“Institutional Lack of Candor”

A primer on recent unauthorized activity by the Intelligence Community

About Demand Progress
Demand Progress is a national grassroots group with two million affiliated activists who fight for basic rights and freedoms needed for a modern democracy.

Contact information:
Daniel Schuman, policy director, daniel@demandprogress.org
Sean Vitka, counsel, sean@demandprogress.org

EXECUTIVE SUMMARY

At multiple junctures, the FISA Court (FISC) has identified serious compliance problems with Section 702 of FISA, often based on the government's repeated inability to follow basic rules that are supposed to protect Americans. Even when the government and its lawyers have promised to fix these problems, a wide variety of violations have persisted, including unauthorized collection of Americans' communications, prohibited queries using Americans' identifiers, and unlawful sharing of this highly sensitive information.

Fourth Amendment and FISA Violations (p. 2-4)
The FISC has twice found that certain Section 702 collection violated the Fourth Amendment. In 2011 the government revealed that as part of its "upstream" Section 702 collection it collected non-targeted, entirely domestic communications. When NSA violated the rules that were supposed to make this collection legal, FISC again deemed the practice "a very serious Fourth Amendment issue."

For almost 12 years, both under Section 702 and other programs before it, NSA was always engaging in or retaining some kind of electronic surveillance the FISC would go on to deem unauthorized, and NSA would only fix the problem when threatened with criminal sanctions.

Minimization Violations: Prohibited Upstream Searches (p. 4)
To prevent constitutional and legal violations, the FISC imposes rules to make sure the NSA does not collect and access entirely domestic communications. For years, the NSA violated one of these rules, which prohibited queries on data collected via upstream collection known to include entirely domestic communications.

Breached Attorney-Client Privilege (p. 5)
FBI's minimization procedures require it to sequester Attorney-Client communications collected under Section 702 pertaining to a matter for which someone has been indicted. In recent years, the FBI has admitted a number of violations of this requirement.

Noncompliant Data Repositories (p. 5-6)
Another persistent problem involves agency dissemination of data to repositories that don't meet the security and authorization terms mandated by minimization procedures. FBI has formally notified the FISC of several such violations, storing Title I, Title III, and Section 702 data in repositories without the required minimization markings, or ability to track queries or log access, posing a risk that the data might be searched by unauthorized users or for unauthorized purposes, and providing data to users not authorized to access it.

Delayed Reporting of Violations to the FISC (p. 6-8)
The FISC has no independent means to verify compliance and so must rely on the government to self-report any violations. The government claims it informs the FISC of violations in a timely fashion. But judges have repeatedly complained about delays in notice of violations and other key information, in one 2017 opinion accusing the government of ''an institutional 'lack of candor.'"

Failure to Give Notice to Individuals in Criminal Cases and Other Legal Proceedings (p. 8)
After misleading the Supreme Court, the Department of Justice issued a handful of notices to defendants who had been prosecuted based in part on Section 702 information. Some of the defendants received notice only years after their trials had concluded. In recent years, Section 702 notices have again disappeared.

Primer on recent unauthorized activity by the Intelligence Community

At multiple junctures, the FISA Court (FISC) has identified serious constitutional and statutory problems with Section 702 of FISA, often based on the government's repeated inability to follow the basic rules that are supposed to protect Americans. Even when the government and its lawyers have promised to fix these problems, a wide variety of violations have persisted, including unlawful collection of Americans' communications, unlawful queries using Americans' identifiers, and unlawful sharing of this highly sensitive information.

Fourth Amendment Violations

On at least two occasions, the FISC has found that certain Section 702 collection violated the Fourth Amendment.

The first of those came in 2011 after the government revealed that as part of its "upstream" surveillance under Section 702 it was collecting bundled communications (what it calls multiple communication transactions or MCTs). This resulted in the collection of non-targeted, entirely domestic communications. This unauthorized collection continued for more than three years before the FISC was informed. After reviewing the government's plan for MCTs, Judge John Bates explained that "[u]nder 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."[1] By the time the government agreed to address the problems with upstream collection, it had been seizing and searching Americans' private domestic communications for four years.

The government failed to keep those promises, and for over five more years, the government conducted queries on upstream collection in violation of procedures Judge Bates approved in response to the 2011 disclosures. After the new violations were revealed in late 2016, FISC Judge Rosemary Collyer called those queries "a very serious Fourth Amendment issue," and she later scolded the government for "the extent of non-compliance with 'important safeguards for interests protected by the Fourth Amendment.'"[2]

Unauthorized Electronic Surveillance and Persistent Overcollection

For almost 12 years, both under Section 702 and other programs before it, NSA was always engaging in or retaining some kind of electronic surveillance the FISC would go on to deem unauthorized, and NSA would only fix the problem when threatened with criminal sanctions.

