (in which case the entire MCT is deleted).[55] See Aug. 30 Submission at 8-10.

Except in the case of those recognized as containing at least one wholly domestic communication, MCTs that have been reviewed by analysts remain available to other analysts in NSA's repositories without any marking to identify them as MCTs. See id.; Sept. 7, 2011 Hearing Tr. at 61. Nor will MCTs be marked to identify them as containing discrete communications to or from United States persons but not to or from a targeted selector, or to indicate that they contain United States person information. See Aug. 30 Submission at 8-10; Sept. 7, 2011 Hearing Tr. at 61. All MCTs except those identified as containing one or more wholly domestic communications will be retained for a minimum of five years. The net effect is that thousands of wholly domestic communications (those that are never reviewed and those that are not recognized by analysts as being wholly domestic), and thousands of other discrete

[55] The government's submissions make clear that, in many cases, it will be difficult for analysts to determine whether a discrete communication contained within an MCT is a wholly domestic communication. NSA's recent manual review of a six-month representative sample of its upstream collection demonstrates how challenging it can be for NSA to recognize wholly domestic communications, even when the agency's full attention and effort are directed at the task. See generally Aug. 16 and Aug. 30 Submissions. It is doubtful that analysts whose attention and effort are focused on identifying and analyzing foreign intelligence information will be any more successful in identifying wholly domestic communications. Indeed, each year the government notifies the Court of numerous compliance incidents involving good-faith mistakes and omissions by NSA personnel who work with the Section 702 collection.

communications that are not to or from a targeted selector but that are to, from, or concerning a United States person, will be retained by NSA for at least five years, despite the fact that they have no direct connection to a targeted selector and, therefore, are unlikely to contain foreign intelligence information.

It appears that NSA could do substantially more to minimize the retention of information concerning United States persons that is unrelated to the foreign intelligence purpose of its upstream collection. The government has not, for instance, demonstrated why it would not be feasible to limit access to upstream acquisitions to a smaller group of specially-trained analysts who could develop expertise in identifying and scrutinizing MCTs for wholly domestic communications and other discrete communications of or concerning United States persons. Alternatively, it is unclear why an analyst working within the framework proposed by the government should not be required, after identifying an MCT, to apply Section 3(b)(4) of the NSA minimization procedures to each discrete communication within the transaction. As noted above, Section 3(b)(4) states that "[a]s a communication is reviewed, NSA analyst(s) will determine whether it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime." NSA Minimization Procedures § 3(b)(4). If the MCT contains information "of" or "concerning" a United States person within the meaning of Sections (2)(b) and (2)(c) of the NSA minimization procedures, it is unclear why the analyst should not be required to mark it to identify it as such. At a minimum, it seems that the entire MCT could be marked as an MCT. Such markings would

alert other NSA personnel who might encounter the MCT to take care in reviewing it, thus reducing the risk of error that seems to be inherent in the measures proposed by the government, which are applied by each analyst, acting alone and without the benefit of his or her colleagues' prior efforts.[56] Another potentially helpful step might be to adopt a shorter retention period for MCTs and unreviewed upstream communications so that such information "ages off" and is deleted from NSA's repositories in less than five years.

This discussion is not intended to provide a checklist of changes that, if made, would necessarily bring NSA's minimization procedures into compliance with the statute. Indeed, it may be that some of these measures are impracticable, and it may be that there are other plausible (perhaps even better) steps that could be taken that are not mentioned here. But by not fully exploring such options, the government has failed to demonstrate that it has struck a reasonable balance between its foreign intelligence needs and the requirement that information concerning United States persons be protected. Under the circumstances, the Court is unable to find that, as applied to MCTs in the manner proposed by the government, NSA's minimization procedures are "reasonably designed in light of the purpose and technique of the particular surveillance to minimize the . . . retention . . . of nonpublicly available information concerning unconsenting

---

[56] The government recently acknowledged that "it's pretty clear that it would be better" if NSA used such markings but that "[t]he feasibility of doing that [had not yet been] assessed." Sept. 7, 2011 Hearing Tr. at 56.

United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[57] See 50 U.S.C. §§ 1801(h)(1) & 1821(4)(A).

iii. Dissemination

The Court next turns to dissemination. At the outset, it must be noted that FISA imposes a stricter standard for dissemination than for acquisition or retention. While the statute requires procedures that are reasonably designed to "minimize" the acquisition and retention of information concerning United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information, the procedures must be reasonably designed to "prohibit" the dissemination of information concerning United States persons consistent with that need. See 50 U.S.C. § 1801(h)(1) (emphasis added).

---

[57] NSA's minimization procedures contain two provisions that state, in part, that "[t]he communications that may be retained [by NSA] include electronic communications acquired because of limitations [redacted]. The government further represented that it "ha[d] not seen" such a circumstance in collection under the Protect America Act ("PAA"), which was the predecessor to Section 702. Id. at 29, 30. And although NSA apparently was acquiring Internet transactions under the PAA, the government made no mention of such acquisitions in connection with these provisions of the minimization procedures (or otherwise). See id. at 27-31. Accordingly, the Court does not read this language as purporting to justify the procedures proposed by the government for MCTs. In any event, such a reading would, for the reasons stated, be inconsistent with the statutory requirements for minimization.

As the Court understands it, no United States-person-identifying information contained in any MCT will be disseminated except in accordance with the general requirements of NSA's minimization procedures for "foreign communications" "of or concerning United States persons" that are discussed above. Specifically, "[a] report based on communications of or concerning a United States person may be disseminated" only "if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person." NSA Minimization Procedures § 6(b). A report including the identity of the United States person may be provided to a "recipient requiring the identity of such person for the performance of official duties," but only if at least one of eight requirements is also met – for instance, if "the identity of the United States person is necessary to understand foreign intelligence information or assess its importance." Id.[58]

This limitation on the dissemination of United States-person-identifying information is helpful. But the pertinent portion of FISA's definition of minimization procedures applies not merely to information that identifies United States persons, but more broadly to the dissemination of "information concerning unconsenting United States persons." 50 U.S.C. § 1801(h)(1) (emphasis added).[59] The government has proposed several additional restrictions that

---

[58] Although Section 6(b) uses the term "report," the Court understands it to apply to the dissemination of United States-person-identifying information in any form.

[59] Another provision of the definition of minimization procedures bars the dissemination of information (other than certain forms of foreign intelligence information) "in a manner that

(continued...)

will have the effect of limiting the dissemination of "nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to disseminate foreign intelligence information." Id. First, as noted above, the government will destroy MCTs that are recognized by analysts as containing one or more discrete wholly domestic communications. Second, the government has asserted that NSA will not use any discrete communication within an MCT that is determined to be to or from a United States person but not to, from, or about a targeted selector, except when necessary to protect against an immediate threat to human life. See Aug. 30 Submission at 9. The Court understands this to mean, among other things, that no information from such a communication will be disseminated in any form unless NSA determines it is necessary to serve this specific purpose. Third, the government has represented that whenever it is unable to confirm that at least one party to a discrete communication contained in an MCT is located outside the United States, it will not use any information contained in the discrete communication. See Sept. 7, 2011 Hearing Tr. at 52. The Court understands this limitation to mean that no information from such a discrete communication will be disseminated by NSA in any form.

Communications as to which a United States person or a person inside the United States

---

[59](...continued)
identifies any United States person," except when the person's identity is necessary to understand foreign intelligence information or to assess its importance. See 50 U.S.C. §§ 1801(h)(2), 1821(4)(b). Congress's use of the distinct modifying terms "concerning" and "identifying" in two adjacent and closely-related provisions was presumably intended to have meaning. See, e.g., Russello v. United States, 464 U.S. 16, 23 (1983).

is a party are more likely than other communications to contain information concerning United States persons. And when such a communication is neither to, from, nor about a targeted facility, it is highly unlikely that the "need of the United States to disseminate foreign intelligence information" would be served by the dissemination of United States-person information contained therein. Hence, taken together, these measures will tend to prohibit the dissemination of information concerning unconsenting United States persons when there is no foreign-intelligence need to do so.[60] Of course, the risk remains that information concerning United States persons will not be recognized by NSA despite the good-faith application of the measures it proposes. But the Court cannot say that the risk is so great that it undermines the reasonableness of the measures proposed by NSA with respect to the dissemination of information concerning United States persons.[61] Accordingly, the Court concludes that NSA's

---

[60] Another measure that, on balance, is likely to mitigate somewhat the risk that information concerning United States persons will be disseminated in the absence of a foreign-intelligence need is the recently-proposed prohibition on running queries of the Section 702 upstream collection using United States-person identifiers. See Aug. 30 Submission at 10-11. To be sure, any query, including a query based on non-United States-person information, could yield United States-person information. Nevertheless, it stands to reason that queries based on information concerning United States persons are at least somewhat more likely than other queries to yield United States-person information. Insofar as information concerning United States persons is not made available to analysts, it cannot be disseminated. Of course, this querying restriction does not address the retention problem that is discussed above.

[61] In reaching this conclusion regarding the risk that information concerning United States persons might be mistakenly disseminated, the Court is mindful that by taking additional steps to minimize the retention of such information, NSA would also be reducing the likelihood that it might be disseminated when the government has no foreign intelligence need to do so.

minimization procedures are reasonably designed to "prohibit the dissemination[] of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to . . . disseminate foreign intelligence information." See 50 U.S.C. § 1801(h)(1).[62]

4. NSA'S Targeting and Minimization Procedures Do Not, as Applied to Upstream Collection that Includes MCTs, Satisfy the Requirements of the Fourth Amendment

The final question for the Court is whether the targeting and minimization procedures are, as applied to upstream collection that includes MCTs, consistent with the Fourth Amendment. See 50 U.S.C. § 1881a(i)(3)(A)-(B). The Fourth Amendment provides:

> 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.

The Court has assumed in the prior Section 702 Dockets that at least in some circumstances, account holders have a reasonable expectation of privacy in electronic communications, and hence that the acquisition of such communications can result in a "search" or "seizure" within the meaning of the Fourth Amendment. See, e.g., Docket No. [redacted]. The government accepts the proposition that the acquisition of

---

[62] The Court further concludes that the NSA minimization procedures, as the government proposes to apply them to MCTs, satisfy the requirements of 50 U.S.C. §§ 1801(h)(2)-(3) and 1821(4)(B)-(C). See supra, note 59 (discussing 50 U.S.C. §§ 1801(h)(2) & 1821(4)(B)). The requirements of 50 U.S.C. §§ 1801(h)(4) and 1821(4)(D) are inapplicable here.

electronic communications can result in a "search" or "seizure" under the Fourth Amendment. See Sept. 7, 2011 Hearing Tr. at 66. Indeed, the government has acknowledged in prior Section 702 matters that the acquisition of communications from facilities used by United States persons located outside the United States "must be in conformity with the Fourth Amendment." Docket Nos [redacted]. The same is true of the acquisition of communications from facilities used by United States persons and others within the United States. See United States v. Verdugo-Urquidez, 494 U.S. 259, 271 (1990) (recognizing that "aliens receive constitutional protections when they have come within the territory of the United States and developed substantial connections with this country").

a. The Warrant Requirement

The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the "foreign intelligence exception" to the warrant requirement of the Fourth Amendment. See Docket No. [redacted]. The government's recent revelations regarding NSA's acquisition of MCTs do not alter that conclusion. To be sure, the Court now understands that, as a result of the transactional nature of the upstream collection, NSA acquires a substantially larger number of communications of or concerning United States persons and persons inside the United States than previously understood. Nevertheless, the collection as a whole is still directed at [redacted] conducted for the purpose of national security – a

purpose going "'well beyond any garden-variety law enforcement objective.'" See id. (quoting In re Directives, Docket No. 08-01, Opinion at 16 (FISA Ct. Rev. Aug. 22, 2008) (hereinafter "In re Directives")).[63] Further, it remains true that the collection is undertaken in circumstances in which there is a "'high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake.'" Id. at 36 (quoting In re Directives at 18). Accordingly, the government's revelation that NSA acquires MCTs as part of its Section 702 upstream collection does not disturb the Court's prior conclusion that the government is not required to obtain a warrant before conducting acquisitions under NSA's targeting and minimization procedures.

b. Reasonableness

The question therefore becomes whether, taking into account NSA's acquisition and proposed handling of MCTs, the agency's targeting and minimization procedures are reasonable under the Fourth Amendment. As the Foreign Intelligence Surveillance Court of Review ("Court of Review") has explained, a court assessing reasonableness in this context must consider "the nature of the government intrusion and how the government intrusion is implemented. The more important the government's interest, the greater the intrusion that may be constitutionally

[63] A redacted, de-classified version of the opinion in In re Directives is published at 551 F.3d 1004. The citations herein are to the unredacted, classified version of the opinion.

tolerated." In re Directives at 19-20 (citations omitted), quoted in Docket No [redacted]. The court must therefore

> balance the interests at stake. If the protections that are in place for individual privacy interests are sufficient in light of the government interest at stake, the constitutional scales will tilt in 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 (citations omitted), quoted in Docket No [redacted]. In conducting this balancing, the Court must consider the "totality of the circumstances." Id. at 19. Given the all-encompassing nature of Fourth Amendment reasonableness review, the targeting and minimization procedures are most appropriately considered collectively. See Docket No. [redacted] (following the same approach).[64]

The Court has previously recognized that the government's national security interest in conducting acquisitions pursuant to Section 702 "'is of the highest order of magnitude.'" Docket No. [redacted] (quoting In re Directives at 20). The Court has further accepted the government's representations that NSA's upstream collection is "'uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information.'" Docket No. [redacted] (quoting

---

[64] Reasonableness review under the Fourth Amendment is broader than the statutory assessment previously addressed, which is necessarily limited by the terms of the pertinent provisions of FISA.

government filing). There is no reason to believe that the collection of MCTs results in the acquisition of less foreign intelligence information than the Court previously understood.

Nevertheless, it must be noted that NSA's upstream collection makes up only a very small fraction of the agency's total collection pursuant to Section 702. As explained above, the collection of telephone communications under Section 702 is not implicated at all by the government's recent disclosures regarding NSA's acquisition of MCTs. Nor do those disclosures affect NSA's collection of Internet communications directly from Internet service providers [redacted], which accounts for approximately 91% of the Internet communications acquired by NSA each year under Section 702. See Aug. 16 Submission at Appendix A. And the government recently advised that NSA now has the capability, at the time of acquisition, to identify approximately 40% of its upstream collection as constituting discrete communications (non-MCTs) that are to, from, or about a targeted selector. See id. at 1 n.2. Accordingly, only approximately 5.4% (40% of 9%) of NSA's aggregate collection of Internet communications (and an even smaller portion of the total collection) under Section 702 is at issue here. The national security interest at stake must be assessed bearing these numbers in mind.

The government's recent disclosures regarding the acquisition of MCTs most directly affect the privacy side of the Fourth Amendment balance. The Court's prior approvals of the targeting and minimization procedures rested on its conclusion that the procedures "reasonably confine acquisitions to targets who are non-U.S. persons outside the United States," who thus

"are not protected by the Fourth Amendment." Docket No [redacted] [redacted] The Court's approvals also rested upon the understanding that acquisitions under the procedures "will intrude on interests protected by the Fourth Amendment only to the extent that (1) despite the operation of the targeting procedures, U.S. persons, or persons actually in the United States, are mistakenly targeted; or (2) U.S. persons, or persons located in the United States, are parties to communications to or from tasked selectors (or, in certain circumstances, communications that contain a reference to a tasked selector)." Id. at 38. But NSA's acquisition of MCTs substantially broadens the circumstances in which Fourth Amendment-protected interests are intruded upon by NSA's Section 702 collection. Until now, the Court has not considered these acquisitions in its Fourth Amendment analysis.

