Privacy and Civil Liberties Oversight Board
Public Forum to Examine the USA FREEDOM Act
Statement of Caroline G. Lynch
Founder & Owner, Copper Hill Strategies, LLC
May 31, 2019

Thank you Chairman Klein and Board Members for the opportunity to participate in the Board's public forum to examine the USA FREEDOM Act and, specifically, the call detail record program (CDR) authorized by the Act. I previously served as Chief Counsel of the House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. In that capacity, I conducted oversight and advised members on Foreign Intelligence Surveillance Act authorities and participated in the negotiating and drafting the Act.

The USA FREEDOM Act,[1] signed into law by President Obama on June 2, 2015, is one of those rare examples of bipartisan, bicameral legislation painstakingly negotiated in close coordination with multiple executive branch agencies over a series of months. It truly is the epitome of legislative sausage making.

This statement will provide an overview of Section 501 of FISA and the NSA's bulk telephony metadata program, provide background on Congress' response to the leaks by NSA contractor Edward Snowden and describe the legislative process that led to enactment of the USA FREEDOM Act. I will then summarize the CDR program and other reforms made by the Act, provide my thoughts on CDR implementation and other provisions of the Act, and discuss how Congress may address reauthorization of the Act prior to December 15th, when the three temporary provisions of the Act will expire.

Section 501 of FISA and the NSA's Bulk Telephony Metadata Program

Section 501 of FISA, more commonly known by its USA PATRIOT Act moniker as Section 215 Business Records, was enacted by Congress in 1998[2] to authorize the FBI to obtain a FISA Court order to compel the production of records of common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities in foreign intelligence investigations. The government was required to provide to the Court "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[3]

[1] H.R. 2048, P.L. 114-23, 129 Stat. 300.
[2] Intelligence Authorization Act for FY 1999, Pub. L. 105–272, 112 STAT. 2396, tit. VI, § 602 (Oct. 20, 1998).
[3] *Id.*

Section 215 of the 2001 PATRIOT Act[4] amended Section 501 to expand the scope of eligible records to any "tangible thing" and broaden the standard to require that the FBI "specify that the records concerned [were] sought for a [foreign intelligence investigation]." These amendments, however, were made temporary through the use of a four-year "sunset" provision. The 2005 PATRIOT Act reauthorization[5] again amended Section 501 in several respects, including requiring high-level FBI approval for certain sensitive records, modifying judicial review procedures, and changing the legal standard to "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence investigation.]" The law treats records as presumptively relevant if they pertain to:

- a foreign power or an agent of a foreign power;
- the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or
- an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation;

The 2005 amendments were also given temporary effect through a sunset. Congress continued to re-up these amendments through both short-term and long-term PATRIOT Act reauthorizations over the next six years.

The bulk telephony metadata program was initiated as part of the President's Surveillance Program following the 9/11 terrorist attacks. In 2006, the government sought to bring the program under Section 501 of FISA. Relying on the 2005 standard, the FISA Court granted the government permission, in investigations to protect against international terrorism, to collect metadata from American telephone companies.

Records collected included so-called metadata, such as telephone numbers dialed, and call date, time, and length. Names or other personal identifying information, and telephone call content, were not collected. The government argued, and the Court agreed, that this broad-sweeping data collection was warranted under the statute because "[a]nalysts know that the terrorists' communications are located somewhere in the metadata produced under this authority, but cannot know where until the data is aggregated and then accessed by their analytic tools under limited and controlled queries . . . [a]ll of the metadata collected is thus relevant, because the success of this investigative tool depends on bulk collection."[6]

Thus, the government was permitted to collect extraordinary volumes of metadata, on an ongoing basis, including data about millions of Americans, that would then be stored, analyzed, and queried by the NSA to identify possible terror suspects. Although the program

[4] P.L. 107–56, § 215.
[5] P.L. 109-177, § 106.
[6] *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things,* Doc. No. BR 13–109 (FISC Aug. 22, 2013).

was classified, cleared congressional staff engaged in routine oversight and members were afforded classified briefings on the program, typically in anticipation of a looming sunset, including prior to the 2011 PATRIOT Act reauthorization.

