Prepared Statement of Jamil N. Jaffer*
at a
Hearing before the
Senate Committee on the Judiciary
on
Reauthorizing the USA FREEDOM Act of 2015

November 6, 2019

I. Introduction

Chairman Graham, Ranking Member Feinstein, and Members of the Committee, thank you for inviting me to discuss foreign intelligence collection under the USA Freedom Act and, in particular, the call data records (CDR) program. I want to commend the Chairman and the Ranking Member for holding this hearing to ensure that the Senators present here, as well as the American public, have the opportunity to hear the diverse range of views presented on the panel today on this critically important matter. This hearing represents a unique—and perhaps all too rare—opportunity for policymakers and the national security community to discuss these matters in public and to talk candidly about the costs and benefits of intelligence collection, particularly as it takes place in the context of protecting our nation against the very real and continuing threat of international terrorism.

As the members of this Committee all too well know, if Congress does not act by December 15, 2019, the national security authorities that we are discussing today will expire. That is, if Congress does not enact specific legislation in the next 40 days, core provisions that have been in the law since just a few weeks after the catastrophic terrorist attacks of September 11, 2001—the roving wiretap authority and the so-called "business records" provision—as well as lone wolf authority provided in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), and the modifications to certain of these authorities made by the USA FREEDOM Act of 2015, including the CDR program, and the various privacy and civil liberties-enhancing provisions of these laws, will revert back to the law that existed two decades ago, prior to the attacks that killed nearly 3,000 Americans on our soil.

There is little question, therefore, that Congress must act and must act soon. The key question that confronts this Committee is what Congress ought do when to comes to reauthorization. Two of these core provisions—the lone wolf and roving authorities—while perhaps somewhat controversial once upon a time, today generate fairly limited concern, and have been reauthorized with little debate consistently by

* Jamil N. Jaffer currently serves as the Founder and Executive Director of the National Security Institute at George Mason University's Antonin Scalia Law School, where he also serves as an Assistant Professor of Law and Director of the National Security Law & Policy Program. Mr. Jaffer is also affiliated with Stanford University's Center for International Security and Cooperation and serves as Vice President for Strategy & Partnerships for IronNet Cybersecurity, a startup technology company founded by Gen. (ret.) Keith B. Alexander, the former Director of the National Security Agency and Founding Commander of U.S. Cyber Command. Among other things, Mr. Jaffer previously served on the leadership staff of the Senate Foreign Relations Committee as Chief Counsel & Senior Advisor under Chairman Bob Corker (R-TN) and on the leadership team of the Justice Department's National Security Division as Counsel to the Assistant Attorney General for National Security in the Bush Administration. Mr. Jaffer also previously served as Senior Counsel to the House Permanent Select Committee on Intelligence under Chairman Mike Rogers (R-MI) and as an Associate Counsel to President George W. Bush. Mr. Jaffer's testimony before the Committee is presented in his academic and personal capacity and does not represent the views of any of his current or former employers.

Congress a number of times over the last 18 years. In addition, the third core authority—the so-called "business records" provision of the Foreign Intelligence Surveillance Act (FISA)—which provides investigative authority similar to that which exists in a range of criminal and civil matters through grand jury subpoenas and administrative subpoenas (albeit with significantly more protections in the FISA context, including the involvement of a federal judge), is also fairly uncontroversial, having been significantly modified in the USA FREEDOM Act of 2015 to prohibit bulk data collection and to require the use of a specific selection term. As described further herein, with respect to these three authorities, there ought be little debate on reauthorization and, indeed, Congress ought seriously consider making them permanent. Indeed, there is significant precedent for doing so. While 17 provisions of the USA PATRIOT Act were subject to sunset after that statute was enacted in October 2001,[1] since then, all but the three provisions being discussed today—along with the CDR authority created by the USA FREEDOM Act—have been permanently reauthorized.

