September 17, 2019

Chairman Jerrold Nadler
U.S. House Judiciary Committee
2138 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Doug Collins
U.S. Judiciary Committee
2142 Rayburn House Office Building
Washington, D.C. 20515

Re: FISA Oversight Hearing

AMERICAN CIVIL LIBERTIES UNION

National Political
Advocacy Department
915 15th St. NW, 6th FL
Washington, D.C. 20005
aclu.org

Susan Herman
President

Anthony Romero
Executive Director

Ronald Newman
National Political Director

Dear Chairman Nadler, Ranking Member Collins, and Members of the Committee:

On behalf of the American Civil Liberties Union ("ACLU"), we submit this letter for the record in connection with the House Judiciary Committee's hearing, "Oversight of the Foreign Intelligence Surveillance Act," which is scheduled to take place on September 18, 2019.

In 2015, in response to revelations that the NSA and FBI abused their surveillance powers, members of this committee worked on a bipartisan basis to pass the *USA Freedom Act*.[1] The goal of this legislation was to stop large-scale surveillance under the Patriot Act, increase transparency, and institute other reforms to ensure that Americans' constitutional rights were protected. Since passage of this Act, two things have become apparent. One, the reforms in the *USA Freedom Act* did not go far enough to protect Americans' rights. And, two, many of the reforms in the *USA Freedom Act* are not working as intended.

On December 15, 2019, Section 215 and other provisions of the Patriot Act extended by *the USA Freedom Act* are once again set to expire. **We urge Congress to use this opportunity to pass comprehensive surveillance reform that remedies the deficiencies in the 2015 legislation. Absent meaningful reform, the ACLU urges Congress to sunset Section 215 and the other expiring Patriot Act provisions.**

There are many issues that must be addressed in any meaningful surveillance reform legislation. However, we want to highlight several key reforms that should be included in any legislation:

[1] H.R. 2048, USA FREEDOM Act of 2015, Pub. L. No. 114-23.

- **Ending Section 215's call detail record authority,** which has been used to collect over 1 billion call records[2], has no proven intelligence value, and has been suspended due to persistent compliance violations;

- **Limiting the types of records that can be obtained under Section 215** to exclude location information health information, tax records, and sensitive data that the government generally cannot obtain without a probable cause warrant;

- **Preventing discrimination and strengthening existing First Amendment protections,** including by prohibiting the government from targeting individuals based on First Amendment conduct or discriminating against Americans on the basis of race, religion, nationality, or other protected class status;

- **Requiring notice to criminal defendants and others** who have Section 215 information used against them;

- **Closing the Section 702 backdoor search loophole**, which the government uses to search for information about Americans, thereby circumventing Section 702's prohibition against reverse targeting Americans;

- **Limiting large-scale collection and dissemination of information** under Section 215 and other Patriot Act authorities; and

- **Increasing transparency and oversight**, including by requiring the government to fully disclose the number of individuals whose information is collected under Section 215, requiring additional information be made public about the government's use of other surveillance tools, and making clear that existing law requires the government to promptly declassify novel or significant Foreign Intelligence Surveillance Court (FISC) opinions issued prior to 2015.

1. Ending the call detail record program

It is now apparent that the NSA's call detail record program is unsalvageable. Despite reforms in 2015, the NSA continued to collect an immense amount of Americans' information under the program – amassing over 1 billion records from 2016 to 2018 alone.[3] It has also consistently operated the program in violation of the law. While the NSA has reportedly shuttered the call detail record program, Congress must end this authority to ensure that it can never be restarted.

[2] Office of the Director of National Intelligence, STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES, CALENDAR YEAR 2018, at 30 (Apr. 2019), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf.
[3] *Id.* at 30.

The call detail program has been beset with compliance problems. Documents obtained by the ACLU revealed compliance incidents in November 2017 and February 2018, with the latter resulting in the collection of records that the agency did not have the authority to collect.[4] The Office of Civil Liberties, Privacy, and Transparency (CLPT) assessed that this incident had a "significant impact on civil liberties and privacy."[5] In addition, the NSA reportedly "relied" on this inaccurate information in targeting requests that were approved by the FISC, which may have resulted in improper surveillance.[6]

Following the discovery of the compliance violation, in June 2018, the NSA disclosed that it began deleting *all call detail records* collected under the program because the unauthorized records could not be "identified and isolated." However, the NSA stated that the "root cause of the problem has since been addressed for future CDR acquisitions."[7] Despite these promises, on or around October 2018, it appears that the NSA again received erroneous call records.[8]

In the wake of these persistent problems, the NSA has suspended the program. According to the ODNI, this decision was made after "balancing the program's relative intelligence value, associated costs, and compliance and data integrity concerns caused by the unique complexities of using these company-generated business records for intelligence purposes." In other words, even the ODNI has concluded the value of the intelligence value of the call detail record program does not outweigh its significant costs. This is perhaps unsurprising given that the Privacy and Civil Liberties Oversight Board concluded in 2014 that the call record program had never played a substantial role in stopping a terrorist attack or identifying a terrorist suspect.[9]

It is abundantly clear the call detail records program cannot be operated in a way that does not threaten Americans' rights. Congress should end this authority and should reject ODNI efforts to make the authority permanent so that the program can be restarted in the future.