I believe it is important to note that Section 501 is not merely the legal authority for metadata collection, either under the prior NSA program or the CDR authority created by the USA FREEDOM Act. It is also relied upon by the FBI in both its counter-terrorism and counter-intelligence investigations. According to public reporting by the Director of National Intelligence, in 2016, 2017, and 2018, the FBI obtained 84 business records orders against 88 targets, 77 orders against 74 targets, and 56 orders against 60 targets, respectively. For those same years, the government sought 40 CDR orders against 42 targets in 2016, 40 CDR orders against 40 targets in 2017, and 14 orders against 11 targets in 2018.[7]

The FBI's "traditional" business records authority can also be used by the FBI to obtain CDRs separate from the new CDR program, although not on an ongoing basis. As discussed in greater detail below, preserving the FBI's use of Section 501 was a key factor in how Congress structured the targeted CDR authority and the prohibition on bulk collection.

Congress' Response to the Snowden Leaks

The initial leaks by Edward Snowden revealed the NSA's telephony metadata program and the separate PRISM program operated pursuant to Section 702 of FISA.[8] As noted above, Congress had previously reauthorized the temporary PATRIOT Act provisions in 2011. The FISA Amendments Act, originally enacted in 2008, was reauthorized in 2012. These laws were not scheduled to sunset until 2015 and 2017, respectively. Suffice to say, FISA authorities was not top of mind in Congress when the Snowden leaks began in June 2013.

FISA and its implementation by intelligence agencies present a unique challenge for Congress. While the statute is public, specific details about how it is used are not. This was particularly true in 2013, prior to Congress implementing a variety of provisions to bring greater transparency to the use of FISA's intelligence-gathering tools. All members of Congress are privy to certain classified information. In practice, however, routine oversight of FISA falls to the committees of jurisdiction and a finite number of cleared staff. The majority of this oversight is conducted in a classified facility or SCIF, further complicating member education. Likewise, personal staff are ineligible for TS/SCI clearance, thereby limiting their role in the member education process.

---

[7] *See* Director of National Intelligence Statistical Transparency Report Regarding Use of National Security Authorities for CY 2018, *available at* https://www.dni.gov/index.php/newsroom/press-releases/item/1983-odni-releases-annual-intelligence-community-transparency-report.

[8] *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN, Jun. 6, 2013, *available at* https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Since the 2001 enactment of the PATRIOT Act, sunsets on certain intelligence-gathering authorities have become commonplace. A biproduct of sunsets is that Congress typically reserves all-Member classified briefings on FISA-authorized programs to the months or weeks leading up to an impending expiration date. Classified briefings were offered to members prior to the 2011 PATRIOT Act and 2012 FISA Amendments Act reauthorizations. Despite this, not all members availed themselves of the briefings or necessarily recalled what they had learned one or two years later.

In the meantime, the 2012 election ushered in a new freshman class of the 113th Congress, including twelve new senators (half of whom had previously served in the House) and 82 new representatives (nine of whom had previously served in the House).

All of these factors resulted in many members of Congress caught unaware of the existence of these programs, sparking outrage and opposition from many. Further exacerbating this response was that, in the immediate aftermath of the leaks, the programs remained classified, limiting member and staff access to information.

Yet another complicating factor, particularly with the telephony metadata program, was the document used to reveal its existence – a so-called "secondary" order to Verizon.[9] The secondary order served as the means to compel production of telephony records. A separate, more fulsome and classified "primary" order issued by the FISA Court, set the parameters for the use of this metadata and provided the legal analysis of the program's operation under Section 501 of FISA. With access to only the truncated secondary order, members of Congress, the media, and the general public were quick to deem the Court little more than a "rubber stamp" of the executive's use of FISA authorities to collect millions of records about innocent Americans.

The USA FREEDOM Act Legislative Process

Within weeks of the leaks, the House Judiciary Committee and other committees of jurisdiction convened public and classified hearings on both the telephony metadata and 702 PRISM programs. Hearings continued in 2014 following reports by President Obama's Review Group on Intelligence and Communications Technologies and this Board.

Members and staff had a daunting task ahead of them. First and foremost was member education, not simply about the programs but about FISA itself. Confusion persisted about the nuance between Section 501 of FISA and Section 215 of the PATRIOT Act, about the distinction between Section 501 and Section 702, about whether and under what circumstances FISA can be used to target US persons, about the FISA Court, and myriad other issues.

[9] *See Verizon forced to hand over telephone data—full court ruling,* The Guardian, Jun. 5, 2013, *available at* https://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephonedata-court-order.

The USA FREEDOM Act was initially introduced in both chambers in Fall 2013. But Congress remained sharply divided on fundamental policy issues. Some members were content to keep the telephony metadata program intact; many others wanted to abolish it altogether. Members were also divided on reforms to Section 702 and other FISA authorities, changes to the National Security Letter statutes, and reforms to the FISA Court.