With respect to the CDR program authorities, there still remains some significant debate. You have already heard today from the United States Department of Justice, including the National Security Division and the Federal Bureau of Investigation, as well as from the National Security Agency, that they (and the Administration writ large) unanimously support the permanent reauthorization of the CDR authority along with the lone wolf, roving, and business records authorities currently set to expire in a few short weeks.[2] As the Committee also knows, however, the NSA recently stopped using the CDR program for certain "technical and operational reasons,"[3] including the fact that companies required to produce CDRs to NSA had provided data that NSA was not authorized to receive.[4] Notwithstanding the fact that

---

[1] *See, e.g.*, Charles Doyle, *USA PATRIOT Act Sunset: A Sketch* at 1-2, Congressional Research Service (Feb. 6, 2006) *available online at* <https://crsreports.congress.gov/product/pdf/RS/RS21704>.

[2] *See, e.g.*, Brad Wegmann, et al., *Joint Statement for the Record at the Hearing Concerning Oversight of the Foreign Intelligence Surveillance Act*, U.S. Senate Committee on the Judiciary, at 1-2 (Sept. 16, 2019), available online at <https://docs.house.gov/meetings/ju/ju00/20190918/109936/hhrg-116-ju00-20190918-sd002.pdf> ("We urge the Committee to consider permanently reauthorizing these authorities based not only on the Government's demonstrated record and the importance of the authorities to national security, but also on the significant reforms contained in the FREEDOM Act….In the wake of repeated reviews and bipartisan authorizations over nearly two decades, the Administration's view is that the time has come for Congress to extend these authorities permanently."); *see also* Office of the Director of National Intelligence, *Acting DNI Maguire Statement on USA Freedom Act* at 1 (Sept. 18, 2019), *available online at* <https://www.dni.gov/index.php/newsroom/press-releases/item/2045-acting-dni-maguire-statement-on-usa-freedom-act> ("The Administration supports a clean and permanent reauthorization of all the USA FREEDOM Act provisions of the Foreign Intelligence Surveillance Act that will expire in December 2019, including the 'lone wolf' and 'roving wiretap' authorities, and the acquisition of business records, including call-detail records, under Title V of FISA."); Office of the Director of National Intelligence, *Letter of DNI Dan Coats to the House and Senate Intelligence Committees* at 1 (Aug. 14, 2019) *available online at* <https://int.nyt.com/data/documenthelper/1640-odni-letter-to-congress-about/20bfc7d1223dba027e55/optimized/full.pdf#page=1> ("I write to express the support of the Intelligence Community (IC) and Administration for the permanent reauthorization of the provisions of the USA FREEDOM Act of 2015 that are currently set to expire in December. These provisions provide the IC with key national security authorities, and we look forward to working with the Congress on their permanent reauthorization.")

[3] *See Joint Statement for the Record*, *supra* n. 2 at 2 ("As this Committee is aware, the NSA recently discontinued the CDR program for technical and operational reasons.").

[4] *See* National Security Agency, *NSA Reports Data Deletion* at 1, NSA Release No. PA-010-18 (June 28, 2018) *available online at* <https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/> (noting that at some point "several months" before May 2018, "NSA analysts noted technical irregularities in some data received from telecommunications service providers. These irregularities also resulted in the production to NSA of some CDRs that NSA was not authorized to receive.")

NSA has discontinued its use of this authority and has deleted the data previously collected,[5] the national security community, including former DNI Dan Coats, current acting DNI Joe Maguire, and the Justice Department and NSA witnesses before this committee are unanimous: the CDR program "retains the potential to be a source of valuable foreign intelligence information,"[6] particularly given the "dynamic [threat] environment"[7] we find ourselves in as a nation, where "technology changes [and] our adversaries' tradecraft and communications habits [] continue to evolve and adapt" and therefore ought be reauthorized.[8]

II. The Current State of the Terrorist Threat

As members of this Committee know, the threat of international terrorism remains very real today. Having been afforded relative safety here at home for nearly two decades based, in significant part, on the the continuous, active intelligence and military efforts our government has undertaken to defeat terrorists overseas, it may be somewhat easy for Americans to believe that the threat of terrorism has receded. This would be a mistake. The reality is that terrorist groups like al Qaeda and the Islamic State in Iraq and Syria (ISIS) and their various affiliates still seek to conduct terrorist attacks here in the United States and in Europe, as well as against our allies in the Middle East and elsewhere around the world.