Both in terms of its size and its nature, the intrusion resulting from NSA's acquisition of MCTs is substantial. The Court now understands that each year, NSA's upstream collection likely results in the acquisition of roughly two to ten thousand discrete wholly domestic communications that are neither to, from, nor about a targeted selector, as well as tens of thousands of other communications that are to or from a United States person or a person in the United States but that are neither to, from, nor about a targeted selector.[65] In arguing that NSA's

[65] As discussed earlier, NSA also likely acquires tens of thousands of discrete, wholly domestic communications that are "about" a targeted facility. Because these communications are reasonably likely to contain foreign intelligence information and thus, generally speaking, serve the government's foreign intelligence needs, they do not present the same Fourth Amendment concerns as the non-target communications discussed here. See supra, note 53.

targeting and minimization procedures satisfy the Fourth Amendment notwithstanding the acquisition of MCTs, the government stresses that the number of protected communications acquired is relatively small in comparison to the total number of Internet communications obtained by NSA through its upstream collection. That is true enough, given the enormous volume of Internet transactions acquired by NSA through its upstream collection (approximately 26.5 million annually). But the number is small only in that relative sense. The Court recognizes that the ratio of non-target, Fourth Amendment-protected communications to the total number of communications must be considered in the Fourth Amendment balancing. But in conducting a review under the Constitution that requires consideration of the totality of the circumstances, see In re Directives at 19, the Court must also take into account the absolute number of non-target, protected communications that are acquired. In absolute terms, tens of thousands of non-target, protected communications annually is a very large number.

The nature of the intrusion at issue is also an important consideration in the Fourth Amendment balancing. See, e.g., Board of Educ. v. Earls, 536 U.S. 822, 832 (2002); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 659 (1995). At issue here are the personal [redacted] communications of U.S. persons and persons in the United States. 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. Indeed, the 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. See Katz, 389 U.S. at 352; United States v. United States Dist. Ct. (Keith), 407 U.S. 297, 313 (1972); United States v. Jacobsen, 466 U.S. 109, 114 (1984). The intrusion resulting from the interception of the contents of electronic communications is, generally speaking, no less substantial.[66]

The government stresses that the non-target communications of concern here (discrete wholly domestic communications and other discrete communications to or from a United States person or a person in the United States that are neither to, from, nor about a targeted selector) are acquired incidentally rather than purposefully. See June 28 Submission at 13-14. Insofar as NSA acquires entire MCTs because it lacks the technical means to limit collection only to the discrete portion or portions of each MCT that contain a reference to the targeted selector, the Court is satisfied that is the case. But as the government correctly recognizes, the acquisition of non-target information is not necessarily reasonable under the Fourth Amendment simply

---

[66] Of course, not every interception by the government of a personal communication results in a "search" or "seizure" within the meaning of the Fourth Amendment. Whether a particular intrusion constitutes a search or seizure depends on the specific facts and circumstances involved.

because its collection is incidental to the purpose of the search or surveillance. See id. at 14. There surely are circumstances in which incidental intrusions can be so substantial as to render a search or seizure unreasonable. To use an extreme example, if the only way for the government to obtain communications to or from a particular targeted [redacted] required also acquiring all communications to or from every other [redacted], such collection would certainly raise very serious Fourth Amendment concerns.

Here, the quantity and nature of the information that is "incidentally" collected distinguishes this matter from the prior instances in which this Court and the Court of Review have considered incidental acquisitions. As explained above, the quantity of incidentally-acquired, non-target, protected communications being acquired by NSA through its upstream collection is, in absolute terms, very large, and the resulting intrusion is, in each instance, likewise very substantial. And with regard to the nature of the acquisition, the government acknowledged in a prior Section 702 docket that the term "incidental interception" is "most commonly understood to refer to an intercepted communication between a target using a facility subject to surveillance and a third party using a facility not subject to surveillance." Docket Nos. [redacted] This is the sort of acquisition that the Court of Review was addressing in In re Directives when it stated that "incidental collections occurring as a result of constitutionally permissible acquisitions do not

render those acquisitions unlawful." In re Directives at 30. But here, by contrast, the incidental acquisitions of concern are not direct communications between a non-target third party and the user of the targeted facility. Nor are they the communications of non-targets that refer directly to a targeted selector. Rather, the communications of concern here are acquired simply because they appear somewhere in the same transaction as a separate communication that is to, from, or about the targeted facility.[67]

The distinction is significant and impacts the Fourth Amendment balancing. A discrete communication as to which the user of the targeted facility is a party or in which the targeted

---

[67] The Court of Review plainly limited its holding regarding incidental collection to the facts before it. See In re Directives at 30 ("On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.") (emphasis added). The dispute in In re Directives involved the acquisition by NSA of discrete to/from communications from an Internet Service Provider, not NSA's upstream collection of Internet transactions. Accordingly, the Court of Review had no occasion to consider NSA's acquisition of MCTs (or even "about" communications, for that matter). Furthermore, the Court of Review noted that "[t]he government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary." Id. Here, however, the government proposes measures that will allow NSA to retain non-target United States person information in its databases for at least five years.

The Title III cases cited by the government (see June 28 Submission at 14-15) are likewise distinguishable. Abraham v. County of Greenville, 237 F.3d 386, 391 (4th Cir. 2001), did not involve incidental overhears at all. The others involved allegedly non-pertinent communications to or from the facilities for which wiretap authorization had been granted, rather than communications to or from non-targeted facilities. See Scott v. United States, 436 U.S. 128, 130-31 (1978), United States v. McKinnon, 721 F.2d 19, 23 (1st Cir. 1983), and United States v. Doolittle, 507 F.2d 1368, 1371, aff'd en banc, 518 F.2d 500 (5th Cir. 1975).

facility is mentioned is much more likely to contain foreign intelligence information than is a separate communication that is acquired simply because it happens to be within the same transaction as a communication involving a targeted facility. Hence, the national security need for acquiring, retaining, and disseminating the former category of communications is greater than the justification for acquiring, retaining, and disseminating the latter form of communication.

The Court of Review and this Court have 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. See In re Directives at 29-30; Docket No. [redacted] As explained in the discussion of NSA's minimization procedures above, the measures proposed by NSA for handling MCTs tend to maximize, rather than minimize, the retention of non-target information, including information of or concerning United States persons. Instead of requiring the prompt review and proper disposition of non-target information (to the extent it is feasible to do so), NSA's proposed measures focus almost exclusively on those portions of an MCT that an analyst decides, after review, that he or she wishes to use. An analyst is not required to determine whether other portions of the MCT constitute discrete communications to or from a United States person or a person in the United States, or contain information concerning a United States person or person inside the United States, or, having made such a determination, to do anything about it. Only

those MCTs that are immediately recognized as containing a wholly domestic discrete communication are purged, while other MCTs remain in NSA's repositories for five or more years, without being marked as MCTs. Nor, if an MCT contains a discrete communication of, or other information concerning, a United States person or person in the United States, is the MCT marked as such. Accordingly, each analyst who retrieves an MCT and wishes to use a portion thereof is left to apply the proposed minimization measures alone, from beginning to end, and without the benefit of his colleagues' prior review and analysis. Given the limited review of MCTs that is required, and the difficulty of the task of identifying protected information within an MCT, the government's proposed measures seem to enhance, rather than reduce, the risk of error, overretention, and dissemination of non-target information, including information protected by the Fourth Amendment.

In sum, NSA's collection of MCTs results in the acquisition of a very large number of Fourth Amendment-protected communications that have no direct connection to any targeted facility and thus do not serve the national security needs underlying the Section 702 collection as a whole. Rather than attempting to identify and segregate the non-target, Fourth-Amendment protected information promptly following acquisition, NSA's proposed handling of MCTs tends to maximize the retention of such information and hence to enhance the risk that it will be used and disseminated. Under the totality of the circumstances, then, the Court is unable to find that

the government's proposed application of NSA's targeting and minimization procedures to MCTs is consistent with the requirements of the Fourth Amendment. The Court does not foreclose the possibility that the government might be able to tailor the scope of NSA's upstream collection, or adopt more stringent post-acquisition safeguards, in a manner that would satisfy the reasonableness requirement of the Fourth Amendment.[68]

V. CONCLUSION

For the foregoing reasons, the government's requests for approval of the certifications and procedures contained in the April 2011 Submissions are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the "upstream collection" of Internet transactions containing multiple communications, or MCTs – is, in some respects, deficient on statutory and constitutional grounds. Specifically, the Court finds as follows:

1. Certifications [redacted] and the amendments to the Certifications in the Prior 702 Dockets, contain all the required elements;

---

[68] As the government notes, see June 1 Submission at 18-19, the Supreme Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." City of Ontario v. Quon, — U.S. —, 130 S. Ct. 2619, 2632 (2010) (citations and internal quotation marks omitted). The foregoing discussion should not be understood to suggest otherwise. Rather, the Court holds only that the means actually chosen by the government to accomplish its Section 702 upstream collection are, with respect to MCTs, excessively intrusive in light of the purpose of the collection as a whole.

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

2. As applied to telephone communications and discrete Internet communications that are to or from a facility tasked for collection, to non-MCT "about" communications falling within the [redacted] categories previously described by the government,[69] and to MCTs as to which the "active user" is known to be a tasked selector, the targeting and minimization procedures adopted in accordance with 50 U.S.C. § 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States;

3. NSA's targeting procedures, as the government proposes to implement them in connection with the acquisition of MCTs, meet the requirements of 50 U.S.C. § 1881a(d);

4. NSA's minimization procedures, as the government proposes to apply them to MCTs as to which the "active user" is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention; and

5. NSA's targeting and minimization procedures, as the government proposes to apply them to MCTs as to which the "active user" is not known to be a tasked selector, are inconsistent with the requirements of the Fourth Amendment.

---

[69] See Docket No. [redacted].

Orders approving the certifications and amendments in part are being entered contemporaneously herewith.

ENTERED this 3rd day of October, 2011.

JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

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

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

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

ORDER

These matters are before the Court on: (1) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [redacted], which was filed

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

on April 20, 2011; (2) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [redacted], which was filed on April 22, 2011; and (3) the "Government's Ex Parte Submission of Reauthorization Certification and Related Procedures, Ex Parte Submission of Amended Certifications, and Request for an Order Approving Such Certification and Amended Certifications" for DNI/AG 702(g) Certifications [redacted], which was also filed on April 22, 2011 (collectively, the "April 2011 Submissions").

Through the April 2011 Submissions, the government seeks approval of the acquisition of certain telephone and Internet communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA" or the "Act"), 50 U.S.C. § 1881a, which requires judicial review for compliance with both statutory and constitutional requirements. For the reasons set forth in the accompanying Memorandum Opinion, the government's requests for approval are granted in part and denied in part. The Court concludes that one aspect of the proposed collection – the "upstream collection" of Internet transactions containing multiple communications, or "MCTs" – is, in some respects, deficient on statutory and constitutional grounds. Specifically, the Court finds as follows:

1. DNI/AG 702(g) Certifications [redacted], as well as the amendments to the other certifications listed above and contained in the April 2011 Submissions,

contain all the required elements;

2. As applied to telephone communications and discrete Internet communications that are to or from a facility tasked for collection, to non-MCT "about" communications falling within the [redacted] categories previously described by the government,[1] and to MCTs as to which the "active user" is known to be a tasked selector, the targeting and minimization procedures adopted in accordance with 50 U.S.C. § 1881a(d)-(e) are consistent with the requirements of those subsections and with the Fourth Amendment to the Constitution of the United States;

3. NSA's targeting procedures, as the government proposes to implement them in connection with the acquisition of MCTs, meet the requirements of 50 U.S.C. § 1881a(d);

4. NSA's minimization procedures, as the government proposes to apply them to MCTs as to which the "active user" is not known to be a tasked selector, do not meet the requirements of 50 U.S.C. § 1881a(e) with respect to retention; and

5. NSA's targeting and minimization procedures, as the government proposes to apply them to MCTs as to which the "active user" is not known to be a tasked selector, are inconsistent with the requirements of the Fourth Amendment.

Accordingly, pursuant to 50 U.S.C. § 1881a(i)(3)(B), the government shall, at its election:

(a) not later than 30 days from the issuance of this Order, correct the deficiencies identified in the accompanying Memorandum Opinion; or,

---

[1] See Docket No. 702(i)-08-01, Sept. 4, Memorandum Opinion at 17-18 n.14.

(b) cease the implementation of the Certifications insofar as they permit the acquisition of MCTs as to which the "active user" is not known to be a tasked selector.

ENTERED this 3rd day of October, 2011, at 4:55 p.m. Eastern Time.

JOHN D. BATES
Judge, United States Foreign
Intelligence Surveillance Court

I, [redacted] Deputy Clerk, FISC, certify that this document is a true and correct copy of the original. (b) (1) (A)

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

Plaintiff's Exhibit 17

IC ON THE RECORD

- Section 702 Overview
- NEW
  - CY2017 Transparency Report
- CY2016 SIGNALS INTEL REFORM REPORT
- IC TRANSPARENCY PLAN



DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)

Wednesday, August 21, 2013

In June, President Obama requested that Director of National Intelligence James R. Clapper declassify and make public as much information as possible about certain sensitive NSA programs while being mindful of the need to protect sensitive classified intelligence and national security.

Consistent with this directive and in the interest of increased transparency, DNI Clapper has today authorized the declassification and public release of a number of documents pertaining to the Intelligence Community's collection under Section 702 of the Foreign Intelligence Surveillance Act (FISA). DNI Clapper has determined that the release of these documents is in the public interest.

These documents and other unclassified information related to foreign intelligence surveillance activities are available on a new Intelligence Community website established at the direction of the President. The new www.icontherecord.tumblr.com is designed to provide immediate, ongoing and direct access to factual information related to the lawful foreign surveillance activities carried out by the U.S. Intelligence Community.

The Administration is undertaking a careful and thorough review of whether and to what extent additional information or documents pertaining to this program may be declassified, consistent with the protection of national security. *IC on the Record* provides a single online location to access new information as it is made available from across the Intelligence Community.

Shawn Turner
Director of Public Affairs
Office of the Director of National Intelligence

Documents being released today include:

DNI James Clapper's Cover Letter Announcing the Document Release

October 3, 2011 – Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates) *

November 30, 2011 – Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates) - Part 1 | Part 2

September 25, 2012 – Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates)

December 8, 2011 — Lisa Monaco, John C. ("Chris") Chris Inglis, Robert Litt - Statement for the Record before the House Permanent Select Committee on Intelligence

February 9, 2012 — Lisa Monaco, John C. ("Chris") Inglis, Robert Litt - Statement for the Record before the House Permanent Select Committee on Intelligence

May 4, 2012 — Letters to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence Leadership regarding Section 702 Congressional White Paper entitled The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act

October 31, 2011 — Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702, as amended

August 2013 — Semi-Annual Assessment of Compliance with the 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

---

June 19, 2017 *NYT FOIA* Release Documents

- Motion for Secondary Orders **
- Motion to Extend Time **
- November 7, 2011 Order **
- FISC Questions Regarding Amended 2011 Section 702 Certifications **

September 13, 2017 *NYT FOIA* Release Documents

- Govt Clarification of NSA Upstream Collection dated May 2, 2011
- FISC Briefing Order dated May 2011
- FISC Section 702 Order dated 2011
- FISC Hearing Transcript dated Sep. 7, 2011
- Govt Letter to FISC with Additional Information re 702 dated Sep. 9, 2011
- Govt Supplement Letter to FISC dated Sep. 13, 2011
- FISC Section 702 Order dated Sep. 14, 2011
- FISC Briefing Order dated Oct. 13, 2011
- Govt Preliminary Notice of Compliance Incidents dated Apr. 19, 2011
- FISC Order dated 2011
- Govt Motion for Secondary Orders dated Oct. 4, 2011
- Notice of Filing of Govt Responses to FISC Questions dated Nov 15 2011

October 11, 2017 NYT FOIA Release Documents

- Motion to Extend Time Limits dated May 5, 2011
- Government's Reauthorization Certification and Related Documents dated Apr. 22, 2011
- Follow-Up Questions Regarding Section 702 Certifications dated Jun. 17, 2011
- Government's Response to May 9, 2011 Briefing Order dated Jun. 1, 2011
- Motion to Extend Time Limits dated Jul. 14, 2011
- Government's Supplement to June 1 and June 28, 2011 Submissions dated Aug. 16, 2011
- Government's Amendment to Section 702 Certification and Amended Minimization Procedures dated Oct. 31, 2011
- Government's Notice of Clarifications dated Aug. 16, 2011
- Government's Response to October 13, 2011 Briefing Order dated Nov. 22, 2011
- Government's Request for Issuance of Notices dated Oct. 31, 2011
- Government's Notice dated Nov. 29, 2011

** Updated 07/16/14 to reflect additional declassification concerning the now-discontinued NSA bulk electronic communications metadata program.*

*** Updated 6/19/17 to reflect additional declassification concerning the now-discontinued NSA bulk electronic communications metadata program.*

- #Declassified
- #Section 702
- #FISA
- #NSA

- 5 years ago
- 194
- Permalink

Share

Short URL
https://tmblr.co/ZZQjsqsvMU

TwitterFacebookPinterestGoogle+

194 Notes/ Show

← Previous • Next →

IC ON THE RECORD:

Direct access to factual information related to the lawful foreign surveillance activities of the U.S. Intelligence Community.