---

[1] See October 3, 2011 John Bates opinion at 78-79. Available at https://www.aclu.org/foia-document/october-3-2011-john-bates-fisc-opinion.
[2] See April 26, 2017 Rosemary Collyer opinion at 19 and 22. Available at https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

The FISC has made clear the seriousness of multiple violations by telling the government that it may be breaking the law. Starting in 2010, the Court started leveraging 50 U.S.C. § 1809(a)(2) of FISA, which is a criminal prohibition on the use or disclosure of any information obtained, "knowing or having reason to know," that the data came from electronic surveillance not authorized by FISA. On at least five occasions, detailed below, judges have warned the government that if they used data collected in violation of minimization procedures (such as in another FISA application), they might be found in violation of 1809(a)(2). By 2015, the FISC had deemed NSA collection or retention spanning from 2004 to 2015 to be potential violations of 1809(2)(a). Some of that data was not purged until 2016.

In that time, the FISC deemed the following practices to be possible violations of 1809(a)(2):

- From 2004 until 2009, in spite of twice quarterly Office of General Counsel spot checks imposed to prevent it, "'[v]irtually every PR/TT record' generated [by the bulk Internet metadata program] included some data that had not been authorized for collection."[3]
- From 2007 until 2011, NSA collected entirely domestic and untargeted communications as part of Multiple Communication Transaction bundles without restricting access to the unrelated communications.[4]
- In June 2010, NSA admitted it had improperly retained Title I data in a management system that the court had deemed an overcollection; in May 2011, FISC found this retention problematic under 1809(a)(2).[5] The government even argued that prohibitions on using unlawfully collected information "only applied to interceptions authorized by the Court and did not apply to the fruits of unlawful surveillance."[6]

---

[3] See [caption and date redacted] John Bates opinion at 21. Available at https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf. Though the date is redacted, the opinion dates to some time in July 2010. Footnote 78 cites the Supreme Court decision in *Holder v. Humanitarian Law Project*, released on June 21, 2010, using a Westlaw citation, suggesting the opinion must date to before July 23, when the Supreme Court citation became available. A May 25, 2011 NSA Inspector General Report confirms the date as July 2010. https://www.documentcloud.org/documents/2271057-savage-nyt-foia-nsa-ig-fisa-br-reports.html#document/p211/a234924 FISC authorized the PRTT dragnet on July 14, 2004. See NSA IG Report at 39. https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf. After disclosure of the problems, the NSA and FISC halted collection in the first quarter of FY 2010, between October 1 and December 31, 2009. See Intelligence Oversight Board Report, March 15, 2010 5-6. https://www.nsa.gov/news-features/declassified-documents/intelligence-oversight-board/assets/files/FY2010_1Q_IOB_Report.pdf.

[4] See October 3, 2011 Bates opinion fn 15 at 17. https://www.aclu.org/foia-document/october-3-2011-john-bates-fisc-opinion. See also October 13, 2011 Bates order fn 1 at 2. Available at https://assets.documentcloud.org/documents/3865017/Eff-16-Cv-02041hsg-Doc-17-06-13-17-Redacted.pdf

[5] See November 6, 2015 Thomas Hogan opinion at 57. Available at https://www.aclu.org/foia-document/fisc-memorandum-opinion-and-order-re-section-702.

[6] See November 6, 2015 Thomas Hogan opinion at 56.

- From 2011 to 2016, NSA retained Section 702 overcollection in its management systems, in spite of the 2011 FISC retention precedent ruling such retention a violation of 1809(a)(2).[7]
- In 2013, NSA discovered its post-tasking checks to ensure targeted phones had not roamed into the United States had not functioned properly for some redacted period of time (possibly dating back to 2008), meaning some of the telephone collection from that period may have been collected on individuals located inside the United States in violation of 702.[8]

Other Minimization Violations: Prohibited Upstream Searches

Three other recurring minimization procedure violations present persistent privacy concerns with 702.

