November 6, 2019

The Honorable Lindsey Graham
Chairman
Committee on the Judiciary
U.S. Senate
224 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Diane Feinstein
Ranking Member
Committee on the Judiciary
U.S. Senate
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Graham, Ranking Member Feinstein, and Members of the Committee:

My name is Patrick Eddington, and I am Research Fellow at the Cato Institute where I work at the nexus of issues involving national security and the Bill of Rights. I appreciate the Committee's willingness to hear my thoughts on the looming expiration of the USA Freedom Act and the opportunity the sunset provision gives us for considering broader surveillance authority reform. Let me note at the outset that the views I express today are mine alone and do not necessarily reflect the views of the Cato Institute, its board or leadership.

Today, I will discuss multiple examples of domestic surveillance abuses and related reform proposals, but let me begin with the central topic of today's hearing: the USA Freedom Act and the PATRIOT Act Sec. 215 telephone metadata program.

Section 215

Over the last six years, the Congress and the public at large have received ample evidence that the Section 215 telephone metadata program (often referred to in technical terms as the "call detail record" or CDR program per the USA Freedom Act) has 1) never stopped a terrorist attack on the United States, 2) resulted in the collection of data on millions of innocent Americans, and 3) wasted considerable tax dollars in the process.

President Obama's Review Group on Intelligence and Communications Technologies concluded in December 2013 that the CDR program "was not essential to preventing attacks" and should be terminated.[1] A month later, the Privacy and Civil Liberties Board issued its own report on the Section 215 program, which offered an even more scathing assessment:

> Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.[2]

---

[1] *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technology*, pp. 104, 119.
[2] 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*, p. 11.

Despite the clear evidence presented by two independent bodies that the CDR program was a failure, violative of American's rights, and a waste of taxpayer money, Congress elected in 2015 to renew the program via the USA Freedom Act (PL 114-23). In the intervening four years, ample additional evidence has emerged that the program remains a debacle.

Indeed, in May 2018, the Office of the Director of National Intelligence (ODNI) released a report showing that the number of Americans' phone calls and text messages collected under the CDR program tripled between 2016 and 2017—from more than 151 million to more than 534 million, the exact opposite effect that the "reforms" of USA Freedom Act were intended to produce.[3] Less than a year later, NSA itself recommended that the CDR program be terminated due to "logistical and legal burdens" associated with it.[4] In June 2019, the *Wall Street Journal*, working from NSA documents obtained by the ACLU via a Freedom of Information Act (FOIA) lawsuit, reported that NSA had—for at least the second time—again collected calls and text messages on innocent Americans without the approval of the secret Foreign Intelligence Surveillance Court (FISC).[5]

Yet despite these damning revelations, on August 14, 2019, this committee and the Senate Select Committee on Intelligence received a letter from then-DNI Dan Coats asking that the CDR program authority be renewed.[6] DNI Coats offered that "as technology changes, our adversaries' tradecraft and communications habits will continue to evolve and adapt. In light of this dynamic environment, the Administration supports reauthorization of this provision as well."[7]

In October 2019, the conservative/libertarian FreedomWorks Foundation joined with the liberal Demand Progress Education Fund to issue a joint report on the history of abuses of the Sec. 215 telephone metadata/CDR program. The report relies largely on declassified Executive branch documents and FISC opinions that serve as a clear rebuttal to DNI Coats assertions about CDR program.[8] Simply stated, there is no rational reason for the CDR program to be renewed.

Indeed, of the 160 or so provisions of the PATRIOT Act that are law, the author is not aware of a single public example of any of them being linked with the prevention of a terrorist attack on the United States. It would serve the Committee well to formally ask the Government Accountability Office (GAO), the Congressional Research Service (CRS), and the Congressional Budget Office (CBO) whether there is, in fact, any data directly linking any of the PATRIOT Act's provisions to the thwarting of a terrorist attack on America.

---

[3] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities, Calendar Year 2017*, p. 35.

[4] Dustin Volz and Warren P. Strobel, "NSA Recommends Dropping Phone-Surveillance Program," *Wall Street Journal*, April 24, 2019 (digital edition)

[5] Dustin Volz, "NSA Improperly Collected U.S. Phone Records a Second Time," *Wall Street Journal*, June 26, 2019 (digital edition)

[6] Letter from DNI Coats to the Senate Committee on the Judiciary and the Senate Select Committee on Intelligence, August 14, 2019. Available at https://int.nyt.com/data/documenthelper/1640-odni-letter-to-congress-about/20bfc7d1223dba027e55/optimized/full.pdf

[7] Ibid, pp. 1-2.