Created at the direction of the President of the United States and maintained by the Office of the Director of National Intelligence.

Guide to Posted Documents Regarding Use of National Security Authorities

---

CONTENT:

- - Official Statements
- - Declassified Documents
- - Testimony
- - Speeches & Interviews
- - Fact Sheets
- - Oversight & Compliance
- - Video
- - IC Budget

HOT TOPICS:

- - Civil Liberties
- - FISA
- - FISC
- - Section 215
- - Section 702

THEIR OWN WORDS:

- - Mike Rogers, Dir. NSA
- - Rick Ledgett, Dep. Dir. NSA
- - Alex Joel, CLPT, ODNI
- - Becky Richards, CLPO, NSA

(Former IC Officials)

- - James Clapper, DNI
- - Keith Alexander, Dir. NSA
- - John Inglis, Dep. Dir. NSA
- - Robert Litt, GC, ODNI
- - Rajesh De, GC, NSA
- - John Delong, CD, NSA

Search this site

This website is maintained by the Office of the Director of National Intelligence.

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

Plaintiff's Exhibit 18

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

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

Plaintiff's Exhibit 19

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

U.S. Department of Justice

National Security Division

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2011 MAY -2 AM 11:48
LEEANN FLYNN HALL
CLERK OF COURT

~~TOP SECRET//COMINT//NOFORN~~

Washington, D.C. 20530

May 2, 2011

The Honorable John D. Bates
United States Foreign Intelligence Surveillance Court
333 Constitution Avenue, N.W.
Washington, D.C. 20001

Re: Clarification of National Security Agency's Upstream Collection Pursuant to Section 702 of FISA ~~(S//SI//NF)~~

Dear Judge Bates:

On April 21, 2011, the National Security Agency (NSA) provided the National Security Division (NSD) and the Office of the Director of National Intelligence (ODNI) information clarifying the manner in which NSA acquires certain communications through its upstream collection platforms pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (FISA). Although NSA, NSD, and ODNI are still reviewing this matter and assessing its import, we are providing preliminary notice at this time pursuant to Rule 13(a) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, effective November 1, 2010, in order provide the Court with this additional clarifying information. We have worked closely in these efforts with NSA officials, who have assisted in drafting and reviewing this notice to the Court. ~~(TS//SI//NF)~~

As previously described to the Court, in conducting upstream collection using electronic communication accounts/addresses/identifiers (hereinafter "selectors") pursuant to Section 702, NSA acquires Internet communications that are to or from a tasked selector, or which contain a reference to a tasked selector. The term "Internet communications," as described by the Director of NSA in affidavits supporting DNI/AG 702(g) certifications, "is intended to include electronic communications that [redacted] See, e.g., DNI/AG 702(g) Certification [redacted] Affidavit of General Keith B. Alexander, Director, NSA, filed [redacted] 2010, ¶ 6.

~~TOP SECRET//COMINT//NOFORN~~

~~Classified by: Tashina Gauhar, Deputy Assistant Attorney General, NSD, DOJ~~
~~Reason: 1.4(c)~~
~~Declassify on: May 2, 2036~~

OI Tracking No. 104876

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

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

In past representations to the Court, the Government used as an example of upstream collection the acquisition of [redacted] that contained a selector that NSA had tasked under Section 702, such that NSA acquired the [redacted] while it was being transmitted to or from a user of the non-tasked account.[1] [redacted] Based on recent discussions among NSA, NSD, and ODNI regarding one specified category of Internet communications acquired through upstream collection—"electronic communications [redacted]"—and in view of the complexity of this issue and the prior representations to the Court, the Government believes that further description of the scope of NSA's upstream collection is warranted. ~~(TS//SI//NF)~~

One type of "electronic communications [redacted][2] ~~(TS//SI//NF)~~

Depending on [redacted], the data transmitted [redacted] may also include [redacted]

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

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

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

[redacted] including e-mail messages that are not to, from, or about a Section 702-targeted individual. For example, [redacted] The content of [redacted] would be acquired through NSA's Section 702 upstream collection if a tasked selector appeared anywhere [redacted] ~~(TS//SI//NF)~~

As this example demonstrates, an individual Internet communication can contain a single piece of information [redacted], or it could contain multiple pieces of information [redacted] ~~(TS//SI//NF)~~

Additionally, as described in the NSA's targeting procedures, "in those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will employ either an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or [redacted]" See, e.g., DNI/AG 702(g) Certification [redacted] Exhibit A at 2. It is through these measures that NSA prevents the intentional acquisition of Internet communications that contain a reference to a targeted selector where the sender and all intended recipients are known at the time of acquisition to be located in the United States. See, e.g., In re DNI/AG Certification [redacted] No. 702(i)-08-01, Mem. Op. at 19 (USFISC Sept. 4, 2008). NSA, NSD, and ODNI are continuing to examine what affect, if any, the type of Internet communications collection discussed in this letter has on the efficacy of these measures. ~~(TS//SI//NF)~~

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

NSA, NSD, and ODNI are continuing to review and assess this matter and will provide additional information to the Court as appropriate. We appreciate the Court's consideration of this matter and welcome additional opportunities to present further information to the Court. ~~(TS//SI//NF)~~

Respectfully submitted,

[redacted]

Office of Intelligence, NSD
U.S. Department of Justice

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

Plaintiff's Exhibit 20

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

STATISTICAL TRANSPARENCY REPORT

Regarding Use of National Security Authorities

~ Calendar Year 2017 ~

LEADING INTELLIGENCE INTEGRATION

Office of Civil Liberties, Privacy, and Transparency

April 2018

STATISTICAL TRANSPARENCY REPORT

Regarding Use of National Security Authorities

~ Calendar Year 2017 ~

Table of Contents

Introduction 3
A. Background. 3
B. Areas Covered in this Report. 4
C. Context and Clarity. 5
D. Key Terms. 5
FISA Probable Cause Authorities 7
A. FISA Titles I and III 7
B. FISA Title VII, Sections 703 and 704 7
C. Statistics 8
FISA Section 702 10
A. Section 702 10
B. Statistics—Orders and Targets 12
C. Statistics—U.S. Person Queries 14
D. Section 702 and FBI Investigations. 19
NSA Dissemination of U.S. Person Information under FISA Section 702 20
A. Section 702 20
B. Statistics 22
FISA Criminal Use and Notice Provisions 25
A. FISA Sections 106 and 305 25
B. Statistics 25
FISA Title IV – Use of Pen Register and Trap and Trace (PR/TT) Devices 27
A. FISA Pen Register/Trap and Trace Authority. 27
B. Statistics 27
FISA Title V – BUSINESS RECORDS 30
A. Business Records FISA 30
B. Statistics – "Traditional" Business Records Statistics Orders, Targets & Identifiers 31
C. Statistics – Call Detail Record (CDR) Orders, Targets & Identifiers 32
D. Statistics – Call Detail Records Queries 35
NATIONAL SECURITY LETTERS (NSLs) 36
A. National Security Letters 36
B. Statistics – National Security Letters and Requests of Information 36
APPENDIX A 39

Introduction

Today, consistent with the USA FREEDOM Act and the FISA Amendments Reauthorization Act of 2017 (the reauthorized FAA) requirements to release certain statistics (codified in 50 U.S.C. § 1873(b)) and the Intelligence Community's (IC) Principles of Intelligence Transparency, we are releasing our **fifth** annual *Statistical Transparency Report Regarding Use of National Security Authorities* presenting statistics on how often the government uses certain national security authorities. Providing these statistics allows for an additional way to track the use of Foreign Intelligence Surveillance Act (FISA) authorities and gives further context to the IC's rigorous and multi-layered oversight framework that safeguards the privacy of United States person information acquired pursuant to FISA. The report goes beyond its statutory duty of providing statistics and further provides the public with detailed explanation as to how the IC uses these national security authorities.

Additional public information on national security authorities is available at the Office of the Director of National Intelligence's (ODNI) website, www.dni.gov, and ODNI's public tumblr site, *IC on the Record*. Furthermore, since the release of the previous report, ODNI has created the new website, www.intelligence.gov, that contains additional public information on the IC's activities.

A. Background.

In June 2014, the Director of National Intelligence (DNI) began releasing statistics relating to the use of critical national security authorities, including the FISA, in an annual report called the *Statistical Transparency Report Regarding Use of National Security Authorities* (hereafter the *Annual Statistical Transparency Report*). Subsequent *Annual Statistical Transparency Reports* were released in 2015, 2016, and 2017.

On June 2, 2015, the USA FREEDOM Act was enacted, codifying a requirement to publicly report many of the statistics already reported in the *Annual Statistical Transparency Report.* The Act also expanded the scope of the information included in the reports by requiring the DNI to report information concerning United States person (U.S. person or USP) search terms and queries of certain FISA-acquired information, as well as specific statistics concerning call detail records. *See* 50 U.S.C. § 1873(b). On January 19, 2018, the reauthorized FAA was signed. *See* 50 U.S.C. § 1881a. The reauthorized FAA (also referred to as the Section 702 Reauthorization Act of 2017) codified additional statistics that must be publicly released, including many statistics that the government previously reported pursuant to its commitment to transparency.

B. Areas Covered in this Report.

This report provides statistics in the following areas (the terms used below are defined and explained later in this report):

- **FISA Probable Cause Authorities.** The number of orders—and the number of targets under those orders—for the use of FISA authorities that require probable cause determinations by the Foreign Intelligence Surveillance Court (FISC), under Titles I and III, and Section 703 and 704, of FISA.

- **FISA Section 702.**
  - The number of orders—and the number of targets under those orders—issued pursuant to Section 702 of FISA.
  - The number of U.S. person queries of Section 702-acquired content and metadata.
  - The number of instances in which the Federal Bureau of Investigation (FBI) personnel received and reviewed Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence.
  - The number of instances in which the FBI opened, under the Criminal Investigative Division, an investigation of a U.S. person (who is not considered a threat to national security) based wholly or in part on Section 702-acquired information.
  - The number of National Security Agency (NSA)-disseminated Section 702 reports containing U.S. person identities (various statistics relating to reports where the U.S. person identity was openly named or originally masked and subsequently unmasked).

- **Use in Criminal Proceedings.** The number of criminal proceedings in which the United States or a State or political subdivision provided notice under FISA of the government's intent to enter into evidence or otherwise use or disclose any information derived from electronic surveillance, physical search, or Section 702 acquisition.

- **Pen Register and Trap and Trace Devices.** The number of orders—and the number of targets under those orders—for the use of FISA's pen register/trap and trace devices, and the number of unique identifiers used to communicate information collected pursuant to those orders.

- **Business Records.** The number of orders—and the number of targets under those orders—issued pursuant to FISA's business records authority, and the number of unique identifiers used to communicate information collected pursuant to those orders. In

addition, the number of orders—and the number of targets under those orders—issued pursuant to FISA's business record authority for the production of call detail records, and the number of call detail records received from providers and stored in NSA repositories.

- **National Security Letters**. The number of national security letters issued, and the number of requests for information within those national security letters.

C. Context and Clarity.

Consistent with the IC's *Principles of Intelligence Transparency*, this report seeks to enhance public understanding by including explanations and charts for context and clarity. For example, the report provides charts that place the statistics in this report in context with the statistics in prior reports. While these statistics provide an important point of reference for understanding the use of these authorities, it is important to keep in mind the statistics' limitations. The statistics fluctuate from year to year for a variety of reasons (e.g., operational priorities, world events, technical capabilities), some of which cannot be explored in an unclassified setting. Moreover, there may be no relationship between a decrease in the use of one authority and an increase in another. Nonetheless, we believe this report provides helpful information about how the IC uses these vital national security authorities.

D. Key Terms.

Certain terms used throughout this report are described below. Other terms are described in the sections in which they are most directly relevant.

- **U.S. Person**. As defined by Title I of FISA, a U.S. person is "a citizen of the United States , an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)]." 50 U.S.C. § 1801(i). Section 602 of the USA FREEDOM Act, however, uses a narrower definition. Since the broader Title I definition governs how U.S. person queries are conducted pursuant to the relevant minimization procedures, it will be used throughout this report.

- **Target.** Within the IC, the term "target" has multiple meanings. With respect to the statistics provided in this report, the term "target" is defined as the individual person, group, entity composed of multiple individuals, or foreign power that uses the selector such as a telephone number or email address.

- **Orders.** There are different types of orders that the FISC may issue in connection with FISA cases, for example: orders granting or modifying the government's authority to conduct foreign intelligence collection; orders directing electronic communication service providers to provide any technical assistance necessary to implement the authorized foreign intelligence collection; and supplemental orders and briefing orders requiring the government to take a particular action or provide the court with specific information. The FISC may amend an order one or more times after it has been issued. For example, an order may be amended to add a newly discovered account used by the target. This report *does not count such amendments* separately. The FISC may renew some orders multiple times during the calendar year. Each authority permitted under FISA has specific time limits for the FISA authority to continue (e.g., a Section 704 order against a U.S. person target outside of the United States may last no longer than 90 days but FISA permits the order to be renewed, *see* 50 U.S.C. § 1881c(c)(4)). Each renewal requires a separate application submitted by the government to the FISC and a finding by the FISC that the application meets the requirements of FISA. Thus, unlike amendments, this report *does count each such renewal* as a separate order. These terms will be used consistently throughout this report.

- **"Estimated Number."** Throughout this report, when numbers are *estimated,* the estimate comports with the statutory requirements to provide a "good faith estimate" of a particular number.

- **Dissemination.** In the most basic sense, dissemination refers to the sharing of minimized information. As it pertains to FISA (including Section 702), if an agency (in this instance NSA) lawfully collects information pursuant to FISA and wants to disseminate that information, the agency must first apply its minimization procedures to that information.

FISA Probable Cause Authorities

A. FISA Titles I and III

FISA Title I, Title III, and Title VII Section 703 and 704

→ *All of these authorities require individual court orders based on probable cause.*

→ *Titles I and III apply to FISA activities directed against persons within the United States.*

→ *Sections 703 and 704 apply to FISA activities directed against U.S. persons outside the United States.*

To conduct electronic surveillance or physical search under FISA Title I or FISA Title III, a probable cause court order is required regardless of U.S. person status. Under FISA, Title I permits electronic surveillance and Title III permits physical search in the United States of foreign powers or agents of a foreign power for the purpose of collecting foreign intelligence information. *See* 50 U.S.C. §§ 1804 and 1823. Title I (electronic surveillance) and Title III (physical search) are commonly referred to as "Traditional FISA." Both require that the FISC make a probable cause finding, based upon a factual statement in the government's application, that (i) the target is a foreign power or an agent of a foreign power, as defined by FISA and (ii) the facility being targeted for electronic surveillance is used by or about to be used, or the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power. In addition to meeting the probable cause standard, the government's application must meet the other requirements of FISA. *See* 50 U.S.C. §§ 1804(a) and 1823(a).