In January 2014, President Obama announced several changes to the telephony metadata program, reducing from three to two the number of "hops" in metadata collection, and requiring FISA Court approval before data could be queried. President Obama also announced an end to the ongoing "bulk" collection of telephony metadata, opting instead to leave the records with the telephone companies to be acquired following query approval by the Court.[10]

These reforms offered a roadmap for Congress to design a new program that would meet the government's intelligence needs and provide a political middle ground for lawmakers. The first attempt at codifying this process cleared the House in May 2014. Similar legislation failed to achieve cloture in the Senate in November 2014.

That brought us to the beginning of the 114th Congress (and more newly elected members of Congress) and five months away from the next PATRIOT Act sunset date. House and Senate negotiators would spend a significant portion of that time hammering out the version of the Act enacted on June 2, 2015.

Getting the Act across the finish line was no easy feat. The Act passed the House with a 338-88 vote on May 22, 2015. While their was majority support for the Act, there certainly was not unanimity, with some concerned that it went too far to curtail NSA's intelligence-gathering capabilities and others concerned it did not go far enough to protect American's privacy and civil liberties.

Senate consideration was even more contentious. Following a failed cloture vote to end debate on the Act, and the rejection of a separate two-month extension of the expiring provisions, the Senate adjourned for the Memorial Day recess. On May 31, 2015, with Section 215, roving authority, and the lone wolf definition set to expire at midnight, the Senate proceeded with debate on the House-passed bill. After rejecting a handful of amendments, the Senate ultimately passed the Act on June 2, 2015. President Obama signed the bill later that day.

This process and previous FISA-related reauthorizations are instructive about the process the Board and congressional leadership should anticipate with USA FREEDOM Act renewal.

---

[10] *See Press Release, The White House, Office of the Press Secretary, Statement by the President on the Section 215 Bulk Metadata Program (Mar. 27, 2014), available at http://www.whitehouse.gov/the-press-office/2014/03/27/statement-president-section-215-bulk-metadataprogram.*

The USA FREEDOM Act

At the heart of the USA FREEDOM Act is the CDR program,[11] which replaced the NSA's bulk telephony metadata program. Like the NSA program, CDR collection is authorized under Section 501 of FISA and is limited to investigations to protect against international terrorism. Unlike the NSA program, the CDR program eschews indiscriminate, "bulk" collection of metadata in favor of FISA Court-approved targeted collection.

Congress faced several challenges in constructing this program within Section 501. It needed to simultaneously authorize CDR collection, prohibit "bulk" collection, and preserve the FBI's traditional use of the 501. Congress, therefore, opted to keep the "relevancy" standard in place, while separately authorizing CDR collection and adding an additional requirement that each 501 application include a "specific selection term" or SST.[12]

The SST is simultaneously restrictive and enabling. By requiring the government to include a SST in each application, it serves as the mechanism to prohibit "bulk" collection. But the term was also carefully defined to not disrupt the FBI's traditional use of the authority, despite the required inclusion of a SST in each application. The Act provides a separate, more narrow definition of SST for use in CDR applications.[13] The Act also prohibits bulk collection under the FISA Pen Register Trap and Trace provision and four of the National Security Letter statutes with the addition of slightly modified SST requirements.[14]

Using the new CDR authority, the government can acquire records held by the telephone companies if it demonstrates to the Court 1) there are reasonable grounds to believe that the call detail records sought to be produced based on the SST are relevant to such investigation, and there is 2) a "reasonable articulable suspicion" that the SST is associated with a foreign power or an agent of a foreign power engaged in international terrorism or activities in preparation therefor. The government may also acquire records on an ongoing basis for up to 180 days and up to two "hops" worth of data. Congress required the government to adopt minimization procedures requiring the prompt destruction of non-foreign intelligence records.

Congress made a number of other reforms to Title V of FISA, including emergency business records authority, expanded FISA Court authority to assess the adequacy of minimization procedures, authority to promptly challenge a nondisclosure order, and enhanced liability protections for third parties.

The Act also includes a variety of provisions to provide greater public transparency and accountability for the use of certain FISA authorities, including expanded reporting

[11] H.R. 2048, § 101 (amending 50 U.S.C. § 1861(b)).
[12] *Id.*, § 107 (codified at 50 U.S.C. 1861(k)).
[13] *Id.*
[14] *Id.*, titles II and V.

requirements to Congress and oversight by the DOJ and IC Inspectors General. The Act authorizes the FISA Court to seek input from amicus curiae as it deems appropriate. Given the sensitive nature of the matters heard by the Court, Congress directed the Court to establish a pool of potential amici, who possess or can be issued the necessary security clearances, to provide timely, meaningful legal or technical assistance to the Court.