As former DNI Dan Coats noted in his written testimony before the Senate Select Committee on Intelligence earlier this year, "[g]lobal jihadists in dozens of groups and countries threaten local and regional US interests, despite having experienced some significant setbacks in recent years, and some of these groups will remain intent on striking the US homeland."[9] Indeed, the former DNI noted that global jihadist groups in parts of Africa and Asia have, in the last year alone, expanded their abilities to strike local US interests and that the war in Syria and Iraq has "generated a large pool of battle-hardened fighters with the skills to conduct attacks and bolster terrorist groups' capabilities."[10] And last month, Russell Travers, the Acting Director of the National Counterterrorism Center, told a congressional committee that "the overall threat from radical Islamic terrorists has not abated and, in some regions, is growing," noting specifically that both ISIS and al Qaeda "are expanding into new areas and reinforcing their networks' cohesion, bolstering the overall movement's reach, resiliency, and threat to US

[5] *See DNI Coats Letter*, *supra* n. 2 at 1 ("The National Security Agency has suspended the call detail records program that uses this authority and deleted the call detail records acquired under this authority."); CQ Congressional Transcripts, *Transcript: House Judiciary Committee Holds Hearings on the Foreign Intelligence Surveillance Act*, at 8 (Sept. 18, 2019) ("As this committee is aware, the NSA recently discontinued the CDR program and deleted the records acquired under the CDR authority after balancing the programs' intelligence value, associated costs and compliance and data integrity concerns.") (Testimony of Susan Morgan).

[6] *See Joint Statement for the Record*, *supra* n. 2 at 2

[7] *See DNI Coats Letter*, *supra* n. 2 at 1

[8] *Id*.

[9] *See* Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community* at 10, Senate Select Committee on Intelligence (Jan. 29, 2019), *available online at* <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.

[10] *Id*. at 11.

interests."[11] Indeed, Travers specifically highlighted the fact that "[d]espite our successes, leaders of both al-Qa'ida and ISIS retain the intent to strike the US" and the organizations themselves, as well as "several of their local affiliates and branches[,] retain key competencies and resources—including explosives expertise and foreign operatives— that could support attacks in the US or the West."[12]

And while much has been (rightly) made of the "territorial defeat" of ISIS, as well as the successful operation to kill ISIS leader Abu Bakr al Baghdadi last month, the stark reality made clear by the former DNI's testimony and that of NCTC Director Travers' is that ISIS may actually be gaining strength, particularly in the aftermath of our catastrophic decision to abandon our Kurdish allies, creating a situation advantageous to terrorist groups and those nations, like Russia and Iran, that oppose our policy in the Middle East. Indeed, the former DNI testified that as of January 2019, ISIS still commanded thousands of fighters in the Iraq and Syria region, and had eight branches, over a dozen networks, and thousands of supporters around the world, many bent on pursing external attacks against the United States and the West.[13] More recently, NCTC Director Travers noted that "ISIS's global network remains robust and—in some areas—is expanding, thanks to its approximately 20 global branches and networks" including the establishment of three new branches this year.[14] Indeed, Travers made clear that ISIS groups in Afghanistan, the Philippines, the Sinai Peninsula, and West Africa "have the capacity to conduct sophisticated attacks against local security forces and target US interests and personnel" and noted that in 2019 alone, ISIS launched several "synchronized attack and propaganda campaigns," relying on multiple branches and networks.[15] Thus, while there is no doubt that we have made significant gains against ISIS in the Middle East, these facts are not the hallmarks of a group that is—as the some have suggested—on the verge of total defeat.

Likewise, while we have continued to keep the pressure up on al Qaeda, forcing its leaders to adapt their approach and to focus more on regional and local attacks against the United States and the West, the fact is that al Qaeda's senior leadership continues to "strengthen[] the network's global command structure and continu[es] to encourage attacks against the West, including the United States."[16] Specifically, we know that this past September, Dr. Ayman al-Zawahiri "reiterated his [long-standing] call for attacks against US and Israeli targets," and we've seen a ramp up in attacks by al Qaeda-affiliated regional groups like al Shabaab and Jama'at Nusrat al-Islam wal-Muslimin.[17]