B. FISA Title VII, Sections 703 and 704

FISA Title VII Sections 703 and 704 similarly require a court order based on a finding of probable cause for the government to undertake FISA activities targeting U.S. persons located outside the United States. Section 703 applies when the government seeks to conduct electronic surveillance or to acquire stored electronic communications or stored electronic data, in a manner that otherwise requires an order pursuant to FISA, of a U.S. person who is reasonably believed to be located outside the United States. Section 704 applies when the government seeks to conduct collection overseas targeting a U.S. person reasonably believed to be located outside the United States under circumstances in which the U.S. person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted in the United States. Both Sections 703 and 704 require that the FISC make a

probable cause finding, based upon a factual statement in the government's application, that the target is a U.S. person reasonably believed to be (i) located outside the United States and (ii) a foreign power, agent of a foreign power, or officer or employee of a foreign power. Additionally, the government's application must meet the other requirements of FISA. *See* 50 U.S.C. §§ 1881b(b) and 1881c(b).

C. Statistics

How targets are counted. If the IC received authorization to conduct electronic surveillance and/or physical search against the same target in four separate applications, the IC would count one target, not four. Alternatively, if the IC received authorization to conduct electronic surveillance and/or physical search against four targets in the same application, the IC would count four targets. Duplicate targets across authorities are not counted.

Figure 1a: Table of FISA "Probable Cause" Court Orders and Targets

Titles I and III and Sections 703 and 704 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of orders	1,767	1,519	1,585	1,559	**1,437**
Estimated number of targets of such orders*	1,144	1,562	1,695	1,687	**1,337**

See 50 U.S.C. §§ 1873(b)(1) and 1873(b)(1)(A).

* Although providing this statistic was first required by the USA FREEDOM Act, the reauthorized FAA of 2017 enumerated this requirement at 50 U.S.C. § 1873(b)(1)(A).

Figure 1b: Chart of FISA "Probable Cause" Court Orders and Targets

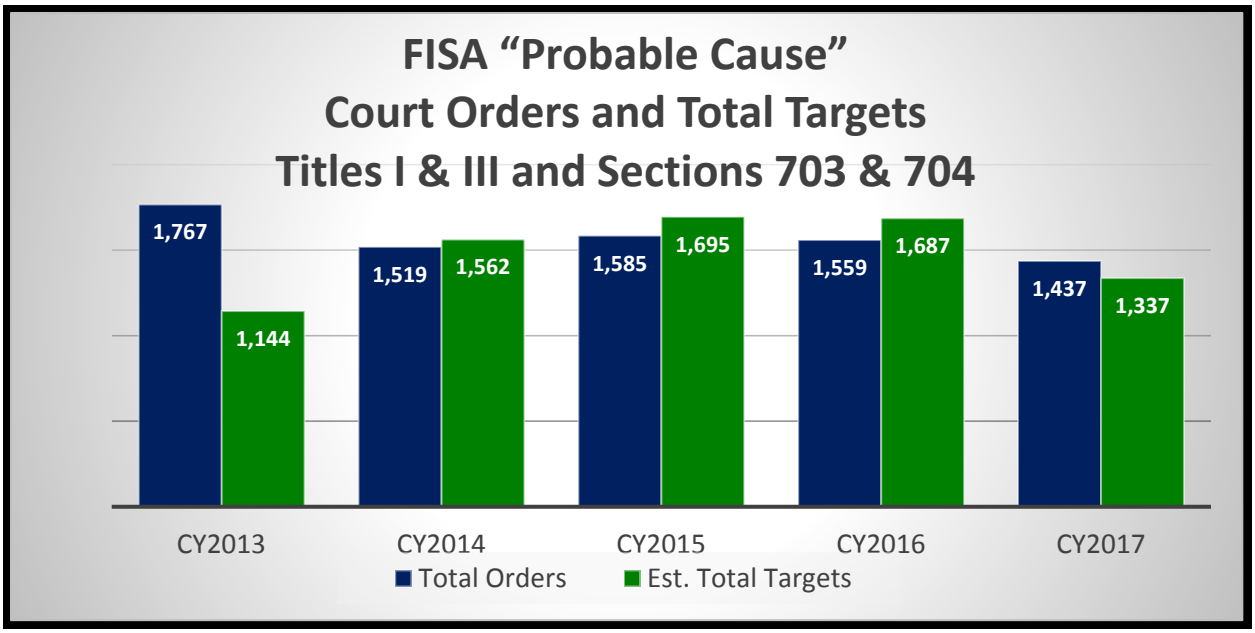


Figure 2: Table of FISA "Probable Cause" Targets – U.S. Persons

Titles I and III and Sections 703 and 704 -- Targets	CY2016	CY2017
Estimated number of targets who are *non*-U.S. persons*	1,351	**1,038**
Estimated number of targets who are U.S. persons*	336	**299**
Estimated percentage of targets who are U.S. persons	19.9%	**22.4%**

See 50 U.S.C. §§1873(b)(1)(B) and 1873(b)(1)(C) for rows one and two, respectively.

* Previously the IC was not statutorily required to publicly provide these statistics but provided them consistent with transparency principles. The reauthorized FAA of 2017 codified this requirement at 50 U.S.C. §§ 1873(b)(1)(B) and 1873(b)(1)(C).

FISA Section 702

A. Section 702

Title VII - FISA Amendments Act (FAA) Section 702

→ *Commonly referred to as "Section 702."*

→ *Requires individual targeting determinations that the target (1) is a non-U.S. person (2) who is reasonably believed to be located outside the United States and (3) who has or is expected to communicate or receive foreign intelligence information.*

Title VII of FISA includes Section 702, which permits the Attorney General and the DNI to jointly authorize the targeting of (i) non-U.S. persons (ii) reasonably believed to be located outside the United States (iii) to acquire foreign intelligence information. *See* 50 U.S.C. § 1881a. All three elements must be met. Additionally, Section 702 requires that the Attorney General, in consultation with the DNI, adopt targeting procedures, minimization procedures, and querying procedures that they attest satisfy the statutory requirements and are consistent with the Fourth Amendment. Additional information on how the government uses Section 702 is posted on *IC on the Record*.

Section 702 Targets and "Tasking." Under Section 702, the government "targets" a particular non-U.S. person, group, or entity reasonably believed to be located outside the United States and who possesses, or who is likely to communicate or receive, foreign intelligence information, by directing an acquisition at – i.e., "*tasking*" – selectors (e.g., telephone numbers and email addresses) that are assessed to be used by such non-U.S. person, group, or entity, pursuant to targeting procedures approved by the FISC. Before "tasking" a selector for collection under Section 702, the government must apply its targeting procedures to ensure that the IC appropriately tasks a selector used by a non-U.S. person who is reasonably believed to be located outside the United States and who will likely possess, communicate, or receive foreign intelligence information.

NSA and FBI task selectors pursuant to their respective Section 702 targeting procedures, which are discussed below. All agencies that receive unminimized (i.e., "raw") Section 702 data – NSA, FBI, Central Intelligence Agency (CIA), and National Counterterrorism Center (NCTC) – handle the Section 702-acquired data in accordance with minimization procedures, which are explained below.

The FISC's role. Under Section 702, the FISC determines whether *certifications* provided jointly by the Attorney General and the DNI meet all the requirements of Section 702. If the FISC determines that the government's certifications its targeting, minimization, and, as described below, querying procedures meet the statutory requirements of Section 702 and are consistent with the Fourth Amendment, then the FISC issues an order and supporting statement approving the certifications. The 2016 FISC order and statement approving certifications was publicly released in May 2017 and posted on *IC on the Record*.

Certifications. The certifications are jointly executed by the Attorney General and DNI and authorize the government to acquire foreign intelligence information under Section 702. Each annual certification application package must be submitted to the FISC for approval. The package includes the Attorney General and DNI's certifications, affidavits by certain heads of intelligence agencies, targeting procedures, minimization procedures, and, as described below, querying procedures. Samples of certification application packages have been publicly released on *IC on the Record*, most recently in May 2017. The certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information, through the targeting of non-U.S. persons reasonably believed to be located outside the United States. The certifications have included information concerning international terrorism and other topics, such as the acquisition of information concerning weapons of mass destruction.

Targeting procedures. The targeting procedures detail the steps that the government must take before tasking a selector, as well as verification steps after tasking, to ensure that the user of the tasked selector is being targeted appropriately – specifically, that the user is a non-U.S. person, located outside the United States, who is being tasked to acquire foreign intelligence information. The IC must make individual determinations that each tasked selector meets the requirements of the targeting procedures. Each agency's Section 702 targeting procedures are approved by the Attorney General and then reviewed, as part of the certification package, by the FISC, which reviews the sufficiency of each agency's targeting procedures including assessing the IC's compliance with the procedures. NSA's targeting procedures (signed in 2017) for the 2016 certification package have been publicly released *IC on the Record*.

Minimization procedures. The minimization procedures detail requirements the government must meet to use, retain, and disseminate Section 702 data, which include specific restrictions on how the IC handles non-publicly available U.S. person information acquired from Section 702 collection of non-U.S. person targets, consistent with the needs of the government to obtain, produce, and disseminate foreign intelligence information. Each agency's Section 702 minimization procedures are approved by the Attorney General and then reviewed, as part of the certification package, by the FISC, which reviews the sufficiency of each agency's

minimization procedures, including assessing the IC's compliance with past procedures. The 2016 certification minimization procedures have been released on *IC on the Record*.

Querying procedures. With the reauthorized FAA of 2017, Congress amended Section 702 to require that querying procedures be adopted by the Attorney General, in consultation with the DNI. Section 702(f) requires that a record of each U.S. person query term be kept. Similar to the other procedures, the querying procedures are required to be reviewed by the FISC as part of the certification package for consistency with the statute and the Fourth Amendment. Congress added other requirements in 702(f), which pertain to the access of certain results of queries conducted by FBI; those requirements will be discussed later in this report.

To date, each agency's court-approved minimization procedures have provided the rules under which the agency may query their databases containing previously acquired Section 702 data (content and metadata) using a U.S. person query term. As described above, with the reauthorized FAA of 2017, Congress amended Section 702 to require that, going forward, querying procedures must be adopted by the Attorney General. Query terms may be date-bound, and may include alphanumeric strings, such as telephone numbers, email addresses, or terms, such as a name, that can be used individually or in combination with one another. Pursuant to court-approved procedures, an agency can only query Section 702 information if the query is reasonably likely to return foreign intelligence information or, in the case of the FBI, evidence of a crime. Additional information about U.S. person queries is posted on *IC on the Record*.

Compliance. The IC's adherence to the targeting and minimization procedures, including query requirements, is subject to robust internal agency oversight and to rigorous external oversight by the Department of Justice (DOJ), ODNI, Congress, and the FISC. Every identified incidence of non-compliance is reported to the FISC (through individual notices or in reports) and to Congress in semiannual reports. DOJ and ODNI also submit semiannual reports to Congress that assess the IC's overall compliance efforts. Past assessments have been publicly released.

B. Statistics—Orders and Targets

Counting Section 702 orders. As explained above, the FISC may issue a single order to approve more than one Section 702 certification to acquire foreign intelligence information. Note that, in its own transparency report, which is required pursuant to 50 U.S.C. § 1873(a), the Director of the Administrative Office of the United States Courts (AOUSC) counted each of the Section 702 certifications associated with the FISC's order. Because the number of the government's Section 702 certifications remains a classified fact, the government requested that the AOUSC redact the number of certifications from its transparency report prior to publicly releasing it.

In 2016, the government submitted a certification application package to the FISC. Pursuant to 50 U.S.C. § 1881a(j)(2), the FISC extended its review of the 2016 certification package. The FISC may extend its review of the certifications "as necessary for good cause in a manner consistent with national security." *See* 50 U.S.C. § 1881a(j)(2) (note that with the reauthorized FAA of 2017, this section has been updated to § 1881a(k)(2)). Thus, because the FISC did not complete its review of the 2016 certifications during calendar year 2016, the FISC did not issue an order concerning those certifications in calendar year 2016. The 2015 order remained in effect during the extension period. On April 26, 2017, the FISC issued an order authorizing the 2016 certifications.

Figure 3: Table of Section 702 Orders

Section 702 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of orders issued	1	1	1	0	**1**

See 50 U.S.C. § 1873(b)(2).

Estimating Section 702 targets. The number of 702 "targets," provided below, reflects an estimate of the number of non-U.S. persons who are the users of tasked selectors. This estimate is based on information readily available to the IC. Unless and until the IC has information that links multiple selectors to a single foreign intelligence target, each individual selector is counted as a separate target for purposes of this report. On the other hand, where the IC is aware that multiple selectors are used by the same target, the IC counts the user of those selectors as a single target. This counting methodology reduces the risk that the IC might inadvertently understate the number of discrete persons targeted pursuant to Section 702.

Figure 4: Table of Section 702 Targets (recall that only non-USPs are targeted)

Section 702 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017
Estimated number of targets of such orders*	89,138	92,707	94,368	106,469	**129,080**

See 50 U.S.C. § 1873(b)(2)(A).

* Previously the IC was not statutorily required to publicly provide this statistic, but provided it consistent with transparency principles. The reauthorized FAA of 2017 codified this requirement at 50 U.S.C. § 1873(b)(2)(A).

C. Statistics—U.S. Person Queries

In July 2014, the Privacy and Civil Liberties Oversight Board (PCLOB or Board) issued a report on Section 702 entitled, "*Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*" (*PCLOB's Section 702 Report*), which reported U.S. person query statistics for calendar year 2013. *See PCLOB's Section 702 Report,* at 57-58. The USA FREEDOM Act, enacted in 2015, required the public reporting of statistics regarding the number of U.S. person queries of Section 702. Specifically, the Act required the "number of search terms concerning a known United States person used to retrieve the unminimized contents […]" – referred as *query terms of content* – and "the number of queries concerning a known United States person of unminimized noncontents information […]" – referred as *queries of metadata*. *See* 50 U.S.C. § 1873(b)(2)(B) and (b)(2)(C), respectively. Thus, ODNI began reporting on these statistics in the *Annual Statistical Transparency Report* covering calendar year 2015.

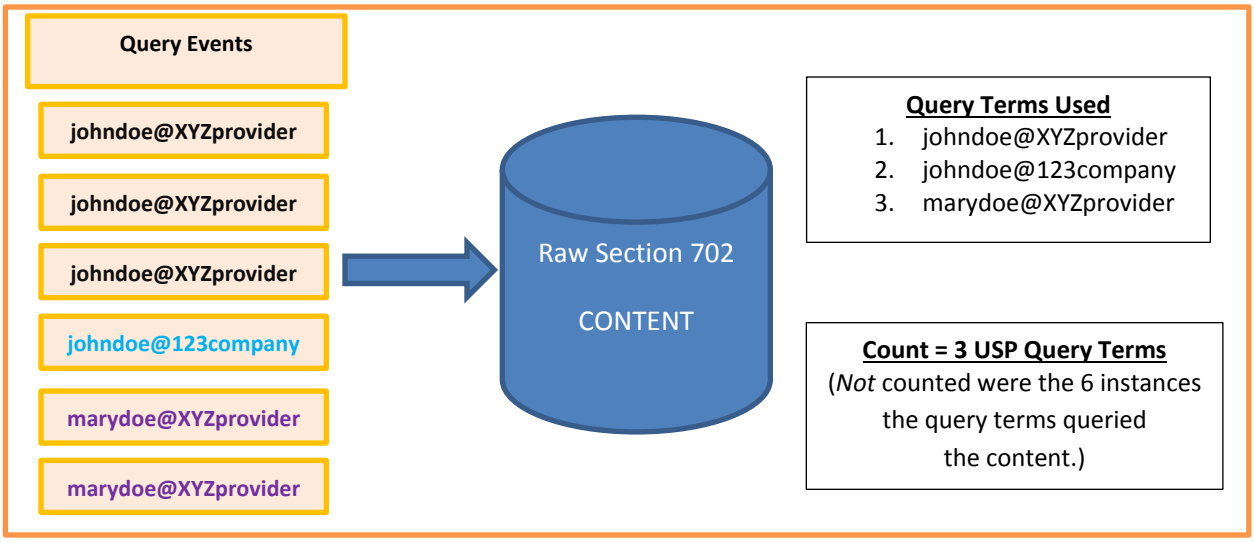
Below are statistics for U.S. person queries of raw, unminimized Section 702-acquired data.[1] The U.S. person statistics are based on (a) approved U.S. person *query terms* used to query

[1] With the reauthorization of FAA in 2017, Congress codified new requirements regarding the access of results of certain queries conducted by the FBI. Specifically under Section 702(f)(2)(A), an order from the FISC is now required before the FBI can review the contents of a query using a U.S. person query term when the query was not designed to find and extract foreign intelligence information and was performed in connection with a predicated criminal investigation that does not relate to national security. Before the FISC may issue such an order based on a finding of probable cause, an FBI officer must apply in writing, to include the officer's justification that the query results would provide evidence of criminal activity, and the application must be approved by the Attorney General.