The Act expands the role of the FISA Court of Review, imposes a declassification mandate of significant or novel interpretations of law, authorizes public reporting by FISA order recipients, corrects constitutional infirmities with nondisclosure procedures, and restricts the use of information concerning U.S. persons improperly obtained under Section 702 of FISA. The Act also closes gaps in the law that required surveillance to cease when a target leaves or enters the country and codifies various U.S. nuclear treaty obligations.

Implementation of CDR Authority

To prevent intelligence gaps, the USA FREEDOM Act delayed the prohibition on bulk collection and CDR authority for six months,[15] thereby enabling the government time to transition to the new program. Despite this, the government has reportedly encountered technical issues with CDR implementation. The NSA reported in 2018 that it had deleted millions of records after discovering substantial overcollection going back to 2015.[16] A congressional leadership aide revealed in a March podcast that the CDR program had not been operating the program for some months and expressed doubt as to whether the government would seek renewal of CDR authority.[17] In April of this year, the NSA allegedly recommended to the White House that the CDR program be terminated. According to a Wall Street Journal report, the NSA indicated that "the logistical and legal burdens of keeping it outweigh its intelligence benefits."[18]

These reports are publicly unconfirmed by the Trump administration, and specific details are lacking. So I believe it is imperative for the Board and Congress to fully assess the status of the program. Is this simply a technological issue that may be overcome in a matter of months or years? Are CDRs diminishing in intelligence value as terror targets transition away from traditional telephony to new communication techniques? Perhaps it's a little of both.

Congress should also assess whether a shift in communication techniques by foreign terrorist organizations has created intelligence gaps limiting our ability to monitor and track terror suspects. It should come as little surprise if we are to learn that CDRs are decreasingly

[15] H.R. 2048, § 109.
[16] *NSA deletes phone records, citing 'technical irregularities'*, ASSOCIATED PRESS, Jun. 28, 2018, *available at* https://www.apnews.com/d5b4debc1c1c4932ae79557c2a512f90.
[17] *Disputed N.S.A. Phone Program Is Shut Down, Aide Says,* NEW YORK TIMES, Mar. 4, 2019, *available at* https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html.
[18] *NSA Recommends Dropping Phone-Surveillance Program,* WALL STREET JOURNAL, *available at* https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247.

beneficial for counter-terrorism investigators. For several years now, our intelligence and law enforcement agencies have cautioned that terror groups like ISIS are increasingly relying on encrypted apps and other communication platforms to lure recruits and plot attacks. We should also presume that terror groups pay close attention to our national security programs and altered their communication techniques after learning of classified intelligence techniques through the Snowden leaks.

As the December sunset approaches, Congress must take care to fully assess these factors. For instance, would a wholesale repeal of CDR authority inspire these terror groups to actually return to more traditional telephony under the belief that those records are no longer monitored? This may not be the case, but Congress should presume that terrorist organizations will be closely monitoring what changes, if any, it makes to the USA FREEDOM Act.

Reauthorization Options for Congress

Congress has several options for how to address the expiring authorities: 1) allow the authorities to expire, 2) amend the statute to repeal or modify CDR authority (and possibly make other changes) and further extend the expiring provisions, or 3) pass a "clean" or straight reauthorization.

If Congress opts not to renew the temporary provisions, Section 501 (and Section 502) will revert to their pre-2001 PATRIOT Act form. While this would effectively repeal the CDR authority, it would also remove all of the other amendments to these sections made since 2001. The FBI's traditional use of the authority would be severely handicapped for both its counter-terrorism and its counter-intelligence investigations. The amendments offering additional rights to court order recipients, expanding the role of the Court, providing more robust reporting to Congress, and enabling emergency authority would also be repealed.

So too would the prohibition on bulk collection via the SST requirement. Some may argue that a prohibition on bulk collection is unnecessary if the business records standard and scope return to their 1998 version. Congress may nonetheless wish to preserve the bulk collection prohibition in Section 501 to make its legislative intent clear. This would also preserve consistency with the bulk collection prohibitions in the PR/TT and NSL statutes, which are not subject to sunsets. In addition to Section 501 amendments, the roving and lone wolf authorities would also expire.