Moreover, tensions with Iran will almost certainly continue to increase as we continue to strongly implement our maximum pressure campaign against brutal and oppressive regime in Tehran, in order to force a renegotiation of the nuclear deal negotiated by the prior Administration. And given Iran's longstanding and expansive support for its Hizballah terrorist proxy organization, as well as the

---

[11] *See* Russell Travers, *Statement for the Record: Global Terrorism: Threats to the Homeland* at 2. House Homeland Security Committee (Oct. 30, 2019), available online at https://www.dni.gov/files/documents/Newsroom/Testimonies/2019-10-30_ODNI-NCTC_Travers_SFR_for_HCHS_Hrg_on_Global_Terrorism_-_Threats_to_Homeland.pdf>.

[12] *Id*. at 3.

[13] *See* Coats, *Worldwide Threat Assessment*, *supra* n. 9 at 11.

[14] *See* Travers, *Global Terrorism*, *supra* n. 11 at 4.

[15] *Id*. at 5.

[16] *See* Coats, *Worldwide Threat Assessment*, *supra* n. 9 at 12.

[17] *See* Travers, *Global Terrorism*, *supra* n. 11 at 5.

increasing pace of activities both in the region and in the West by its intelligence and military organizations,[18] it would not be at all surprising if Iran leverages terrorist activities to try and force a change in U.S. policy.[19] Indeed, the former DNI reported that less than a year ago, Belgium and Germany stopped a plot by the Iranian government to blow up an opposition gathering in Paris that included a number of well-known European and American guests[20] and we have already seen a dramatic uptick in direct Iranian activities in the region, with recent destructive attacks on shipping in the Arabian Gulf, the downing of a U.S. drone, and the cruise missile attack against Saudi Aramco.[21] The more that such activities go unchallenged, the more we might expect Iran (and others) to engage in further testing of our resolve, whether through proxy terrorist attacks or otherwise.[22]

And we've seen the very real consequences and human suffering brought about by terrorist attacks around world. The Easter Sunday bombings in Sri Lanka, which killed over 320 people and injured nearly 500,[23] are but one example of the consequences of letting down our guard. In that case, there have been indications that the Sri Lankan government was warned of the potential of such attacks but failed to take action to protect its people.[24] While it may be debated whether the Sri Lankan example is directly relevant to the ability of the United States to collect intelligence and protect our people against such threats, it nonetheless represents a key recent example of the horrific results of failing to collect—or act swiftly and decisively—on terrorist threat intelligence.

It is likewise worth noting that the serious challenge posed by the rising trend of ethno-supremacist and ultranationalist groups in Europe and elsewhere.[25] While these groups may not present a direct threat to the United States at a national level, the reality is that the hateful ideology they (and their supporters) spread contributes, in a significant manner, to the increasing threat of international terrorism

---

[18] *See* Coats, *Worldwide Threat Assessment*, *supra* n. 9 at 12-13; *see also* Travers, *Global Terrorism*, *supra* n. 11 at 6 ("In Iran, the regime continues to use terrorism to threaten the United States, our allies, and other opponents, as well as to cement its long-term political influence throughout the Middle East. As we have observed in recent months from Tehran's attacks on international shipping and Saudi oil facilities, the regime is intent on escalating its efforts to intimidate and impose costs on its opponents, posing a growing direct and indirect threat to US interests and personnel….Iran can also call upon a wide-range of proxy groups to support its terrorist and regional influence operations… Iranian leaders also nurture these alliances in pursuit of long-term political advantage, similar to its decades-long partnership with Hizballah, which wields significant political influence within Lebanon and possesses a formidable military force including thousands of rockets.")

[19] *See, e.g.*, Gen (ret.) Keith B. Alexander & Jamil N. Jaffer, *Iran's Coming Response: Increased Terrorism and Cyber Attacks?*, The Hill (May 15, 2019) *available online at* <https://thehill.com/opinion/national-security/443610-irans-coming-response-increased-terrorism-and-cyber-attacks >.

[20] *See* Coats, *Worldwide Threat Assessment*, *supra* n. 9 at 12.

[21] *See* Travers, *Global Terrorism*, *supra* n. 11 at 6.