Section 702 *content* and (b) U.S. person *queries* conducted of Section 702 *noncontents* (i.e., metadata). It is important to understand that these two very different numbers cannot be combined because they use *different counting methodologies* (approved query terms versus queries conducted) and *different data types* (content versus noncontents).

Counting approved U.S. person *query terms* used to query Section 702 *content*. The NSA counts the number of U.S. person identifiers it approved to query the content of unminimized Section 702-acquired information. For example, if the NSA used U.S. person identifier "johndoe@XYZprovider" to query the content of Section 702-acquired information, the NSA would count it as one regardless of how many times the NSA used "johndoe@XYZprovider" to query its 702-acquired information. The CIA started using this model in 2016 for counting query terms and those statistics were included in the *Annual Statistical Transparency Report* covering CY2016. When the NCTC began receiving raw Section 702 information, NCTC followed a similar approach of counting U.S. person query terms that were used to query Section 702 content.

Figure 5: Illustration of how the IC counts approved U.S. person query terms used to query Section 702 content



50 U.S.C. Section 1873(b)(2)(A) requires annual reporting of the number of times the FBI received an order pursuant to 702(f)(2)(A); this statistic will be provided in future transparency reports.

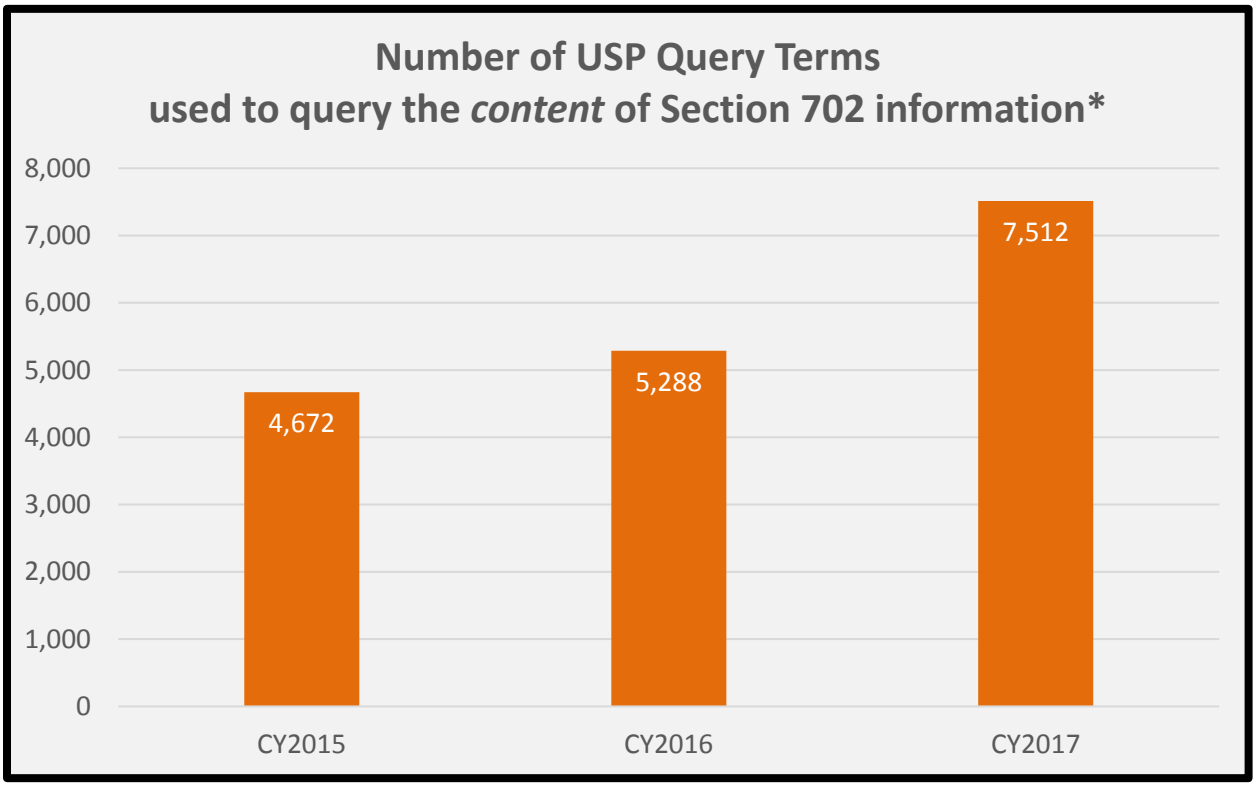
Figure 6a: Table of U.S. Person Query Terms Used to Query Section 702 Content

Section 702 of FISA	CY2015	CY2016	CY2017
Estimated number of search terms concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702 (excluding search terms used to prevent the return of U.S. person information)*	4,672	5,288	**7,512**

See 50 U.S.C. § 1873(b)(2)(B).

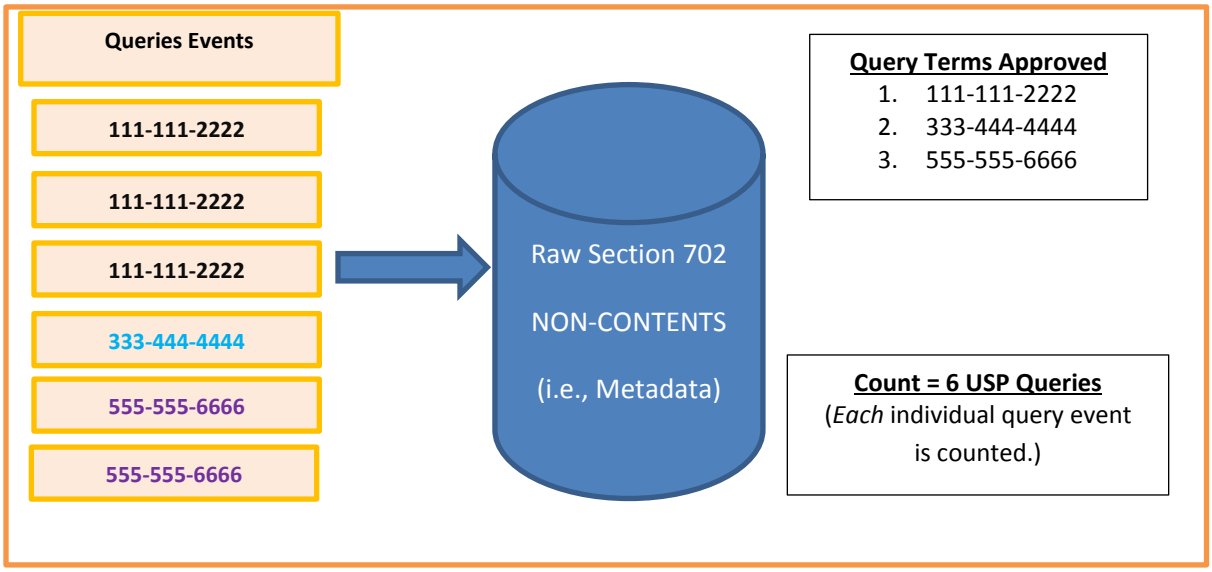
* Consistent with 50 U.S.C. § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI. However, the reauthorized FAA of 2017 codified a new reporting requirement for the FBI under 50 U.S.C. § 1873(b)(2)(D), which is addressed later in this report.

Figure 6b: Chart of U.S. Person Query Terms Used to Query Section 702 Content



Counting *queries* using U.S. person identifiers of noncontents collected under Section 702. This estimate represents the number of times a U.S. person identifier is used to query the noncontents (i.e., metadata) of unminimized Section 702-acquired information. For example, if the U.S. person identifier telephone number "111-111-2222" was used 15 times to query the noncontents of Section 702-acquired information, the number of queries counted would be 15.

Figure 7: Illustration of how the IC counts U.S. person queries of Section 702 noncontents



As with last year's transparency report, one IC element, the CIA, remains currently unable to provide the number of queries using U.S. person identifiers of unminimized Section 702 noncontents information for CY2017. Under 50 U.S.C. § 1873(d)(3)(A), if the DNI concludes that this good-faith estimate cannot be determined accurately because not all of the relevant elements of the IC are able to provide this good faith estimate, then the DNI is required to (i) certify that conclusion in writing to the relevant Congressional committees; (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate; (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and (iv) make such certification publicly available on an Internet web site. Because the CIA remained unable to provide such information for calendar year 2017, the DNI made a certification, pursuant to 50 U.S.C. § 1873(d)(3)(A) to the relevant Congressional committees. As required by statute, this certification is being made publicly available as an attached appendix to this current report (see Appendix A). As described in Appendix A, CIA will be able to provide a good faith estimate of these queries for calendar year 2018; such information will be included in the 2019 annual transparency report.

Figure 8: Table of U.S. Person Queries of Noncontents of Section 702

Section 702 of FISA	CY2013	CY2014	CY2015	CY2016	CY2017
Estimated number of queries concerning a known U.S. person of unminimized noncontents information obtained under Section 702 (excluding queries containing information used to prevent the return of U.S. person information)*	9,500	17,500	23,800	30,355	**16,924**

See 50 U.S.C. § 1873(b)(2)(C).

* Consistent with 50 U.S.C. § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI. However, the reauthorized FAA of 2017 codified a new reporting requirement for the FBI under 50 U.S.C. § 1873(b)(2)(D), which was addressed earlier in this report.

FISC Order Requiring Certain Section 702 Query Reporting by FBI. On November 6, 2015, the FISC granted the government's application for renewal of the 2015 certifications and, among other things, concluded that the FBI's U.S. person querying provisions in its minimization procedures, "strike a reasonable balance between the privacy interests of the United States persons and persons in the United States, on the one hand, and the government's national security interests, on the other." *Memorandum Opinion and Order* dated November 6, 2015, at 44 (released on *IC on the Record* on April 19, 2016). The FISC further stated that the FBI conducting queries, "designed to return evidence of crimes unrelated to foreign intelligence does not preclude the Court from concluding that taken together, the targeting and minimization procedures submitted with the 2015 Certifications are consistent with the requirements of the Fourth Amendment." *Id*.

Nevertheless, the FISC ordered the government to report in writing, "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." (Emphasis added). *Id*. at 44 and 78. The FISC directed that the report contain details of the query terms, the basis for conducting the query, the manner in which the query will be or has been used, and other details. *Id.* at 78. In keeping with the IC's *Principles of Transparency*, the DNI declassified the number of each such query reported to the FISC in calendar year 2016. This year, the DNI has again declassified the number reported for calendar year 2017, as noted in Figure 10.

Figure 9: Table Regarding Required Section 702 Query Reporting to the FISC

Section 702 of FISA	CY2016	CY2017
Per the FISC Memorandum Opinion and Order dated November 6, 2015: Each reported instance in which FBI personnel *received and reviewed* Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence.	1	**0**

D. Section 702 and FBI Investigations.

The reauthorized FAA of 2017 now requires that the FBI report on the number of instances in which the FBI opened a criminal investigation of a U.S. person, who is not considered a threat to national security, based wholly or in part on Section 702-acquired information. *See* 50 U.S.C. § 1873(b)(2)(D). This statistic will provide transparency with regard to how often Section 702 collection is used for non-national security investigations conducted by the FBI. Figure 10 provides the required statistic.

Figure 10: Table Regarding Number of FBI Investigations Opened on USPs Based on Section 702 Acquisition

Section 702 of FISA	CY2017
The number of instances in which the FBI opened, under the Criminal Investigative Division or any successor division, an investigation of a U.S. person (who is not considered a threat to national security) based wholly or in part on an acquisition authorized under Section 702.	**0**

See 50 U.S.C. § 1873(b)(2)(D).

NSA Dissemination of U.S. Person Information under FISA Section 702

A. Section 702

In July 2014, the *PCLOB's Section 702 Report* contained 10 recommendations. Recommendation 9 focused on "accountability and transparency," noting that the government should implement 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." *PCLOB's Section 702 Report* at 145-146. Specifically, the PCLOB recommended that "the NSA should implement processes to annually count […] (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, such as telephone numbers or e-mail addresses, potentially associated with individuals." *Id.* at 146. This recommendation is commonly referred to as Recommendation 9(5). In response to the PCLOB's July 2014 Recommendation 9(5), NSA previously publicly provided (in the *Annual Statistical Transparency Report* for calendar year 2015) and continues to provide the following additional information regarding the dissemination of Section 702 intelligence reports that contain U.S. person information. Because the PCLOB issued its recommendation in 2014, these statistics were not included in *Annual Statistical Transparency Report* for calendar years 2013 or 2014.

NSA has been providing similar information to Congress since 2009, in classified form, per FISA reporting requirements. For example, FISA Section 702(m)(3) requires that NSA annually submit a report to applicable Congressional committees regarding certain numbers pertaining to the acquisition of Section 702-acquired information, including the number of "disseminated intelligence reports containing a reference to a United States person identity." *See* 50 U.S.C. § 1881a(m)(A)(3)(i) (prior to the reauthorized FAA of 2017under § 1881a(l)(3)(A)(i)). Section 702a(m)(A)(3) also requires that the number of "United States-person identities subsequently disseminated by [NSA] in response to request for identities that were not referred to by name or title in the original reporting." *See* 50 U.S.C. § 1881a(m)(3)(A)(ii). This second requirement refers to NSA providing the number of approved unmasking requests, which is explained below. Additionally, NSA provides the number of NSA's disseminated intelligence reports containing a U.S. person reference to Congress as part of the Attorney General and the DNI's joint assessment of compliance. *See* 50 U.S.C. § 1881a(m)(1) (prior to the reauthorized FAA of 2017under § 1881a(l)(1)).

Prior to the PCLOB issuing its *Section 702 Report*, NSA's Director of the Civil Liberties, Privacy, and Transparency Office published "*NSA's Implementation of Foreign Intelligence Surveillance Act Section 702,"* on April 16, 2014, (hereinafter "NSA DCLPO Report"), in which it explained

NSA's dissemination processes. *NSA DCLPO Report* at 7-8. NSA "only generates classified intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information." *NSA DCLPO Report* at 7.

Section 702 only permits the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. Such targets, however, may communicate information to, from, or about U.S. persons. NSA minimization procedures (publicly released on May 11, 2017) permit the NSA to disseminate U.S person information if the NSA masks the information that could identify the U.S. person. The minimization procedures also permit NSA to disseminate the U.S. person identity only if doing so meets one of the specified reasons listed in NSA's minimization procedures, including that the U.S. person consented to the dissemination, the U.S. person information was already publicly available, the U.S. person identity was necessary to understand foreign intelligence information, or the communication contained evidence of a crime and is being disseminated to law enforcement authorities. Even if one these conditions applies, as a matter of policy, NSA may still mask the U.S. person information and will include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. *Id.* In certain instances, however, NSA makes a determination prior to releasing its original classified report that the U.S. person's identity is appropriate to disseminate in the first instance using the same standards discussed above.

