ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

May 10, 2016

The Honorable Charles Grassley
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

The Honorable Patrick Leahy
Senate Committee on the Judiciary
152 Dirksen Senate Office Building
Washington, D.C. 20510-6050

Dear Chair Grassley and Ranking Member Leahy:

We submit this letter for the record in connection with the Senate Judiciary Committee's hearing on May 10, 2016 titled "Oversight and Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy, and Civil Liberties."

The Electronic Frontier Foundation (EFF) has strongly opposed Section 702 of the Foreign Intelligence Surveillance Act ("Section 702") since its enactment because the statute is used to conduct unconstitutional and warrantless surveillance.

The Judiciary Committee is uniquely positioned to foster a much-needed national conversation on surveillance conducted under the statute. Key questions about the government's use of Section 702 remain unanswered despite the declassification of documents and helpful reporting by the Privacy and Civil Liberties Oversight Board.[1] For instance, the public still does not know the number of Americans' communications or the number of innocent foreigners' communications collected under the statute. The public does not know the procedures used by the Department of Justice to notify criminal defendants that Section 702-derived information was used in a prosecution. And the public does not know how often the FBI searches Section 702 data for non-national security purposes. These questions must be publicly answered well before Section 702's expiration in December 2017.

Given what *is* known about Section 702's invasive surveillance, we urge the Committee to, at minimum:

1) Limit the Scope of Surveillance or Stop It Entirely
2) Require the Government to Submit Surveillance Targets for Judicial Review
3) Prohibit Backdoor Searches
4) Mandate Transparency and Oversight

Limit the Scope of Surveillance or Stop It Entirely

The government relies on Section 702 to perform at least two types of surveillance: PRISM and "upstream" collection.[2] An October 3, 2011 Foreign Intelligence Surveillance Court

[1] See, https://www.pclob.gov/library/702-Report.pdf and icontherecord.tumblr.com ("PCLOB 702 Report").
[2] As the Privacy and Civil Liberties Oversight Board notes: "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. The National Security Agency ("NSA") receives all data collected through PRISM. In addition, the

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

(FISC) order ("Bates Opinion") revealed the programs store more than 250 million communications annually in NSA repositories.[3] Since the law's passage in 2008, surveillance at this rate would account for the collection of over 1.5 billion Internet communications. While both techniques threaten civil liberties, we strongly urge the Judiciary Committee to investigate upstream surveillance and the particular threats that technique poses to privacy and free expression.

Upstream surveillance conducted under Section 702 "occurs with the compelled assistance of providers that control the telecommunications 'backbone' over which telephone and Internet communications transit."[4] The technique encompasses both wholly domestic communications sent and received by United States Persons (USP), as well as non-targeted foreigners. Indeed, in 2011, the Bates Opinion ascertained that the NSA had collected tens of thousands of wholly domestic U.S. communications under its upstream collection annually.[5] We believe that upstream surveillance poses unique and grave concerns for privacy, and the Committee should take steps to ensure this technique is stopped entirely.

One clear example of the threat to privacy posed by upstream surveillance is so-called "about" surveillance. "About" surveillance includes searching the *content* of communications that are neither *to nor from* a surveillance target for specific "selectors," such as email addresses, IP addresses, or phone numbers believed to relate to a surveillance target.[6] Warrantless searches of the content of Americans' communications—even if only for specific "selectors"—plainly violates the Fourth Amendment.

Lastly, upstream surveillance is not limited to Section 702. The technique appears to be used within the United States under Executive Order 12333 ("EO 12333").[7] The same problems plaguing Section 702 upstream surveillance—like the collection of wholly domestic communications—can almost certainly be found in upstream surveillance conducted under EO 12333. As a result, we urge the Committee to investigate EO 12333, the constitutionality of surveillance conducted under that authority (particularly when carried out within the United States), and the privacy harms stemming from EO 12333 surveillance. At minimum, the Judiciary Committee should request the completed study of EO 12333 activities written by the Senate Select Committee on Intelligence.[8]

Central Intelligence Agency ("CIA") and the Federal Bureau of Investigation ("FBI") each receive a select portion of PRISM collection." See, Pg. 7, https://www.pclob.gov/library/702-Report.pdf

[3] See, Pg. 29, Memorandum Opinion of October 3, 2011 by the Foreign Intelligence Surveillance Court ("Bates Opinion"). https://www.eff.org/document/october-3-2011-fisc-opinion-holding-nsa-surveillance-unconstitutional.