[8] Section 215: A Brief History of Violations, Demand Progress Education Fund and FreedomWorks Foundation, September 2019. Available online at https://www.section215.org/.

Moreover, the failed CDR program is only one of several that require far greater Congressional oversight and remedial action.

The FISA Amendments Act

Within 72 hours of the September 11, 2001 Al Qaeda attacks on the United States, then-NSA Director Michael Hayden took the unprecedented—and unconstitutional—step of authorizing NSA personnel to "conduct specified electronic surveillance on targets related to Afghanistan and international terrorism for 30 days. Because the surveillance included wire and cable communications carried in or out of the United States, it would otherwise have required [Foreign Intelligence Surveillance Court] authority."[9]

The program, which ultimately went under the umbrella codename of STELLAR WIND, was officially sanctioned by then-President George W. Bush via a Top Secret directive on October 4, 2001 and the scope of the program soon expanded beyond Afghanistan to include Iraq.[10] None of these surveillance activities were sanctioned by the FISC prior to the program's public exposure by the *New York Times* on December 16, 2005.[11] Despite the clear illegality of the program, no Bush administration official was prosecuted or impeached and removed from office for authorizing or implementing STELLAR WIND.

Instead, for the next two years the Congress debated how to make the previously illegal mass surveillance program legal. The result, passed in 2008, was the FISA Amendments Act (herein after referred to as the "FAA").[12] The legislation added a new Title VII to FISA, the purpose of which was to create "new separate procedures for targeting non-U.S. persons and U.S. persons reasonably believed to be outside the United States."[13]

From the very beginning, civil liberties advocates argued that the law's language allowed for "reverse targeting" of American's communications (i.e. officially targeting the communications of a foreign national while the real, undeclared purpose was to monitor the communication of American citizen), a fear that was confirmed five years after the FAA's enactment by Senator Ron Wyden (D-OR).[14] In its July 2014 oversight report on the Section 702 program, the PCLOB confirmed Wyden's assertions by acknowledging two incidents of "reverse targeting" that were attributed to analyst errors.[15] However, the PCLOB assessment relied on data supplied by the Department of

---

[9] ST-09-0002 Working Draft report on the STELLAR WIND program, March 24, 2009, p. 3.
[10] Ibid, p. 8.
[11] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005, p. A1.
[12] For an overview of the key provision of Section 702 of the legislation, see Edward Liu, "Reauthorization of the FISA Amendments Act," Congressional Research Service, R42725, April 8, 2013.
[13] Ibid, Summary page.
[14] James Ball and Spencer Ackerman, "NSA loophole allows warrantless search for US citizens' emails and phone calls," *The Guardian*, August 9, 2013 (digital edition).
[15] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Sec7on 702 of the Foreign Intelligence Surveillance Act*, July 2, 2014, p. 118.

Justice (DoJ) and ODNI internal oversight elements, not a truly independent, forensic level audit by the Government Accountability Office (GAO).

By September 2017, the Open Technology Institute had published a 63-page list of Section 702 violations based on all available public data, including declassified FISC opinions.[16] And just last month, newly declassified FISC opinions revealed massive FBI "back door" searches of Section 702 data on Americans collected and stored by the federal government. As the *New York Times* story on the revelations noted

> Specifically, F.B.I. agents had carried out several large-scale searches for Americans who generically fit into broad categories — like they were F.B.I. employees or contractors — so long as agents had a reason to believe that someone within that category might have relevant information.[17]

Congress's decision to allow FISA activities to be carried out at a standard lower than the Fourth Amendment's probable cause requirement is the proximate cause of these and related surveillance violations, whether the authority is the PATRTIOT Act, the FAA or other statutory authorities. Until the Fourth Amendment's probable cause standard is restored to all surveillance practices, and aggressive, sustained oversight actions are mounted to ensure compliance, the kinds of abuses I have catalogued thus far are certain to continue.

Thus far, I have discussed the statutory domestic electronic surveillance abuses that are, to varying degrees, actually known. The Committee should be equally concerned about potential domestic surveillance activities—electronic or otherwise—that are underway absent a statutory basis or any meaningful oversight.

Executive Order 12333

First promulgated in 1981, EO 12333, *United States Intelligence Activities*, is the day-to-day Executive branch regulatory framework for governing American intelligence operations globally. In the nearly 40 years EO 12333 has been in effect, there has never been a public Congressional examination of the order or the activities carried out under it. Prior to losing a quorum of members in January 2017, the PCLOB had largely completed at least one so-called "deep dive" report on one so far unidentified Intelligence Community's (IC) component's activities under EO 12333. Once the Board regained a functioning quorum in October 2018, it resumed work on existing and planned oversight projects, including one or more reports on IC activities carried out under EO 12333.