[22] *See* Gen. (ret.) Keith B. Alexander & Jamil N. Jaffer, *Only a Serious Response Will Reverse Iran's Growing Aggression*, The Hill (Oct. 3, 2019) *available online at* <https://thehill.com/opinion/national-security/463758-only-a-serious-response-will-reverse-irans-growing-aggression>.

[23] *See, e.g.*, Jeffrey Gettleman, et al., *Sri Lanka Was Warned of Possible Attacks. Why Didn't It Stop Them?*, New York Times (Apr. 22, 2019) *available online at* <https://www.nytimes.com/2019/04/22/world/asia/ntj-warning-sri-lanka-government.html>.

[24] *Id*.

[25] See Coats, *Worldwide Threat Assessment*, *supra* n. 9 at 13.

against Americans and our allies around the world.[26] Indeed, NCTC Director Travers recently noted that the Intelligence Community assesses that "the most predominant terrorist threat to the Homeland [] emanate[s] from US-based lone actors" that are self-radicalized through religious zealotry, as well by racial and ethnic hatred.[27]

III. The Need for Strong Intelligence Collection on Terrorism

What all of this tells us—or at least what it ought to tell us—is that as a nation, the United States cannot and should not, absent some significantly compelling reason, voluntarily take action to limit the ability of our intelligence, military, and law enforcement organizations to collect intelligence and take action to defeat these terrorist groups. And when it comes to some of the specific authorities currently under consideration by this Committee for reauthorization, like the lone wolf authority, roving wiretaps, and the "business records" authority—apart from the CDR program—the current threat environment counsels strongly in favor not just of reauthorizing those provisions, but making them permanent.

A. Lone Wolf Authority

The lone wolf authority itself is instructive. This provision, enacted as part of the authorities put in place in IRTPA back in 2004, permits the Foreign Intelligence Surveillance Court (FISC) to "authorize surveillance of non-United States persons engaged in international terrorism or the international proliferation of weapons of mass destruction, without the need to show that the target is acting on behalf of a particular terrorist group or other foreign power."[28] This authority, which only applies non-U.S. persons (i.e., not American citizens or lawful permanent residents) engaged in or preparing to engage in "international terrorism," a term defined by statute, has never been used in the decade and a half it has been on the books.[29]

Nonetheless, the lone wolf provision remains a critical authority in the modern era because it permits the surveillance of non-Americans who: (1) self-radicalize over the Internet; (2) are inspired, but not directed by a terrorist group; or (3) foreswear a particular terrorist group while nonetheless continuing to plot terrorist attacks against the United States.[30] Given that the number one terrorist threat today, in the view of the U.S. Intelligence Community, is from U.S.-based lone wolf actors,[31] allowing this authority to lapse (or continuing to be subject to periodic recertification) could significantly harm our national security.

---

[26] *See* Travers, *Global Terrorism*, *supra* n. 11 at 2 ("[H]igh profile attacks in the United States and abroad—most notably the March attacks against mosques in Christchurch, New Zealand and the August attack in El Paso, TX —highlight that the US is facing threats from a broader range of terrorist actors, to include violent extremists motivated by racial and ethnic hatred. While primarily a lone actor threat, these violent extremists in the US and abroad are deftly using technology to recruit others to their extreme ideology.").

[27] *Id*. at 1.

[28] *See Joint Statement for the Record*, *supra* n. 2 at 5.

[29] *Id*. at 5-6.

[30] Id. at 6.

[31] *See* Travers, *Global Terrorism*, *supra* n. 11 at 1-2.