2. Limiting the types of records that can be obtained under Section 215

---

[4] National Security Agency, REPORT TO THE INTELLIGENCE OVERSIGHT BOARD ON NSA ACTIVITIES, SECOND QUARTER, CALENDAR YEAR 2018—INFORMATION MEMORANDUM, approved for Release by NSA on Jun. 17, 2019, FOIA Case No. 105767 (litigation), at 049-051, available at https://www.aclu.org/legal-document/nsa-foia-documents-quarterly-reports-intelligence-oversight-board-nsa-activities.

[5] *Id.* at 050.

[6] *Id.* at 050-051.

[7] Press Release, National Security Agency, NSA Reports Data Deletion, (Jun. 28, 2018), https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/.

[8] NSA FOIA Case No. 105767, s*upra* note 4, at 032-033.

[9] 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 (Jan. 23, 2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

Under Section 215, the government asserts the authority to request a broad array of records from third parties, merely if they are considered "relevant" to a counterterrorism or counterintelligence investigation.[10] Though the government has not disclosed a complete list of the types of records it obtains under Section 215, this includes phone records, tax returns, health information, gun records, call records, and a host of other sensitive information.[11]

The government has justified this expansive power by arguing that individuals do not have a privacy interest in personal information held by third parties – an argument the Supreme Court rejected last term in *Carpenter* when it held that the government was required to obtain a warrant when demanding individual's location information.[12] Despite this ruling, as of March of this year, the ODNI had still failed to issue guidance or respond to Congressional inquiries regarding how *Carpenter* should be implemented.[13] Moreover, the ODNI has failed to respond to Congressional requests about whether it believes it can use Section 215 to collect location information[14], which would be contrary to the *Carpenter* ruling.

Given this, it is imperative that Congress amend Section 215 to make clear that it cannot be used to obtain sensitive information, including location information, health records, financial information, and sensitive data that that the government can generally not obtain without a search warrant.

3. Preventing Discrimination and Strengthening First Amendment Protections

Existing law fails to include enough protection against surveillance that is discriminatory or targeted based on First Amendment-protected activity. Section 215 and other Patriot Act authorities prohibit surveillance based "solely" on First Amendment-protected activities.[15] However, opinions that have been partially released by the FISC suggest that these safeguards have been interpreted narrowly.[16] These opinions suggest that the government is not foreclosed from surveilling an individual in cases where all or a substantial portion of the facts relied on in a surveillance application involve First Amendment-protected conduct.

Similarly, Presidential Policy Directive-28 states that the U.S. "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

---

[10] See 50 USC § 1861.
[11] See 50 USC § 1861(a).
[12] *Carpenter v. United States,* 138 S.Ct. 2206 (2018).
[13] Letter from Senator Ron Wyden to DNI Director Daniel Coats (Jul. 30, 2019), available at https://int.nyt.com/data/documenthelper/1528-wyden-letter-to-dni-re-215-and/6e12df714de6eb7df542/optimized/full.pdf#page=1.
[14] *Id.*
[15] *See* 50 USC § 1861(a).
[16] *In Re. Orders of this Court Interpreting Section 215 of the Patriot Act,* Docket No. Misc 13-02 (FISC Aug. 24, 2017), https://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Opinion-1.pdf

religion."[17] However, existing law and policies that are publicly available do not make clear that Patriot Act authorities cannot be used to target individuals based on race, religion, ethnicity, nationality, and other protected classes, and that the government cannot use selection terms that can serve as proxies for membership in a protected class.

To address these deficiencies, Congress should clarify and strengthen existing First Amendment protections to prohibit surveillance in cases where either the purpose of the investigation or the factual predicate for the surveillance is First Amendment protected activities. In addition, Congress should prohibit targeting of Americans or use of selection terms that are based on or serve as proxies for race, religion, nationality, or other protected classes.

4. Notice

Unlike other surveillance authorities, including Section 702 of the Foreign Intelligence Surveillance Act (FISA), Section 215 does not have a statutory provision requiring notice to individuals in cases where information obtained or derived from the authority is used in a criminal, civil, or administrative proceeding. In court filings,[18] the government has denied that it has any obligation to inform defendants when information obtained or derived from Section 215 is used in a criminal case. This position not only violates the Constitution, it also largely forecloses individuals from challenging unconstitutional surveillance in court.