Masked U.S. Person Information. Agency minimization procedures generally provide for the substitution of a U.S. person identity with a generic phrase or term if the identity otherwise does not meet the dissemination criteria; this is informally referred to as "masking" the identity of the U.S. person. Information about a U.S. person is masked when the identifying information about the person is not included in a report. For example, instead of reporting that Section 702-acquired information revealed that non-U.S. person "Bad Guy" communicated with U.S. person "John Doe" (i.e., the actual name of the U.S. person), the report would mask "John Doe's" identity, and would state that "Bad Guy" communicated with "an identified U.S. person," "a named U.S. person," or "a U.S. person."

Unmasking U.S. Person Information. Recipients of NSA's classified reports, such as other federal agencies, may request that NSA provide the U.S. person identity that was masked in an intelligence report. The requested identity information is released only if the requesting recipient has a "need to know" the identity of the U.S. person and if the dissemination of the U.S. person's identity would be consistent with NSA's minimization procedures (e.g., the identity is necessary to understand foreign intelligence information or assess its importance), and additional approval has been provided by a designated NSA official.

As part of their regular oversight reviews, DOJ and ODNI review disseminations of information about U.S. persons that NSA obtained pursuant to Section 702 to ensure that the disseminations were performed in compliance with the minimization procedures.

Additional information describing how the IC protects U.S. person information obtained pursuant to FISA provisions is provided in recent reports by the civil liberties and privacy officers for the ODNI (including NCTC), NSA, FBI, and CIA. The reports collectively documented the rigorous and multi-layered framework that safeguards the privacy of U.S. person information in FISA disseminations. *See ODNI Report on Protecting U.S. Person Identities in Disseminations under FISA* and annexes containing agency specific reports.

B. Statistics

Below are statistics and charts to further explain how NSA disseminates U.S. person information incidentally acquired from Section 702 in classified intelligence reports. NSA may:

i. openly name (i.e., originally reveal) the U.S. person in the report,
ii. initially mask (i.e., not reveal) the U.S. person identity in the report, or
iii. in the instances where the U.S. person identity was initially masked, upon a specific request, later reveal and unmask the U.S. person identity but only to the requestor.

This year's report presents the dissemination numbers in a different format from the previous report to facilitate understanding and to provide consistency with NSA's classified FISA Section 702(m)(3) reports to Congress. This report separates the number of reports (in Figure 11) from the statistics relating to the U.S. person identities later disseminated (in Figure 12).

NSA applies its minimization procedures in preparing its classified intelligence reports, and then disseminates the reports to authorized recipients with a need to know the information in order to perform their official duties. Very few of NSA's intelligence reports from Section 702 collection contain references to U.S. person identities (whether masked or openly named).

The first row of Figure 11 provides "an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity." *See* 50 U.S.C. § 1881a(m)(3)(A)(i). Note that a single report could contain multiple U.S. person identities, masked and/or openly named. NSA's counting methodology is to include any disseminated intelligence report that contains a reference to one or more U.S. person identities, whether masked or openly named, even if the report includes information from other sources. NSA does not maintain records that allow it to readily determine, in the case of an intelligence report that includes information from several sources, from which source a reference to a U.S. person identity was derived. Accordingly, the references to U.S. person identities may have resulted

from Section 702 authorized collection or from other authorized signals intelligence activity conducted by NSA. This counting methodology was used in the previous report and is used in NSA's FISA Section 702(m)(3) report. As noted above, a U.S. person is "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in [50 U.S.C. § 1801(a)(1), (2), or (3)]." *See* 50 U.S.C. § 1801(i).

The second row of Figure 11 provides the *number of reports* containing U.S. person identities *where the U.S. person identity was masked* in the report. The third row provides the *number of reports* containing U.S. person *identities where the U.S. person was openly named* in the report.

Figure 11: Table of Section 702 *Reports* Containing USP information unmasked by NSA

Section 702 Reports Containing U.S. person (USP) information disseminated by NSA	CY2016	CY2017
Reports – Total number of NSA disseminated §702 reports containing USP identities *regardless of whether the identity was openly named or masked*.	3,914	**4,065**
Reports – Total number of NSA disseminated §702 reports containing USP identities *where the USP identity was masked.*	2,964	**3,034**
Reports – Total number of NSA disseminated §702 reports containing USP identities *where the USP was openly named*.	1,200	**1,341**

As explained above, rows 2 and 3 will not total row 1 because one report may contain both masked and openly namely identities.

Figure 12 provides statistics relating to the numbers of U.S. person identities that were originally masked in those reports counted in Figure 11 but which NSA later provided to authorized requestors (i.e., unmasked) during CY2017. This statistic is the number required to be reported to Congress in NSA's FISA Section 702(m)(3) report. In other words, Figure 12 provides "an accounting of the number of United States-person identities subsequently disseminated by [NSA] in response to requests for identities that were not referred to by name or title in the original reporting." *See* 50 U.S.C. § 1881a(m)(3)(A)(ii). This number is different than numbers provided in either CY2015 or the CY2016 *Annual Statistical Transparency Report*. NSA has decided to declassify the total number of U.S. person identities unmasked in response to a request. The U.S. person identities include individuals as well as non-individual entities

whose identities NSA masks pursuant to law or policy. These non-individual entities, include, for example, U.S. IP addresses and artificial "persons" such as corporations.

Previously, the *Annual Statistical Transparency Report* focused on responding to the PCLOB's report recommendation 9(5) by counting only those U.S. person identities where the proper name or title of an individual was unmasked; it did not count any other unmasking such as email addresses or telephone numbers or U.S. IP addresses or U.S. corporations. Rather than distinguishing between the different ways a U.S. person might be named in an intelligence report, NSA will provide the total number of U.S. person identities unmasked in response to a specific request from another agency whether it is a title of an individual, an identifier such as an email address, an IP address or a corporation. Thus, this current *Annual Statistical Transparency Report*, in Figure 12, reports that same metric that is reported in NSA's FISA Section 702(m)(3). However, because NSA's FISA Section 702(m)(3) reports have a time period of September through August, comparing the two reporting years is not an exact comparison.

Figure 12: Table of Section 702 USP Identities disseminated by NSA

Section 702 – U.S. person (USP) identities unmasked by NSA	12 month period Sep 2015-Aug 2016	CY2017
The number of U.S. person identities that NSA unmasked in response to a specific request from another agency.	9,217	**9,529**

Beginning with next year's transparency report (due April 2019), ODNI will report statistics pertaining to how the IC disseminates U.S. person information regardless of the legal authority under which the information was collected (not only FISA Section 702). *See* ICPG 107.1. Specifically, ODNI will report (1) the total number of requests to identify U.S. persons, whose identity was originally omitted, in disseminated intelligence reports, (2) the total number of those requests approved, and (3) the total number of those requests denied.

FISA Criminal Use and Notice Provisions

A. FISA Sections 106 and 305

FISA Sections 106 and 305
– Criminal Use and Notice Provisions –

→ *Commonly referred to as the "criminal use provision."*

→ *Section 106 applies to information acquired from Title I electronic surveillance; Section 305 applies to information acquired from Title III physical search.*

→ *Attorney General advance authorization is required before such information may be used in a criminal proceeding; if such information is used or intended to be used against an aggrieved person, that person must be given notice of the information and have a chance to suppress the information.*

→ *The reauthorized FAA of 2017 codified that statistics must be provided to the public as it pertained to Section 106, Section 305, as well as Section 702 acquired information.*

FISA Section 106 requires advance authorization from the Attorney General before any information acquired through Title I electronic surveillance may be used in a criminal proceeding. This authorization from the Attorney General is defined to include authorization by the Acting Attorney General, Deputy Attorney General, or, upon designation by the Attorney General, the Assistant Attorney General for National Security. Section 106 also requires that if a government entity intends to introduce into evidence in any trial, hearing, or other proceeding, against an aggrieved person, information obtained or derived from electronic surveillance, it must notify the aggrieved person and the court. The aggrieved person is then entitled to seek suppression of the information. FISA Section 706 requires that any information acquired pursuant to Section 702 be treated as electronic surveillance under Title I, including for purposes of the use, notice, and suppression requirements under Section 106.

FISA Section 305 provides the same requirements for information acquired through Title III physical search (i.e., advance authorization, notice, and opportunity to suppress).

B. Statistics

The reauthorized FAA of 2017codified that certain statistics concerning criminal proceedings must be provided to the public pertaining to Sections 106 and 305, including Section 702-acquired information. Specifically, figure 13 provides that, in 2017, the Government filed notice of intent to use FISA-acquired information, pursuant to Section 106 or 305, in seven (7) separate criminal proceedings.

Figure 13: Table Regarding Number of Criminal Proceedings in which the Government Provided Notice of Its Intent to Use Cert FISA Information

FISA Sections 106 and 305	CY2017
The number of criminal proceedings in which the United States or a State or political subdivision thereof provided notice pursuant to Section 106 (including with respect to Section 702-acquired information) or Section 305 of the government's intent to enter into evidence or otherwise use or disclose any information obtained or derived from electronic surveillance, physical search, or Section 702 acquisition.	**7**

FISA Title IV – Use of Pen Register and Trap and Trace (PR/TT) Devices

A. FISA PR/TT Authority

FISA Title IV

→ *Commonly referred to as the "PR/TT" provision.*

→ *Bulk collection is prohibited.*

→ *Requires individual FISC order to use PR/TT device to capture dialing, routing, addressing, or signaling (DRAS) information.*

→ *Government request to use a PR/TT device on U.S. person target must be based on an investigation to protect against terrorism or clandestine intelligence activities and that investigation must not be based solely on the basis of activities protected by the First Amendment to the Constitution.*

Title IV of FISA authorizes the use of pen register and trap and trace (PR/TT) devices for foreign intelligence purposes. Title IV authorizes the government to use a PR/TT device to seek and capture dialing, routing, addressing or signaling (DRAS) information. The government may submit an application to the FISC for an order approving the use of a PR/TT device (i.e., PR/TT order) for (i) "any investigation to obtain foreign intelligence information not concerning a United States person or" (ii) "to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution." 50 U.S.C. § 1842(a). If the FISC finds that the government's application sufficiently meets the requirements of FISA, the FISC must issue an order for the installation and use of a PR/TT device.

B. Statistics

Counting orders. Similar to how orders were counted for Titles I and III and Sections 703 and 704, this report only counts the orders *granting authority to conduct intelligence collection* -- the order for the installation and use of a PR/TT device. Thus, renewal orders are counted as a separate order; modification orders and amendments are not counted.

Estimating the number of targets. The government's methodology for counting PR/TT targets is similar to the methodology described above for counting targets of electronic surveillance and/or physical search. If the IC received authorization for the installation and use of a PR/TT device against the same target in four separate applications, the IC would count one target, not

four. Alternatively, if the IC received authorization for the installation and use of a PR/TT device against four targets in the same application, the IC would count four targets.

Estimating the number of unique identifiers. This statistic counts (1) the targeted identifiers and (2) the non-targeted identifiers (e.g., telephone numbers and e-mail addresses) that were in contact with the targeted identifiers. Specifically, the House Report on the USA FREEDOM Act states that "[t]he phrase 'unique identifiers used to communicate information collected pursuant to such orders' means the total number of, for example, email addresses or phone numbers that have been collected as a result of these particular types of FISA orders--not just the number of target email addresses or phone numbers." [H.R. Rept. 114-109 Part I, p. 26], with certain exceptions noted.

Figure 14: Table of PR/TT Orders, Targets, and Unique Identifiers Collected

Title IV of FISA ***PR/TT FISA***	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of orders	131	135	90	60	**33**
Estimated number of targets of such orders	319	516	456	41	**27**
Estimated number of unique identifiers used to communicate information collected pursuant to such orders*	-	-	134,987#	81,035#†	**56,064#**

See 50 U.S.C. §§ 1873(b)(3), 1873(b)(3)(A), and 1873(b)(3)(B).

* Pursuant to §1873(d)(2)(B), this statistic does not apply to orders resulting in the acquisition of information by the FBI that does not include electronic mail addresses or telephone numbers.

This number represents information the government received from provider(s) electronically for the entire calendar year. The government does not have a process for capturing unique identifiers received by other means (such as hard-copy or portable media).

† Last year, the FBI mistakenly interchanged the number of unique identifiers for business records and PR/TT orders, reporting the number of business records unique identifiers as PR/TT unique identifiers and vice versa. This report corrects the error and accurately identifies the legal authority under which the FBI obtained the unique identifiers.

Figure 15: Table of FISA PR/TT Targets – U.S. Persons and Non-U.S. Persons*

PR/TT Targets	CY2016	CY2017
Estimated number of targets who are *non*-U.S. persons	23	**16**
Estimated number of targets who are U.S. persons	18	**11**
Estimated percentage of targets who are U.S. persons	43.9%	**40.7%**

See 50 U.S.C. §§1873(b)(3)(A)(i) and 1873(b)(3)(A)(ii) for rows one and two, respectively.

* Previously the IC was not statutorily required to publicly provide these statistics, but provided them consistent with transparency principles. The reauthorized FAA of 2017 codified this requirement at 50 U.S.C. §§ 1873(b)(3)(A)(i) and 1873(b)(3)(A)(ii).

FISA Title V – Business Records

A. Business Records FISA

Under FISA, Title V authorizes the government to submit an application for an order requiring the production of any tangible things for (i) "an investigation to obtain foreign intelligence information not concerning a United States person or" (ii) "to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution." 50 U.S.C. § 1861. Title V is commonly referred to as the *"Business Records"* provision of FISA.

FISA Title V

→ *Commonly referred to as "Business Records" provision.*

→ *Bulk collection is prohibited.*

→ *Call Detail Records (CDRs) may be obtained from a telephone company if the FISC issues an individual court order for target's records.*

→ *Request for records in an investigation of a U.S. person must be based on an investigation to protect against terrorism or clandestine intelligence activities and provided that the investigation is not conducted solely upon activities protected by the First Amendment to the Constitution.*

In June 2015, the USA FREEDOM Act was signed into law and, among other things, it amended Title V, including by prohibiting bulk collection. *See* 50 U.S.C. §§ 1861(b), 1861(k)(4). The DNI is required to report various statistics about two Title V provisions – traditional business records and call detail records (discussed further below). On November 28, 2015, in compliance with amendments enacted by the USA FREEDOM Act, the IC terminated collection of bulk telephony metadata under Title V of the FISA (the "Section 215 Program"). Solely due to legal obligations to preserve records in certain pending civil litigation, including *First Unitarian Church of Los Angeles, et al. v. National Security Agency, et al.*, No. C 13-03287-JSW (N.D. Cal.) and *Jewel, et al. v. National Security Agency, et al.*, No. C 08-04373-JSW (N.D. Cal.), the IC continues to preserve previously collected bulk telephony metadata. Under the terms of a FISC order dated November 24, 2015, the bulk telephony metadata cannot be used or accessed for any purpose other than compliance with preservation obligations. Once the government's preservation obligations are lifted, the government is required to promptly destroy all bulk metadata produced by telecommunications providers under the Section 215 Program.

As noted in last year's *Annual Statistical Transparency Report*, on November 30, 2015, the IC implemented certain provisions of the USA FREEDOM Act, including the call detail records provision and the requirement to use a specific selection term. Accordingly, only one month's worth of data for calendar year 2015 was available with respect to those provisions. Any statistical information relating to a particular FISA authority for a particular month remains classified. Therefore, the Title V data specifically associated with December 2015 was only released in a classified annex provided to Congress as part of the report for CY2015. For the CY 2016 report, statistical information was collected for an entire year under the USA FREEDOM Act Title V provisions. As a result, those statistics were included in that report. For the CY 2017 report, statistical information was collected for an entire year under the USA FREEDOM Act Title V provisions. As a result, those statistics are included in this report.

Statistics related to *traditional business records* under Title V Section 501(b)(2)(B) are provided first pursuant to 50 U.S.C. § 1873(b)(5). Statistics related to *call detail records* under Title V Section 501(b)(2)(C) are provided second pursuant to 50 U.S.C. § 1873(b)(6).