The first — which is the Fourth Amendment violation criticized by Judge Collyer above — involves searching for Americans' identifiers in upstream collection. Because upstream collection foreseeably results in the collection of domestic communications, when John Bates first permitted searches of 702 data using US person identifiers in late 2011, he prohibited such searches on upstream data, for fear it would amount to using 702 for domestic surveillance. Yet NSA starting disclosing "many" such violations as early as 2013.[9]

As NSA's compliance organizations started looking more closely in 2015 and 2016, they discovered the NSA was even conducting such searches in systems "that do not interface with NSA's query audit system,"[10] raising questions about their ability to oversee US person queries more generally. NSA discovered that some data obtained using upstream collection had been mislabeled as PRISM collection, meaning it would get no special treatment.[11] With one tool used to conduct queries of Americans located overseas, NSA experienced an 85% noncompliance rate.[12]

When faced with these kinds of difficulties tracking down all the upstream searches that had taken place, NSA chose instead to curtail one practice — "about" collection — that made it more likely upstream queries would search on entirely domestic communications.[13] Despite this change, upstream collection will continue to collect some entirely domestic communications.

---

[7] See Hogan, November 6, 2015 at 57-58. The April 26, 2017 Collyer opinion at 72 reports that as of February 17, 2016 this data had been purged from NSA's systems.
[8] See August 30, 2013 Reggie Walton opinion fn 7 at 11. Available at https://www.documentcloud.org/documents/3865005-Eff-16-Cv-02041hsg-Doc-03-06-13-17-Redacted.html.
[9] See October 2014 Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act at 33. Available at https://www.emptywheel.net/wp-content/uploads/2016/07/2014-October-Semiannual-2013-2013.pdf.
[10] See April 26, 2017 Collyer opinion at 21.
[11] See April 26, 2017 Collyer opinion at 22.
[12] See April 26, 2017 Collyer opinion at 82.
[13] See April 26, 2017 Collyer opinion at 27.

Other Minimization Violations: Breached Attorney-Client Privilege

Another persistent violation involves FBI's failure to abide by its own minimization procedures requiring that the communications for targets who have been federally indicted be reviewed and, if pertaining to the charged matter, sequestered.[14] This means that agents may have access to attorney-client communications collected using Section 702 at the same time the government is criminally prosecuting the target of the surveillance. In addition, there are at least two documented examples of US person-investigations in which FISA was used where attorney-client communications not involving the specific charge were collected.[15]

Other Minimization Violations: Noncompliant Data Repositories

Another persistent problem involves the dissemination of data to repositories that don't meet the security and authorization terms mandated by minimization procedures. In 2013, the FBI reported it had put Title I and III data in repositories without the required minimization markings, or ability to track queries or log access, posing a risk that the data might be searched by unauthorized users or for unauthorized purposes; later that year, it admitted Section 702 data had been treated similarly.[16] That violation resulted in the addition of language in FBI's minimization procedures permitting the use of "ad hoc" databases for FBI investigations, with new restrictions.

---

[14] A July 30, 2014 letter at 5-6 to Judge Reggie Walton reflected notices in February and April, both pertaining to multiple accounts. Available at https://www.dni.gov/files/documents/0928/Letter%20to%20Judge%20Hogan%2030%20July%202014.pdf. The August 26, 2014 Thomas Hogan opinion at 35-36 described "more recent cases" reported in an August hearing. Available at https://www.aclu.org/foia-document/fisc-opinion-and-order-re-702. The November 6, 2015 Thomas Hogan opinion describes reports in all four interim quarterly reports, plus three more preliminary notices submitted after the most recent quarterly report. Fn 38 at 49. The April 26, 2017 Rosemary Collyer opinion describes at least one more individual preliminary notice at 90, an extended discussion on "under-inclusiveness" of the review that is almost entirely redacted at 91-92, as well as another problem identified on November 28 to 30, 2016 at 92-93.

[15] The two US persons are Reaz Qadir Khan and Bakhtiyor Jumaev. For Khan see Memorandum in Support of Motion for Disclosure of Monitoring of Privileged Communications, Minimization Procedures & Filter Team Protocol, available at http://www.emptywheel.net/wp-content/uploads/2014/09/140428-Attorney-Client.pdf and Supplemental Exhibit to Disclosure Motion, available at http://www.emptywheel.net/wp-content/uploads/2014/09/140529-Notice-of-Nelson-Contacts.pdf, also available at OR 3:12-cr-00659. For Jumaev see Defendant Jumaev's Motion Requiring the Government to Provide Notice of Interceptions and/or Surveillance of His Defense Counsel and Members of His Defense Team at 16, available at https://www.emptywheel.net/wp-content/uploads/2014/10/141020-Atty-Client-Spyin.pdf, also available at CO 1:12-cr-00033.