[4] See, Pg. 7, https://www.pclob.gov/library/702-Report.pdf. In another context, the Bates Opinion defines "upstream collection" on page 5 as referring "to NSA's interception of Internet communications as they transit [redacted], rather than to acquisitions directly from Internet service providers such as [redacted]," which presumably refers to PRISM collection).

[5] See, Pg. 39, Bates Opinion.

[6] Savage, Charlie, *NSA Said to Search Content of Messages to and From U.S.*, N.Y. Times, Aug. 8, 2013. (The NSA is "searching the contents of vast amounts of Americans' e-mail and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance"), available at http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html; see also Pg. 84, of PCLOB 702 Report discussing "about" collection.

[7] See, https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet.

[8] See, http://www.mcclatchydc.com/news/nation-world/national/national-security/article24759289.html#storylink=cpy.

Require the Government to Submit Surveillance Targets for Judicial Review

We also recommend the Judiciary Committee review whether the government should submit Section 702 directives or "tasking sheets" to the FISC. "Tasking sheets" are NSA-created documents generated prior to initiating surveillance on a particular target. These sheets contain the selector, a description of what foreign intelligence information the analyst will collect, and citations to information showing why the analyst thinks the selector belongs to a foreign person.[9] The Intelligence Community already shows a small sample of tasking sheets and selectors to the FISC.[10] The Judiciary Committee should require that all tasking sheets, directives, and related documents be provided for the FISC's review.

Currently, Section 702 only requires the government submit certifications, "targeting" procedures, and "minimization" procedures for the FISC's review. Generally speaking, the targeting procedures convey how the acquisition will try to target foreign persons and how the Intelligence Community will try to prevent the intentional acquisition of wholly domestic communications; the minimization procedures convey how the information collected will be processed, retained, and shared. However, Section 702 currently does not require the government to specify to the court who its surveillance targets are, what communications accounts or websites it will subject to surveillance, or what specific information the government's surveillance seeks.

In light of the vast quantity of communications collected and the threat Section 702 surveillance poses to civil liberties, Executive branch employees cannot have such unfettered discretion to decide whom to target, when, where, and under what circumstances. As the Keith Case concluded: "The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised."[11] At minimum, the Executive branch should be required to produce all tasking sheets, directives, and related documents for the FISC's review.

Prohibit Backdoor Searches

Under its implementation of Section 702, the government conducts "backdoor searches"—in which it queries its database of intercepted communications for the communications of specific Americans—without a warrant, prior court authorization, or any external restriction.[12] Nothing in Section 702 prohibits the "incidental" collection and retention of Americans' international communications; indeed, under current minimization guidelines, even unintentionally acquired domestic communications may be retained. Once acquired, these communications may be stored in government databases for several years. And, given the scope of the government's collection, the quantity of communications—including communications of Americans—within these databases is vast.

Nevertheless, the government maintains that having "lawfully collected" the communications of Americans, the government does not need subsequent court approval to

---

[9] See, Pg. 70, PCLOB 702 Report.

[10] See, Pg. 19, https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf.

[11] U.S. v. U.S. District Court, 407 U.S. 297, 317 (1972).

[12] See, Letter from James R. Clapper to Senator Ron Wyden, March 28, 2014, available at https://s3.amazonaws.com/s3.documentcloud.org/documents/1100298/unclassified-702-response.pdf; see also Ackerman, Spencer; and, Ball, James. "*NSA loophole allows warrantless search for U.S. citizens' emails and phone calls*." Guardian, Aug. 9, 2013, available at http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls.

search "information that is [at] the government's disposal to review in the first instance."[13] The President's Review Group disagreed, concluding that this practice should be stopped:

> Because the underlying rationale of Section 702 is that United States persons are entitled to the full protection of their privacy even when they communicate with non-United States persons who are outside the United States, they should not lose that protection merely because the government has legally targeted non-United States persons who are located outside the United States under a standard that could not legally be employed to target a United States person who participates in that communication.[14]

Already, the House of Representatives has sought to prohibit "backdoor" searching.[15] The Committee should follow the recommendation of the President's Review Group and eliminate this sweeping loophole.