To remedy this, Congress should add a statutory notice provision to Section 215, which makes clear that the government must provide notice in any case that it is using or disclosing evidence that would not have been obtained but for surveillance under Section 215 and regardless of any claim that the evidence would inevitably have been discovered.

5. Closing the Section 702 backdoor search loophole

Section 702 explicitly prohibits the government from targeting U.S. persons. The government nevertheless searches Section 702 data looking specifically for information about U.S. persons, a practice often referred to as a "backdoor search." This permits Section 702 to be exploited as a tool against Americans in foreign intelligence and domestic criminal investigations alike. The NSA performs over 30,000 backdoor searches annually. While the FBI refuses to report the number of backdoor searches it performs, the Privacy and Civil Liberties Oversight Board reports that the number of these searches is

[17] Presidential Policy Directive-28 of Jan. 17, 2014 (Signals Intelligence Activities), available at https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[18] Gov't Response at 6, *United States v. Muhtorov*, No. 12-cr-00033 (D. Colo. Feb. 26, 2015) (ECF No. 711).

"substantial," in part because it is "routine practice" for the FBI to conduct a query when an agent initiates a criminal assessment or investigation related to any type of crime.[19]

The original version of the *USA Freedom Act* would have closed the backdoor search loophole by requiring the government to obtain a warrant when querying the Section 702 database to obtain information about Americans. Unfortunately, this reform was not included in the final version of the bill, despite the fact that the House has twice passed appropriations amendments that would close the backdoor search loophole.[20] We urge Congress to ensure that this reform is included in any surveillance reform measure.

6. Limiting Large-Scale Collection and Dissemination

Statistics released by the NSA suggest that the USA Freedom Act has not achieved its goal of preventing bulk and large-scale collection under the Patriot Act. For example, in 2018, using the pen register and trap and trace authority, the government collected information of 132,690 unique accounts, despite the fact that there were only 34 surveillance targets.[21] Similarly, under the Section 215 business records provision, the government collected information of 214,860 unique accounts, yet had only 60 surveillance targets.[22] The NSA and FBI have not disclosed how often this information is searched, and whether any of this information is routinely searched when the FBI initiates an assessment or criminal investigation.

To address these deficiencies, Congress should further limit large-scale collection under the authorities reformed by the USA Freedom Act. In addition, it should prohibit information collected under the Patriot Act from being disseminated and searched for purposes unrelated to the reasons for which it was collected.

7. Increasing Transparency

The transparency provisions in the USA Freedom Act have failed to ensure that the public and Congress have sufficient information about U.S. surveillance practices – in part because the government has failed to fully comply with them. Section 402 of the USA Freedom Act required the government to declassify novel and significant FISA court opinions – yet the government has wrongly interpreted this to only apply to opinions issued after passage of the Act. In addition, there have not been any FISC opinions declassified pursuant to the statute for at least a year, calling into question whether the government is fully complying with this requirement. Similarly, though the *USA Freedom Act* required the government to report information regarding the number of unique accounts impacted under Section 215 surveillance and other authorities, the government has only partially

---

[19] Privacy and Civil Liberties Oversight Board, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SEC.702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (Jul. 2, 2014) https://www.pclob.gov/library/702-Report.pdf. [Hereinafter "PCLOB Report on 702"]
[20] H.R. 4870, Roll Call Vote 327, http://clerk.house.gov/evs/2014/roll327.xml; H.R. 2685, Roll Call Vote 356, http://clerk.house.gov/evs/2015/roll356.xml.
[21] Office of the Dir. of Nat'l Intelligence, STATISTICAL TRANSPARENCY REPORT, *supra* note 2, at 24.
[22] *Id.* at 26.

released these statistics. Government statistics appear to exclude information from non-communications records, or records that were received through hard-copy or portable media.[23]

To address this, Congress should make clear that the government is obligated to promptly disclose novel and significant FISA court opinions, including those that were issued prior to 2015. In addition, they should strengthen existing transparency provisions to ensure that the government is providing a complete picture of surveillance under Section 702 and Patriot Act authorities.

The expiring Patriot Act provisions are an opportunity for Congress to enact meaningful surveillance reform. In addition to the issues highlighted above, Congress should also consider reforms to further enhance transparency, limit dissemination of information, ensure information collection is targeted, increase oversight, and strengthen the FISA court amici. Furthermore, it must address concerns with the "lone wolf" and "roving wiretap" authorities, which are also set to expire in December. Absent meaningful reform, we urge Congress to allow the expiring Patriot Act provisions to sunset.

If you have questions, please contact Senior Legislative Counsel, Neema Singh Guliani at nguliani@aclu.org.

Sincerely,

Ronald Newman
National Political Director

Neema Singh Guliani
Senior Legislative Counsel

cc: Members of the U.S. House Judiciary Committee

[23] *Id.* at 23, 26.