[16] See December 13, 2013 Reggie Walton opinion at 22-25. Available at https://www.documentcloud.org/documents/3865000-Eff-16-Cv-02041hsg-Doc-15-06-13-17-Redacted.html.

Yet even with that provision, FBI had two incidents in recent years where the FBI shared data outside of approved recipients; FBI approved one of those with a Memorandum of Understanding, which Judge Collyer noted made the violation "the result of deliberate decisionmaking … presumably prepared or reviewed by FBI lawyers."[17] Also in 2015, FBI discovered it had made 702 data available to FBI employees who were not cleared to access it.[18]

NSA, too, may have problems with tracking repositories. After proposing to end "about" collection in 2017, it agreed to sequester and destroy only that "about" collection stored in "institutionally managed repositor[ies]," a term Judge Collyer did not recognize but nevertheless did not require the government to define.[19] That suggests that some of the data is in repositories the NSA does not manage. Additionally, in March 2017, five months after NSA first reported the gravity of the upstream problems it had rediscovered, it still was "attempting to identify all systems that store upstream data," which raises questions about NSA's ability to ensure such systems meet 702's heightened standards or even that it can destroy that "about"-collected data.[20]

Delayed Reporting of Violations to the FISC

Although it has ordered Inspector General reports, the FISC has no independent means to verify compliance, and so must rely on the government to self-report any violations. The government claims it informs the FISC of violations in timely fashion. But judges have repeatedly complained about delays in notice of violations and other key information. For example,

- Even before the FISA Amendments Act, the government withheld critical information from the FISC. When the government reorganized how it would conduct PRISM in early 2008 after already having submitted certifications in Yahoo's challenge,[21] for example, it didn't inform the Honorable Reggie Walton, who presided over that challenge. "[T]he government then inexplicably modified and added to those certifications and procedures without appropriately informing the Court or supplementing the record in this matter until ordered to do so."[22]

---

[17] The April 26, 2017 Collyer opinion at 83-87 describes two examples of FBI sharing raw FISA data with contractors, one of which occurred under an interagency Memorandum of Understanding (which therefore makes it a willful violation). Available at https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.
[18] See April 26, 2017 Collyer opinion at 69.
[19] See April 26, 2017 Collyer opinion fn 25 at 24.
[20] See April 26, 2017 Collyer opinion at 22.
[21] Documents pertaining to Yahoo's Protect America Act challenge are available at https://cdt.org/insight/yahoo-v-u-s-prism-documents/.
[22] See April 25, 2008 Reggie Walton opinion at 3-4. Avaialble at https://cdt.org/files/2014/09/38-yahoo702-memorandum-opinion-unredacted.pdf.

- Then, in September 2008, almost immediately after the first 702 certification was approved, NSA had an overcollection violation. It took almost three months before the government informed the court.[23]

- In 2009, "the Court learned that the government's practice has been to report only certain compliance incidents to the Court: those that involve systemic or process issues, those that involve conduct contrary to a specific representation made to the Court, and those that involve the improper targeting of U.S. persons under circumstances in which the analyst knew or should have known that the individual was a U.S. person."[24] As a result, common violations — such as of roamer collection inside the US — did not get noticed to the Court.

- In 2011, the government revealed for the first time that for the entirety of the time it had used "upstream collection" (which first started in May 2007 under a Title I docket) it had been collecting MCTs that might contain entirely domestic unrelated communications.[25] As John Bates noted, following delayed disclosures of problems with the phone and Internet metadata programs, the upstream violation disclosure marked "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."[26] Judge Bates later complained that the government "argued that previous and ongoing collections of [such communications] were in compliance with the Court's orders...despite the fact that the government acknowledged it did not fully inform the Court of this aspect of the collection prior to May 2, 2011."[27]

- In a 2017 opinion describing a number of violations, Judge Collyer repeatedly referred to unacceptable delays in providing notice to Congress. Describing violations identified at

---

[23] See April 19, 2009 Mary McClaughlin opinion, fn 1 at 3, describing presiding judge Colleen Kollar-Kotelly asking why it took nearly three months to disclose to the court. Available at https://www.documentcloud.org/documents/3864999-Eff-16-Cv-02041hsg-Doc-14-06-13-17-Redacted.html.

[24] See 2009 [date redacted] Thomas Hogan opinion, 12-13, describing that the government had not informed the court about roamer detaskings. Available at https://www.documentcloud.org/documents/3865008-Eff-16-Cv-02041hsg-Doc-11-06-13-17-Redacted.html.