B. Roving Wiretap Authority

Similarly, the roving wiretap authority ought be a fairly easy matter for this Committee to consider. This authority—which was put in place in the immediate aftermath of the 9/11 attacks—permits the government, subject to demonstrating that it has a specific need, to obtain a surveillance order from the FISC that can be served on multiple providers without the need to return to the court beforehand. Such orders are used to follow a sophisticated foreign intelligence officers or terrorism targets who seek to actively evade surveillance by rapidly switching phone numbers, email addresses, or service providers (or some combination thereof).[32] This is not to suggest the government's efforts to follow a target under such an order goes without review: to the contrary, not only must the government first demonstrate to the court that the "target's actions may have the effect of thwarting surveillance" but also, after it uses the roving authority, the government must typically return to the court within 10 days to demonstrate that it has the required probable cause to target the new facility.[33] This authority—which mirrors authorities that have long been available in criminal context (for more than three decades) and has been repeatedly upheld in the courts—is only used in a relatively small number of cases every year, and typically is used to deal with foreign intelligence officers who are trained to evade surveillance through the use of tradecraft or terrorist operatives with similar patterns of behavior.[34] Given the fact that similar authority has long been permanently available in the criminal context and there has been no demonstrated abuses of this authority, nor any real controversy in the nearly 20 years that it has been in place, making this provision permanent seems like a reasonable next step for Congress to consider.

C. Section 215 Business Records and Tangible Things Authority

The same is largely true with respect Section 215's "business records" authority, which permits the FISC to issue court orders requiring third parties to provide business records and other tangible things relevant to an authorized national security investigation. This authority, while made controversial following Edward Snowden's illegal disclosure of highly classified material, including a FISA court order granting the government the authority to obtain bulk, non-content metadata from a telecommunications provider—today has been significantly limited by Congressional action and raises only limited

---

[32] *See Joint Statement for the Record*, *supra* n. 2 at 3("In an ordinary case, if [a FISA] target switches to a new communications service provider, the Government must submit a new application and obtain a new set of FISA orders. However, where the Government can demonstrate in advance to the FISA Court that the target's actions may have the effect of thwarting surveillance, such as by rapidly and repeatedly changing providers, FISA's roving wiretap provision allows the FISC to issue a generic secondary order that the Government can serve on the new provider to commence surveillance without first going back to the Court.").

[33] *Id*. ("The Government's probable cause showing that the target is an agent of a foreign power remains the same, and the Government must also demonstrate to the FISC, normally within 10 days of initiating surveillance of the new facility, probable cause that the specific target is using, or is about to use, the new facility.").

[34] *Id*. ("The authority outlined in this provision is similar to the roving wiretap authority that has been available since 1986 in criminal investigations, under the Wiretap Act, and which has repeatedly been upheld in the courts….The Government has used the authority in a relatively small number of cases each year. Those cases tend to involve highly-trained foreign intelligence officers operating within the United States, or other important investigative targets, including terrorism-related targets, who have shown a propensity to engage in activities deliberately designed to thwart surveillance. Similar authority designed to prevent suspects from thwarting surveillance has been a permanent part of our criminal law for over thirty years, and this provision has been renewed as part of FISA repeatedly since 2001 without controversy or evidence of abuse. It remains an important tool, and we strongly support permanent reauthorization.")

controversy.[35] The USA FREEDOM Act, as noted earlier, amended Section 215 to require the use of a specific selection term, specifically bar the bulk collection of data, and to permit the FISA court to impose additional minimization procedures to address concerns with the collection of particular data under this authority.[36] According to the government, the type of records obtained under this provision include things like "driver's license records, hotel records, car rental records, [and] apartment leasing records."[37]

Perhaps most relevant to the question whether Congress ought reauthorize this authority—and consider making it permanent—is the fact that this authority, like the roving wiretaps, has long been available in other investigations without any controversy and with significant less process and protections than those available in the national security context.[38] For example, in a criminal investigation, similar records and tangible things can obtained by the government through a grand jury subpoena issued solely by a prosecutor conducting the investigation; and likewise, in certain civil matters, an administrative subpoena may be issued by agency counsel in order to obtain similar records.[39] As compared to these authorities, the FISA "business records" provision is significantly more limited and protective of the rights of the third party and the underlying target. For example, under the FISA "business records" provision, not only must a court review and approve applications for the production of tangible things, but the statute also permits the individual or business receiving such an order to challenge the order (although, to date, no recipient has done so).[40]

While Section 215, to be fair, has generated some concern among privacy advocates even post-USA FREEDOM. For example, some have argued that Section 215 is too generous to the government in that it only requires the government only show relevance to an appropriate, authorized national security investigation, versus meeting the higher bar of probable cause under the Fourth Amendment.[41] However, the generally held view is that authorities like Section 215 (and grand jury and administrative subpoenas) are not subject to the Fourth Amendment's requirements because they do not constitute a search and