B. Statistics – "Traditional" Business Records Statistics Orders, Targets & Identifiers

Business Record (BR) requests for tangible things include books, records, papers, documents, and other items pursuant to 50 U.S.C. §1861(b)(2)(B), also referred to as Section 501(b)(2)(B) . These are commonly referred to as "Traditional" Business Records.

Estimating the number of unique identifiers. This is an estimate of the number of (1) targeted identifiers (e.g., telephone numbers and email addresses) and (2) non-targeted identifiers that were in contact with the targeted identifiers. This metric represents unique identifiers received electronically from the provider(s). The government does not have a process for capturing unique identifiers received by other means (i.e., hard-copy or portable media).

Explaining how we count BR statistics. As an example of the government's methodology, assume that in 2017, the government submitted a BR request targeting "John Doe" with email addresses john.doe@serviceproviderX, john.doe@serviceproviderY, and john.doe@serviceproviderZ. The FISC found that the application met the requirements of Title V and issued orders granting the application and directing service providers X, Y, and Z to produce business records pursuant to Section 501(b)(2)(B). Provider X returned 10 non-targeted email addresses that were in contact with the target; provider Y returned 10 non-targeted email addresses that were in contact with the target; and provider Z returned 10 non-targeted email addresses that were in contact with the target. Based on this scenario, we would report the following statistics: A) one order by the FISC for the production of tangible things, B)

one target of said orders, and C) 33 unique identifiers, representing three targeted email addresses plus 30 non-targeted email addresses.

Figure 16: Table of "Traditional" Business Records Orders, Targets, and Unique Identifiers Collected

Business Records "BR" – Section 501(b)(2)(B)	CY2016	CY2017
Total number of orders issued pursuant to applications under Section 501(b)(2)(B)	84	**77**
Estimated number of targets of such orders	88	**74**
Estimated number of unique identifiers used to communicate information collected pursuant to such orders	125,354†	**87,834**

See 50 U.S.C. §§ 1873(b)(5), 1873(b)(5)(A), and 1873(b)(5)(B).
† Last year, the FBI mistakenly interchanged the number of unique identifiers for business records and PR/TT orders, reporting the number of business records unique identifiers as PR/TT unique identifiers and vice versa. This report corrects the error and accurately identifies the legal authority under which the FBI obtained the unique identifiers.

C. Statistics – Call Detail Record (CDR) Orders, Targets & Identifiers

Call Detail Records (CDRs) – commonly referred to as "call event metadata" – may be obtained from traditional telecommunications providers pursuant to 50 U.S.C. §1861(b)(2)(C). A CDR is defined as session identifying information (such as originating or terminating telephone number, an International Mobile Subscriber Identity (IMSI) number, or an International Mobile Station Equipment Identity (IMEI) number), a telephone calling card number, or the time or duration of a call. *See* 50 U.S.C. §1861(k)(3)(A). CDRs provided to the government do not include the content of any communication, the name, address, or financial information of a subscriber or customer, or cell site location or global positioning system information. *See* 50 U.S.C. §1861(k)(3)(B). CDRs are stored and queried by the service providers. *See* 50 U.S.C. §1861(c)(2).

Estimating the number of targets of CDR orders. A "target" is the person using the selector. For example, if a target uses four selectors that have been approved, the number counted for purposes of this report would be one target, not four. Alternatively, if two targets are using one selector that has been approved, the number counted would be two targets.

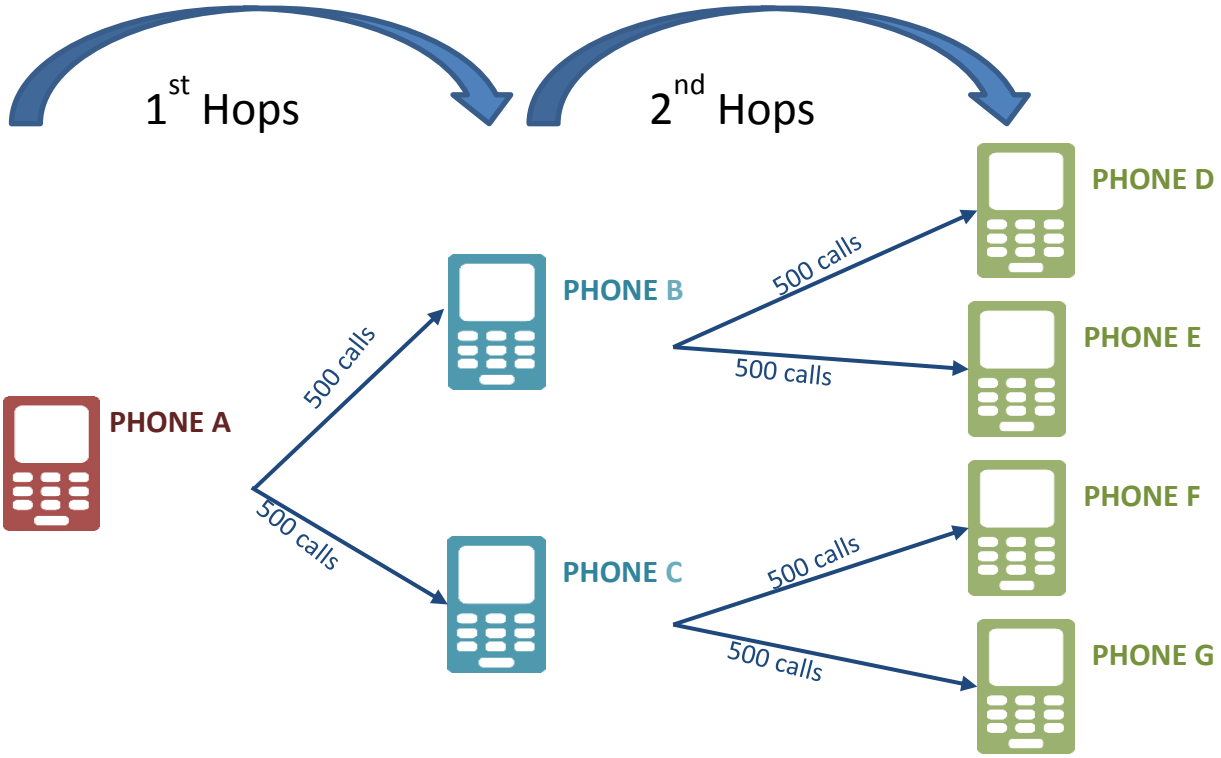
Figure 17: Table of CDR Orders and Targets

Call Detail Records "CDRs" – Section 501(b)(2)(C)	CY2016	CY2017
Total number of orders issued pursuant to applications under Section 501(b)(2)(C)	40	**40**
Estimated number of targets of such orders	42	**40**

See 50 U.S.C. §§ 1873(b)(6) and 1873(b)(6)(A).

The estimated number of Call Detail Records received from providers. This metric represents the number of *records received* from the provider(s) and stored in NSA repositories (records that fail at any of a variety of validation steps are not included in this number). CDRs covered by § 501(b)(2)(C) include call detail records created before, on, or after the date of the application relating to an authorized investigation. While the USA FREEDOM Act directs the government to provide a good faith estimate of "the number of unique identifiers used to communicate information collected pursuant to" orders issued in response to CDR applications (*see* 50 U.S.C. § 1873(b)(5)(B)), the statistic below does *not* reflect the number of unique identifiers contained within the call detail records received from the providers. As of the date of this report, the government does not have the technical ability to isolate the number of unique identifiers within records received from the providers. As explained in the 2016 NSA public report on the USA FREEDOM Act, the metric provided is over-inclusive because the government counts each record *separately even if the government receives the same record multiple times* (whether from one provider or multiple providers). Additionally, this metric includes duplicates of unique identifiers – i.e., because the government lacks the technical ability to isolate unique identifiers, the statistic counts the number of records even if unique identifiers are repeated. For example, if one unique identifier is associated with multiple calls to a second unique identifier, it will be counted multiple times. Similarly, if two different providers submit records showing the same two unique identifiers in contact, then those would also be counted. This statistic includes records that were received from the providers in CY2017 for all orders active for any portion of the year, which includes orders that the FISC approved in 2016. Furthermore, while the records are received from domestic communications service providers, the records received are for domestic and foreign numbers. More information on how NSA implements this authority can be found in the DCLPO report, in particular *see* page 5 for a description and illustration of the USA FREEDOM Implementation Architecture.

Figure 18: Illustration of a hop scenario and counting



Target uses Phone A which is the FISC-approved selector in the FISC order. This would count as **1 order, 1 target**, **7 unique identifiers** (phones A, B, C, D, E, F, G) and, assuming 500 calls between parties, **6000 CDRs** (*produced for both sides of a call event).

Assume an NSA intelligence analyst learns that phone number (**Phone A**) is being used by a suspected international terrorist (target). **Phone A** is the "specific selection term" or "selector" that will be submitted to the FISC (or the Attorney General in an emergency) for approval using the "reasonable articulable suspicion" (RAS) standard. Assume that one provider (provider X) submits a record showing **Phone A** called unique identifier **Phone B** – what is referred to as a "call event." This is the **"first hop."** In turn, assume that NSA submits the "first-hop" Phone B to the provider X, and finds that unique identifier was used to call another unique identifier **Phone D**. This is the **"second-hop."** If the unique identifiers call one another multiple times, then multiple CDRs are produced and duplication occurs. Additionally, the government may receive multiple CDRs for a single call event. NSA may also submit the specific selection Phone A number to another provider (provider Y) who may have CDRs of the same call events.

Not all CDRs provided to the government will be domestic numbers. The targeted "specific selection term" could be a foreign number, could have called a foreign number or the "first-

hop" number could have called a foreign number; thus, these CDRs statistics contain both domestic and foreign number results.

Figure 19: Table of CDRs Received Arising from Such Targets

Call Detail Records "CDRs" – Section 501(b)(2)(C)	CY2016	CY2017
Estimated number of call detail records arising from such targets that NSA received from providers pursuant to Section 501(b)(2)(C) and stored in its repositories*	151,230,968	**534,396,285**

* While the statute directs the government to count the unique identifiers, the government is not technically able to isolate the number of unique identifiers; thus, this number includes duplicate records. Additionally, the number of records contains both domestic and foreign numbers.

D. Statistics – Call Detail Record Queries

The number of search terms associated with a U.S. person used to query the CDR data. Each unique query is counted only once. The same term queried 10 times counts as one query term. A single query with 20 terms counts as 20 query terms.

Figure 20: Table of CDRs -- U.S. person query terms

Call Detail Records "CDRs" – Section 501(b)(2)(C)	CY2016	CY2017
Estimated number of search terms that included information concerning a U.S. person that were used to query any database of call detail records obtained through the use of such orders*	22,360	**31,196**

See 50 U.S.C. § 1873(b)(6)(C).

* Consistent with § 1873(d)(2)(A), this statistic does not include queries that are conducted by the FBI.

National Security Letters (NSLs)

A. National Security Letters

In addition to statistics relating to FISA authorities, we are reporting information on the government's use of National Security Letters (NSLs). The FBI is statutorily authorized to issue NSLs for specific records (as specified below) only if the information being sought is relevant to a national security investigation. NSLs may be issued for four commonly used types of records:

National Security Letters

→ *Not authorized by FISA but by other statutes.*

→ *Bulk collection is prohibited, however, by the USA FREEDOM Act.*

→ *FBI may only use NSLs if the information sought is relevant to international counterterrorism or counterintelligence investigation.*

1) telephone subscriber information, toll records, and other electronic communication transactional records, see 18 U.S.C. § 2709;
2) consumer-identifying information possessed by consumer reporting agencies (names, addresses, places of employment, institutions at which a consumer has maintained an account), see 15 U.S.C. § 1681u;
3) full credit reports, see 15 U.S.C. § 1681v (only for counterterrorism, not for counterintelligence investigations); and
4) financial records, see 12 U.S.C. § 3414.

B. Statistics – National Security Letters and Requests of Information

Counting NSLs. Today we are reporting (1) the total number of NSLs *issued* for all persons, and (2) the total number of requests for information (ROI) contained within those NSLs. When a single NSL contains multiple ROIs, each is considered a "request" and each request must be relevant to the same pending investigation. For example, if the government issued one NSL seeking subscriber information from one provider and that NSL identified three e-mail addresses for the provider to return records, this would count as one NSL issued and three ROIs.

- **The Department of Justice's Report on NSLs.** In May 2018, the Department of Justice released its *Annual Foreign Intelligence Surveillance Act Report* to Congress. That report, which is available online, provides the *number of requests* made for certain information concerning different U.S. persons pursuant to NSL authorities during calendar year 2017. The Department of Justice's report provides the number of individuals subject to an NSL whereas the ODNI's report provides the number of NSLs issued. Because one person may be subject to more than one NSL in an annual period, the number of NSLs issued and the number of persons subject to an NSL differs.

Why we report the number of NSL requests instead of the number of NSL targets. We are reporting the annual number of requests for multiple reasons. First, the FBI's systems are configured to comply with Congressional reporting requirements, which do not require the FBI to track the number of individuals or organizations that are the subject of an NSL. Even if the FBI systems were configured differently, it would still be difficult to identify the number of specific individuals or organizations that are the subjects of NSLs. One reason for this is that the subscriber information returned to the FBI in response to an NSL may identify, for example, one subscriber for three accounts or it may identify different subscribers for each account. In some cases this occurs because the identification information provided by the subscriber to the provider may not be true. For example, a subscriber may use a fictitious name or alias when creating the account. Thus, in many instances, the FBI never identifies the actual subscriber of a facility. In other cases, this occurs because individual subscribers may identify themselves differently for each account (e.g., inclusion of middle name, middle initial, etc.) when creating an account.

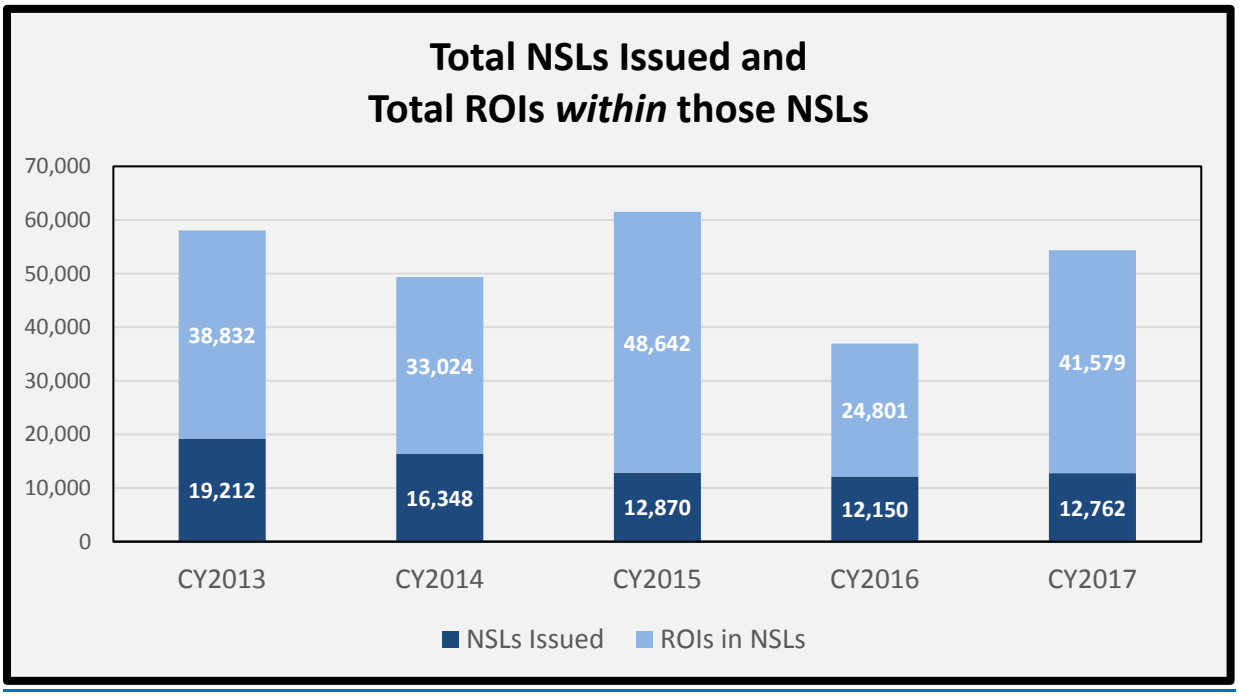
We also note that the actual number of individuals or organizations that are the subject of an NSL is different than the number of NSL requests. The FBI often issues NSLs under different legal authorities, e.g., 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709, for the same individual or organization. The FBI may also serve multiple NSLs for an individual for multiple facilities (e.g., multiple e-mail accounts, landline telephone numbers and cellular phone numbers). The number of requests, consequently, is significantly larger than the number of individuals or organizations that are the subjects of the NSLs.