As I was deeply interested in seeing the results of the PCLOB's investigation of IC activities undertaken via EO 12333, on April 23, 2019 I filed a Freedom of Information Act (FOIA) request for the following:

---

[16] Open Technology Institute, *A History of FISA Section 702 Compliance Violations*, September 28, 2017. Available online at https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/.

[17] Charlie Savage, "F.B.I. Practices for Intercepted Emails Violated 4th Amendment, Judge Ruled," *New York Times*, October 8, 2019 (digital edition).

1. Any Board reports issued on federal department and agency activities conducted pursuant to Executive Order 12333, as amended; and

2. Any correspondence in any form to or from the Board regarding alleged or actual violations of laws, regulations, or executive orders by any federal department or agency under the purview of the Board.

3. Any correspondence in any form to or from the Board regarding refusals by any federal department or agency to provide information requested by the Board pursuant to its statutory oversight mission.

While the PCLOB has agreed to review and release to me material relevant to alleged or actual violations of laws, regulations, or executive orders, it has refused to release any EO 12333 report or any records dealing with by any federal department or agency to provide information requested by the Board.

Regarding the refusal to release even redacted versions of any EO 12333 reports, Board FOIA Officer Logan O'Shaughnessy stated in a September 23, 2019 letter to me that

> Regarding your first request, the PCLOB has heard back from the relevant agency as part of the consultation process. **The agency has determined that the PCLOB's completed deep dive report under Executive Order 12333 is not segregable and no information from the report may be released**. Accordingly, the completed report is withheld pursuant to Exemptions], 3, and 5 of the FOIA, 5 U.S.C. § 552(b)(l), (b)(3), (b)(5).[18] (emphasis added)

While I have appealed the PCLOB's denial, I think it worth noting that Mr. O'Shaughnessy's wholesale invocation of Exemption 1 is contrary to the plain language of the FOIA statute, which explicitly states that "Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt…"

Mr. O'Shaughnessy failed to explain how it would be impossible to, for example, segregate Board comments, opinions, or conclusions about a given program's legality or effectiveness from any specific description of the program or activity itself that could be construed as legitimately classified under EO 12333 in the opinion of the executive agent of the program or activity in question. I should note that in its Section 702 report, the Board did redact certain information from FISA Court opinions while still making public other portions of the opinions and related Board comments or conclusions on the opinions, the operations of the FISC, etc. I also note that nowhere in the PCLOB's enabling legislation (codified at 42 U.S.C. § 2000ee) does it permit the agency or department that is the subject of a PCLOB report to censor the Board's own conclusions, observations, and recommendations.

[18] Letter from PCLOB FOIA Office Logan O'Shaughnessy to the author, September 23, 2019, p. 1.

This is not an academic matter. If agencies or departments that are the subject of PCLOB oversight investigations are allowed to censor the Board's own conclusions, observations and recommendations, it will have the effect of rendering the Board useless as an oversight body.

The same logic applies to the PCLOB's response on item 3 of my request. If IC elements are "stiff-arming" Board requests for information, the Congress and the public at large are entitled to know that immediately, and Congress should take whatever action is required to ensure IC compliance with Board requests for information. At the same time, the Board should not be in the business spuriously using FOIA exemptions to conceal bad faith conduct by IC elements.

Indeed, as federal courts have ruled that communications between an agency such as the Board and Congress cannot be withheld under Exemption 5 as Congress is not an agency in the context of the statute, the Board's invocation of Exemption 5 is in my view illegal.[19] Similarly, any communications to or from the Board and a private third party likewise cannot be withheld under Exemption 5.[20] I respectfully request that the Committee hold an oversight hearing with the Board to examine these issues fully and publicly, and that the Committee require the Board to provide any completed EO 12333 reports to the Committee prior to any vote on surveillance reform legislation this session.

Again, Chairman Graham and Ranking Member Feinstein, I appreciate the opportunity to provide you and your colleagues with my views on this critical public policy issue.

Sincerely,

Patrick G. Eddington
Research Fellow
Cato Institute

[19] *Dow Jones & Co., Inc. v. Dep't of Justice*, 917 F.2d 571, 575 (D.C. Cir. 1990).
[20] *Judicial Watch v. Dep't of Army, 435 F.Supp.2d 81, 91 (D.D.C. 2006)*.