---

[35] *But cf*. Andrew Crocker, *Congress Has a Chance to Finally End the NSA's Mass Telephone Records Program*, Electronic Frontier Foundation (Mar. 21, 2019), *available online at* <https://www.eff.org/deeplinks/2019/03/congress-has-chance-finally-end-nsas-mass-telephone-records-program> ("Finally, it's reasonable to wonder what happens if our legislative and executive branches fail to act before Section 215 sunsets at the end of this year. In that case, the law would revert to a pre-Patriot Act provision from 1998, which allowed the government to collect only a narrow range of business records (not communications records) only from a limited set of companies such as transportation common carriers and other lodging, storage and vehicle facilities, and only if it could make the specific showing that the records belonged to an 'agent of a foreign power.' The government might argue that this would be 'throwing the baby out with the bathwater.' But any surveillance law needs to be justified on its own terms, and the intelligence community would still have many other powers at its disposal.")

[36] *Id*. at 4-5.

[37] *Id*. at 4.

[38] *Id*. ("[T]he records the Government is authorized to obtain—pursuant to a FISC order—are similar to those that the Government could obtain in ordinary criminal or civil investigations—without any court order in most instances—pursuant to a grand jury subpoena in an ordinary criminal case, or pursuant to an administrative subpoena in a civil case. Like a grand jury subpoena or an administrative subpoena, a business records order merely requires the recipient to identify and produce responsive records or other tangible things.")

[39] *Id*.

[40] *Id*.

[41] *Id*.

seizure.[42] As with the other two authorities discussed thus far, the absence of demonstrated abuse of this authority and the absence any major new criticisms of this authority since the USA FREEDOM Act was enacted over four years, as well as the fact that this authority mirrors long-standing criminal and civil authorities ought counsel strongly in favor of reauthorization and full consideration by the Committee of making this critically important authority permanent.

D. Call Data Records Authority

Finally, we turn to the key authority that has been at the heart of the reauthorization debate during this Congress: the Call Data Records provision put in place by the USA FREEDOM Act. The debate over reauthorization of the CDR provision has generally focused on whether: (1) NSA's decision to voluntarily cease its collection of data under this authority; or (2) the perceived lack of value of the program, are significant enough reasons for Congress to take away this key authority.[43] The view that the CDR provision ought be allowed to expire is not a fringe position, as it is supported by nearly 40 privacy and civil liberties groups from across the political and ideological spectrum, including the American Civil Liberties Union (ACLU), Americans for Prosperity (AFP), Center for Democracy and Technology (CDT), Electronic Frontier Foundation (EFF), FreedomWorks, NAACP, New America's Open Technology Institute, and TechFreedom.[44] And it has garnered the support of a bipartisan, bicameral group of Members of Congress who introduced legislation in March of this year to terminate the CDR authority.[45]

And yet, this view, while not a fringe position, is wrong. The fact is that the government's collection of metadata under Section 215 was conducted under for over a decade under court-approved orders, sought by Presidents of both parties, authorized dozens of times by multiple federal district court judges sitting on FISC, and carried out under very close oversight by various inspectors generals and the watchful eye of the FISC judges themselves. To be sure, along the way, there were compliance incidents with the 215 program, but each and every one of those incidents was unintentional, were caught by the intelligence community itself, self-reported to the FISC, and were the subject of extensive back-and-forth efforts between the intelligence collectors, the Justice Department, and the FISC to correct the issues and to ensure the full and appropriate protection of the privacy and civil liberties of all Americans.[46] And

---

[42] *Id*. ("[A]n order issued under the business records provision does not authorize the Government to enter premises, or to search for or seize records or other tangible things. Thus, the Fourth Amendment's probable cause standard generally does not apply.…Like a grand jury subpoena or an administrative subpoena, a business records order merely requires the recipient to identify and produce responsive records or other tangible things.").

[43] *See, e.g.*, Sharon Bradford Franklin, *Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records*, Just Security (Mar. 28, 2019), available online at <https://www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records/>.

[44] *See, e.g.*, ACLU, et al., *Coalition Letter on Reauthorization of Patriot Act's Section 215* (Mar. 18, 2019), *available online at* <https://www.aclu.org/letter/coalition-letter-reuthorization-patriot-acts-section-215>.