[25] Colleen Kollar-Kotelly's January 15, 2008 order at 17-22 describes her authorization of about collection under Protect America Act. Available at https://cdt.org/files/2014/09/49-yahoo702-memorandum-opinion-and-order-dni-ag-certification.pdf. Government's Response to Court's Order of October 11, 2007 at 34 reveals that the May 31, 2007 Primary Order first authorized "about" collection; available at same URL. The May 31, 2007 Roger Vinson order first authorizing about collection is available at https://www.aclu.org/foia-document/may-31-2007-fisc-vinson-order.

[26] See October 3, 2011 Bates opinion at fn 14 at 16. https://www.aclu.org/foia-document/october-3-2011-john-bates-fisc-opinion.

[27] See October 13, 2011 John Bates order at 3. Available at https://assets.documentcloud.org/documents/3865017/Eff-16-Cv-02041hsg-Doc-17-06-13-17-Redacted.pdf.

> least as early as January but not fully disclosed in early October reporting, Collyer accused the government of ''an institutional 'lack of candor.'" In the same opinion, she scoffed at the government's excuses for different eleven and five month delays in notifying the FISC of violations. "Too often, however, the government fails to meet its obligation to provide prompt notification to the FISC when noncompliance is discovered." [28]

Failure to Notify Defendants of Information "Derived from" Section 702 Collection and Misrepresentations Before the Supreme Court

When Congress passed the FISA Amendments Act in 2008, it required the government to follow the same notice provisions as used under traditional FISA. If prosecutors want to use "any information obtained or derived from" Section 702 in a trial, they must tell the defendant.[29] Yet when the government pointed to attacks prevented using Section 702 in the wake of the Edward Snowden leaks, defendants in those cases had not received the required notice. For example, the defendant in the most celebrated case involving an attack thwarted using Section 702, Najibullah Zazi, did not receive notice until July 2015, over five years after he pled guilty.[30]

The government only started giving such notices after it emerged that Solicitor General Don Verrilli falsely informed the Supreme Court that such defendants get notice,[31] when in fact DOJ had a policy that ensured no defendant received notice of Section 702 surveillance for nearly five years. Although this surveillance was subsequently disclosed in a small number of cases, notice to defendants appears to have dried up again.[32]

Based on available information, there are only eight total cases over the past decade in which defendants have received the notice required by law.[33] Only defendants in terrorism cases have gotten notice, in spite of Section 702's likely use in spying and proliferation cases.

---

[28] See Collyer April 26, 2017 opinion at 19, 68 fn 57.
[29] The notice requirement under FAA comes from 18 U.S.C. § 1881e, which cites back to 18 U.S.C. §1806. That notice requirement is available at https://www.law.cornell.edu/uscode/text/50/1806.
[30] Notice letter available at https://ia601409.us.archive.org/7/items/gov.uscourts.nyed.296434/gov.uscourts.nyed.296434.59.0.pdf.
[31] See October 29, 2012 Supreme Court transcript in Clapper v Amnesty Internaional at https://web.archive.org/web/20170619031300/https://www.supremecourt.gov/oral_arguments/argument_transcripts/11-1025.pdf; see also Adam Liptak, "A Secret Surveillance Program Proves Challengeable in Theory Only", July 15, 2013, N.Y. Times, available at http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html.
[32] See Patrick Toomey, "Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?", December 11, 2015, Just Security, available at https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again.
[33] Defendants have received 702 notice in United States v. Muhtorov, No. 12-cr-00033 (D. Colo.), United States v. Mohamud, No. 10-cr-00475 (D. Or.), United States v. Hasbajrami, No. 11-cr-00623 (E.D.N.Y.), United States v. Khan, No. 12-cr-00659 (D. Or.), United States v. Mihalik, No. 11-cr-0833 (S.D. Cal.), United States v. Zazi, No. 09-cr-663 (E.D.N.Y.), United States v. Mohammad, No. 15-cr-358 (N.D. Ohio), and United States v. Al-Jayab, No. 16-cr-00181 (N.D. Ill.).

About Demand Progress
Demand Progress is a national grassroots group with two million affiliated activists who fight for basic rights and freedoms needed for a modern democracy.

Contact information:
Daniel Schuman, policy director, daniel@demandprogress.org
Sean Vitka, counsel, sean@demandprogress.org
Author: Marcy Wheeler