Figure 21a: Table of NSLs Issued and Requests for Information

National Security Letters (NSLs)	CY2013	CY2014	CY2015	CY2016	CY2017
Total number of NSLs issued	19,212	16,348	12,870	12,150	**12,762**
Number of Requests for Information (ROI)	38,832	33,024	48,642	24,801	**41,579**

See 50 U.S.C. § 1873(b)(6).

Figure 21b: Chart of NSLs Issued and Requests for Information



APPENDIX

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

MAY 0 4 2018

The Honorable Richard Burr
Chairman
Select Committee on Intelligence
United States Senate

The Honorable Chuck Grassley
Chairman
Committee on the Judiciary
United States Senate

The Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence
U.S. House of Representatives

The Honorable Robert W. Goodlatte
Chairman
Committee on the Judiciary
U.S. House of Representatives

Dear Messrs. Chairmen:

Section 603(b)(2)(B) of the Foreign Intelligence Surveillance Act (FISA), as amended by the *Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, (P.L.114-23), 129 Stat. 268 (hereinafter USA FREEDOM Act), requires the Director of National Intelligence (DNI) to make publicly available for the preceding 12-month period a good faith estimate of the number of queries concerning a known United States person of unminimized non-content information relating to electronic communications or wire communications obtained through acquisitions authorized under Section 702 of FISA, excluding the number of queries containing information used to prevent the return of information concerning a United States person.

If the DNI concludes that this good faith estimate cannot be determined accurately because not all of the relevant elements of the Intelligence Community (IC) are able to provide this good faith estimate, then FISA requires him to (i) certify that conclusion in writing to the committees identified above; (ii) report the good faith estimate for those relevant elements able to provide such good faith estimate; (iii) explain when it is reasonably anticipated that such an estimate will be able to be determined fully and accurately; and (iv) make such certification publicly available on an Internet website.

I conclude that the good faith estimate required under section 603(b)(2)(B) of FISA cannot be determined accurately because not all of the relevant elements of the IC are able to provide this good faith estimate. Specifically, the Central Intelligence Agency (CIA) remained unable to provide such information for calendar year 2017. The enclosed report includes the good faith estimate for those relevant IC elements that were able to provide such good faith estimate. Based on the information provided to me by the CIA, I reasonably anticipate that such an estimate will be able to be determined fully and accurately by the end of calendar year 2018 so as to be included in the 2019 report.

The Honorable Richard Burr
The Honorable Chuck Grassley
The Honorable Devin Nunes
The Honorable Robert W. Goodlatte

If you have any questions regarding this matter, please contact the Office of the Director of National Intelligence Office of Legislative Affairs at (703) 275-2474.

Sincerely,



Daniel R. Coats

Enclosure:
Statistical Transparency Report

cc: Executive Secretary, National Security Staff
Director, Central Intelligence Agency
Under Secretary of Defense for Intelligence
Under Secretary for Intelligence and Analysis, Department of Homeland Security
Director, National Security Agency
Director, National Reconnaissance Office
Director, Defense Intelligence Agency
Director, National Geospatial-Intelligence Agency
Assistant Secretary for Intelligence and Research, Department of State
Assistant Secretary for Intelligence and Analysis, Department of the Treasury
Executive Assistance Director, Intelligence Branch, Federal Bureau of Investigation
Chief of Intelligence, Senior Officer, Drug Enforcement Administration
Director, Office of Intelligence and Counterintelligence, Department of Energy
Deputy Chief of Staff, G2, U.S. Army
Director of Intelligence, U.S. Marine Corps
Director of Naval Intelligence, N2 U.S. Navy
Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance, A2, U.S. Air Force
Deputy Chief of Staff for Intelligence and Criminal Investigations, U.S. Coast Guard
Assistant Attorney General for National Security, Department of Justice

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

Plaintiff's Exhibit 21

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.





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

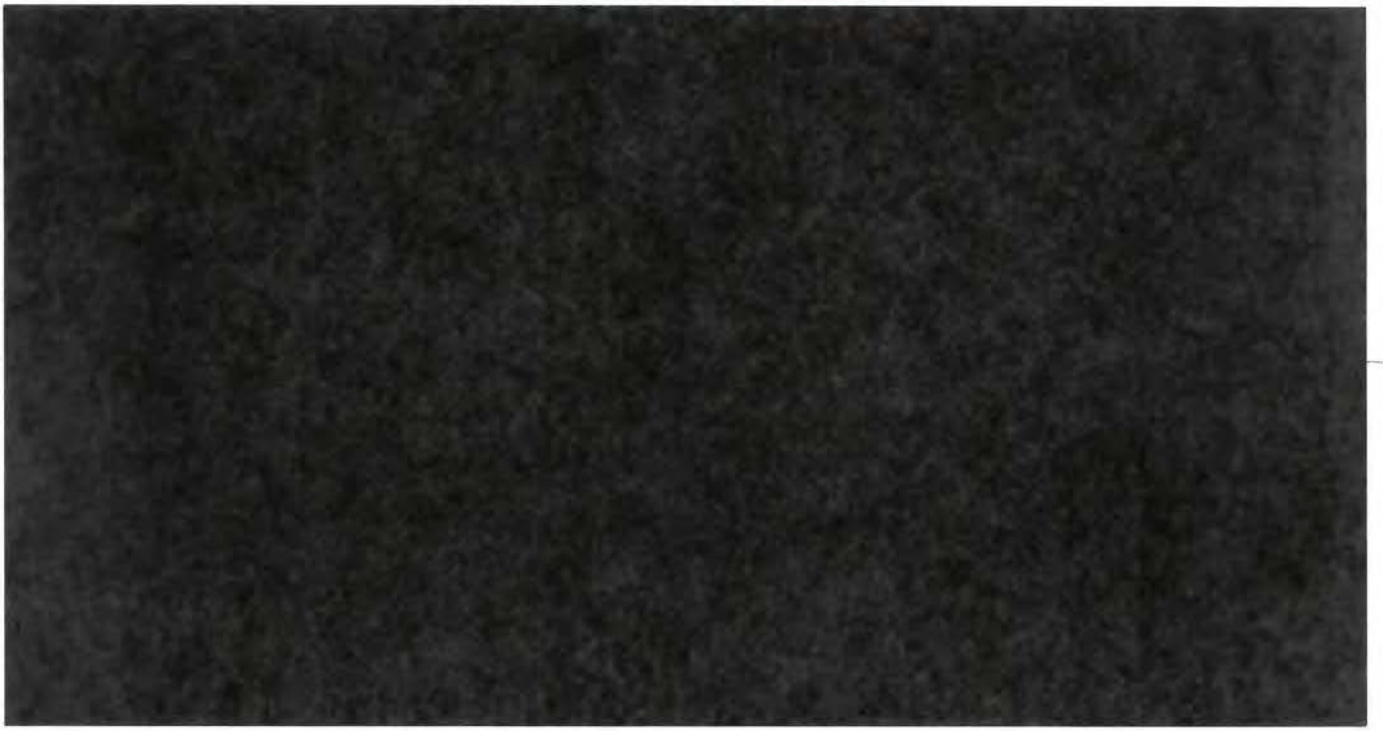
"promptly" if it "uses this provision to respond to such congressional oversight inquiries." September 26, 2016 Memorandum at 7.[47]

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

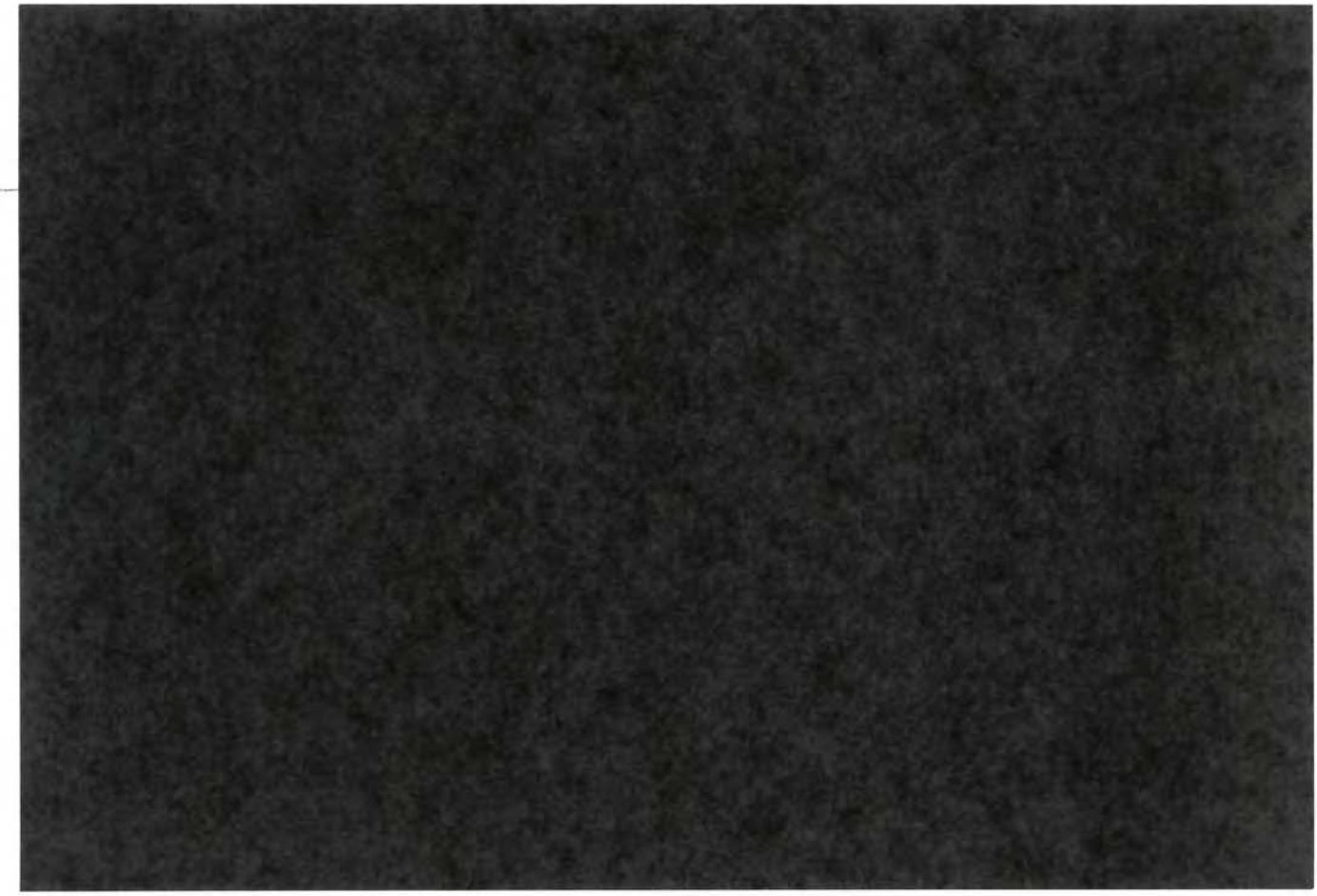
Last year, in the context of approving the standard minimization procedures employed by the FBI for electronic surveillance and physical search conducted under Titles I and III of FISA, a judge of the FISC observed:

> 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]



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.

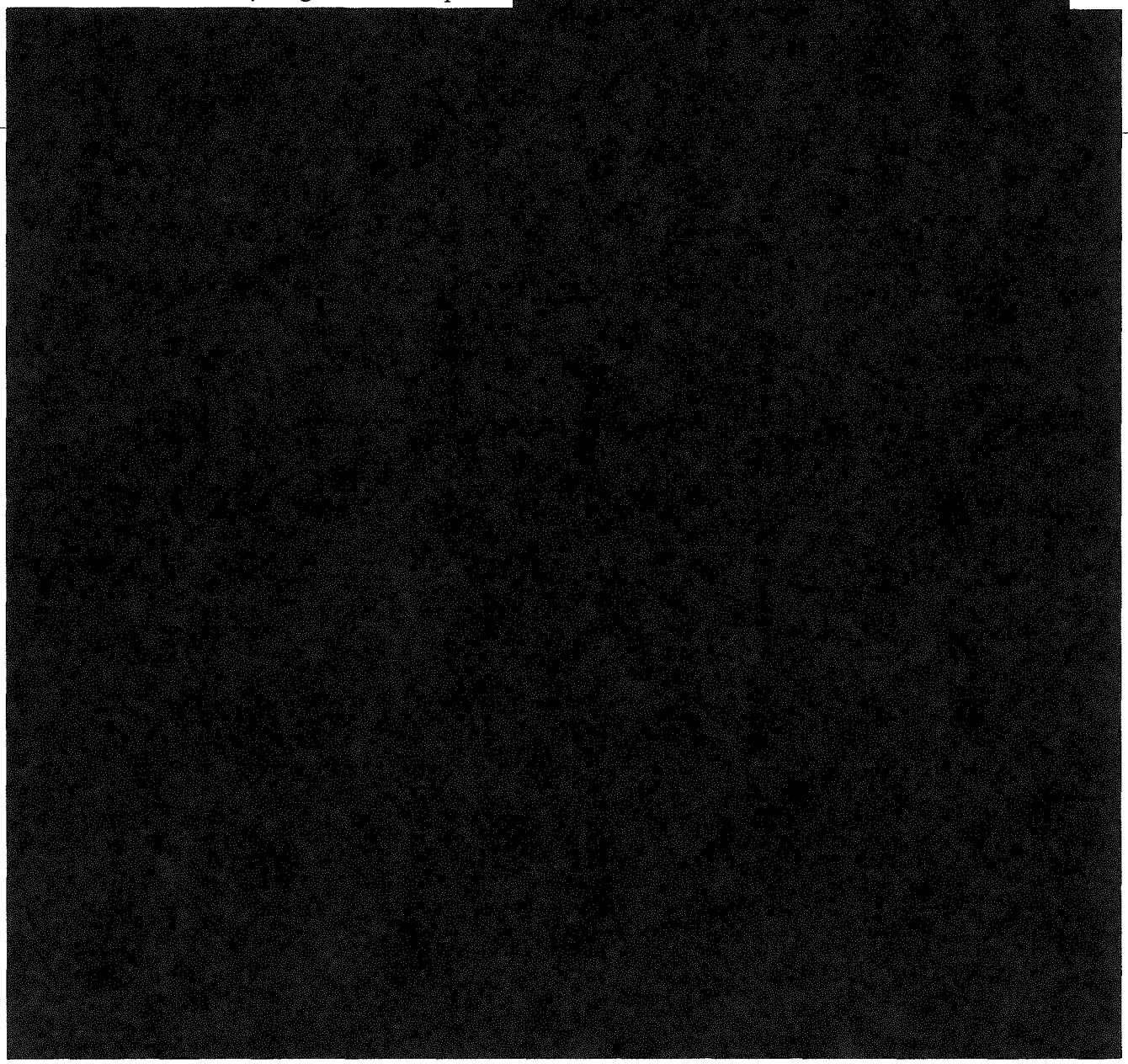
[redacted] targets who have been subject to criminal charges [redacted] there was a delay of over two years in establishing review teams. See [redacted] Preliminary Notice of Compliance Incident Regarding [redacted] Section 702-Tasked Facilities ("[redacted] Preliminary Notice") at 2-3. The primary cause 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] 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.

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

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].

[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]