Advancing Transparency and Oversight

Underlying all of these issues are serious flaws in the classification system. While it is widely acknowledged the system is broken, no serious attempts are being made to fix it. Overbroad classification claims allow the Executive branch to wield undue authority and control over the public discussion concerning these critical surveillance issues. We urge the Judiciary Committee, and the larger Congress, to exert its own power as a coequal branch of government to release documents and other relevant information about Section 702 to the public. In other instances (and as recently as December 2014) individual members of the Senate Judiciary Committee have taken to the Senate floor to release previously classified and/or confidential intelligence information.[16]

The Judiciary Committee can increase transparency around Section 702 by investigating and making public the number of USP communications collected with Section 702. Last month, both privacy advocates and members of the House Judiciary Committee sent letters to the Intelligence Community requesting such a number.[17] In response, Director of National Intelligence James Clapper committed to trying his "best" to calculate an estimate.[18] We urge the Judiciary Committee to follow up on Director Clapper's remarks.

---

[13] See, Pg. 31, Privacy and Civil Liberties Oversight Board, March 19, 2014 Public Hearing ("PCLOB Hearing"). https://www.pclob.gov/events/2014/march19.html.

[14] *Liberty and Security in a Changing World: Report and Recommendations from the President's Review Group on Intelligence and Communications Technologies 145-46 (2013) (emphasis in original).*[14]

[15] See, https://lofgren.house.gov/news/documentsingle.aspx?DocumentID=397951.

[16] See, http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=d2677a34-2d91-4583-92a4-391f68ceae46.

[17] Specifically, see https://www.brennancenter.org/press-release/us-house-judiciary-committee-members-call-director-national-intelligence-disclose and https://www.brennancenter.org/press-release/brennan-center-civil-liberties-groups-press-director-national-intelligence-answers. Privacy groups specifically asked for a public estimate of the number of communications or transactions involving American citizens and residents subject to Section 702 surveillance on a yearly basis; the number of communications or transactions involving U.S. residents whose contents or metadata are "screened" for selectors in the course of upstream surveillance; the number of communications or transactions involving U.S. residents that are retained after their contents or metadata have been screened for selectors in the course of upstream surveillance; the number of communications or transactions involving U.S. persons that are retained in the course of PRISM surveillance; and, the number of U.S. residents whose information is examined or obtained using any other type of surveillance conducted pursuant to Section 702.

[18] See, http://thehill.com/policy/national-security/277501-spies-see-obstacles-for-calculating-surveillance-of-americans.

Other information is equally important for a national conversation on Section 702 before it expires. For instance, we recommend the Committee release information describing:

- government oversight related to the surveillance programs, including detailed information about all compliance issues with Section 702;
- legal rationales under which the programs operate;
- materials sent to Congress in 2006, 2007, 2008, and 2012 about Section 702 and the Protect America Act; and,
- the manner in which the Intelligence Community processes Section 702 communications.

Even without Executive agreement, the Senate Judiciary Committee should publish an index of any documents it reviews, identifying them by author, date, title, general subject matter, relevant statutory provision, and number of pages. Such information should not be classified, and its release could help the public identify, and prioritize, the release of those documents most critical to the ongoing national debate about Section 702.

Conclusion

We are pleased the Senate Judiciary Committee is beginning to review Section 702 in light of its expiration in December 2017. These are only a few of the fundamental issues with Section 702's surveillance techniques that must be fully explored by the public and the Judiciary Committee before December 2017. Please contact Mark Jaycox at jaycox@eff.org or 415.436.9333x128 for any more information.

Sincerely,

Mark Jaycox
Civil Liberties Legislative Lead
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109

Lee Tien
Senior Staff Attorney and Adams Chair for Internet Rights
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109