This option would weaken our ability to protect America's national security. ISIS and other terror groups have suffered significant setbacks in recent years but the threat has not been eliminated. These groups continue to inspire and encourage attacks such as the Easter bombings in Sri Lanka or the Boston Marathon, San Bernardino, and Orlando plots here at home. It would be imprudent to presume that the United States could not fall victim to future plots. Allowing these authorities to expire could also impact critical counter-

intelligence investigations, including efforts by foreign governments to access America's sensitive information, disrupt our elections, or weaken our critical infrastructure.

Amending the statute to repeal or modify CDR authority could prove to be politically challenging. If Congress opts to amend the statute to repeal CDR authority, it could do so while leaving the "relevancy" standard, the SST requirement and other 2015 reforms intact and make the necessary conforming amendments, including to reporting requirements. Even simply opening up the Act to affirmatively remove CDR authority from the statute could invite a variety of amendments to FISA that address politically-charged topics, such as whether and under what criteria FISA authorities can be used to target persons affiliated with a presidential campaign, or revisit proposals rejected by Congress during the 2015 debate or the subsequent FISA Amendments Act reauthorization debate.

Congress may also choose to modify CDR authority to enable the collection of more relevant and accurate communications metadata in counter-terrorism investigations, assuming an intelligence gap exists that warrants such changes within Section 501. A pivot away from collecting traditional telephony metadata to metadata generated by new communication techniques would require the assistance of technology companies and app developers that may be reluctant to cooperate. Given the heightened attention to privacy on Capitol Hill, coupled with civil liberties concerns with the existing CDR program, it seems unlikely that Congress would choose to authorize additional or modified metadata collection via Section 501.

It is certainly Congress' right to debate all of these issues. But with the December 15th expiration date fast approaching, I wouldn't expect the divided chambers to reach consensus on a substantive reform bill, threatening to push reauthorization into a presidential election year and further politicizing the process.

The third option is a "clean" or straight reauthorization – a simple change of the date. This is probably the path of least resistance for Congress but not without its political hurdles. A straight reauthorization would keep CDR authority in place. This wouldn't be the first time that Congress has left unused law on the books. Section 501 does not require the government to collect CDRs, or any business records for that matter. Rather, it authorizes the government to seek permission from the FISA Court to do so. Therefore, keeping CDR authority in the statute would not force the government to operate the program.

Should technological hurdles be overcome in the future -- and CDRs provide an intelligence benefit – collection could resume. A straight reauthorization, however, will likely be met with opposition from many in Congress, but perhaps not a majority, who want to affirmatively repeal CDR authority and from those who wish to pursue other substantive reforms to the law. At this point in the legislative session, however, a straight reauthorization may be the best option for preserving the temporary authorities while steering clear of presidential election politics.

Next Steps

It's time for Congress to begin public oversight and member education. While routine classified oversight is likely ongoing by the relevant committees, no public committee hearings have been convened to date. Congress should conduct holistic oversight of the Act to assess not only the function and utility of the temporary provisions but also of the permanent portions of the law.

Regardless of how Congress ultimately resolves reauthorization, members need to be armed with information about the law and its use by the intelligence agencies. For members newly elected in 2016 and 2018, this will be their first foray into the PATRIOT Act and USA FREEDOM Act. But even veteran members need a refresher, especially those who do not serve on jurisdictional committees. There is a significant amount of publicly available information about the use of FISA authorities from the Director of National Intelligence, the FISA Court, and other sources. I encourage members, staff and the public to take advantage of these resources as the sunset approaches.

I'll conclude with a final word about sunsets. As I noted previously, Congress typically holds hearings and briefings only when an expiration date is looming. But it typically doesn't hold hearings and briefings unless an expiration date is looming. But threats to our national security are constant. It is not a question of "if" but "when" the U.S. will fall victim to another terrorist attack on our soil. And we are increasingly the target of cyber intrusions and other threats to our national security by hostile foreign nations. Congress should adopt more routine public oversight and member education opportunities to ensure that both new and veteran members of Congress possess the necessary understanding of FISA and intelligence-gathering programs.

While a sunset forces legislative action of some kind, Congress routinely fails to meet these deadlines, resulting in short-term extensions or even a lapse in the law, creating operational uncertainty or, worse, a gap in intelligence capabilities. The political climate being what it is today, I'm under no illusion that Congress will entertain permanency this year. But at some point, Congress should have a serious conversation about the utility of perennial sunsets in our national security laws.

###