[45] *See* Press Release, *Wyden, Paul, Amash and Lofgren Introduce Bipartisan Bill to Permanently End Mass NSA Surveillance of Phone Records* (Mar. 28, 2019), available online at <https://www.wyden.senate.gov/news/press-releases/wyden-paul-amash-and-lofgren-introduce-bipartisan-bill-to-permanently-end-mass-nsa-surveillance-of-phone-records->.

[46] *See, e.g.*, Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program*

ultimately, each of these issues was resolved and the program was permitted to continue forward consistent with the law.

It is also worth noting that while the scope of the metadata collection under the pre-USA Freedom Act was massive, the actual scope of the number of queries against that collection was fairly small. So, for example in 2012, the number of seed numbers utilized to query the database was only 288.[47] Similarly, in 2013 and 2014, the number of selectors approved for queries was 423 and 161, respectively.[48] And as the transition to the USA FREEDOM Act began, the number of selectors queried began to drop also, with the first year, 2015, coming in at 56 targets, a number that continued to decrease into 2018, with the number of targets down to 42, 40, and 11, during the period 2016-18, respectively.

To be sure, the nature of the program, pulling multiple hops of data from individual seed numbers, increases the quantity of records implicated by orders of magnitude, thereby also significantly increasing the potential impact of the program on non-targeted individuals. However, it is worth keeping in mind the specific type of data at issue here: when it comes to the CDR program, what is being collected is not the content of communications, but rather artifacts *about* a communication or what is known as a "call event metadata."[49] So, for example, in the context of a telephone call, what is typically being collected is the number initiating a call, the number being called, and the date, time, and duration of the call.[50] No information about the location where the call is being initiated from, the individual subscriber who owns the telephone number, nor the content of the communication may be obtained under this authority.[51] And so, while the sheer quantity of data being collected may be large—particularly under the pre-USA FREEDOM program—the nature of the data is fairly limited from a privacy perspective, at least as far as communications intelligence collection goes. Indeed, without much context as to whom the numbers belong to or where they are calling from, the most you can tell from such a program is essentially the

---

Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, Annex A: Separate Statement by Board Member Rachel Brand at 212, n.692 (Jan. 23, 2014), available online at <https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf >.

[47] *See* Steve Inskeep, *Interview with Chris Inglis: NSA Says It Would Welcome Public Advocate at FISA Court*, National Public Radio (Jan. 4, 2014), available online at <https://www.npr.org/sections/thetwo-way/2014/01/09/261079074/nsa-says-it-would-welcome-public-advocate-at-fisa-court>.

[48] *See* Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2013* (June 26, 2014), *available online at* <https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013>; Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2014* at 4 (Apr. 22, 2014), *available online at* <https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014>.

[49] *See, e.g.*, Office of the Director of National Intelligence, *Statistical Transparency Report Regarding the Use of National Security Authorities – Calendar Year 2018* (April 2019) available online at <https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf> ("Call Detail Records (CDRs)—commonly referred to as "call event metadata"—may be obtained from telecommunications providers on an ongoing basis []. Title V of FISA defines a CDR as session identifying information (such as an originating or terminating telephone number, an International Mobile Subscriber Identity (IMSI) number, or an International Mobile Station Equipment Identity (IMEI) number), a telephone calling card number, or the time or duration of a call. [] By statute, CDRs provided to the government may not include the content of any communication, the name, address, or financial information of a subscriber or customer, or cell site location or global positioning system information.")

[50] *Id*.

[51] *Id*.

calling circles of each phone.

In many ways, using this form of communications intelligence can actually be quite privacy enhancing. For example, investigators might utilize this capability to focus their limited investigative resources on the key communicants, thereby eliminate many potential targets of full-content surveillance simply based metadata collection. That is, if an investigator has a potential pool of suspects that that the they believe are associated with a given known terrorist, if the investigator is able to determine that a only handful of those potential suspects were in regular communication with the known terrorist's phone number, while the vast majority of the suspects were not, the investigator now has a good basis for focusing content collection request on the handful, all the while quickly and efficiently eliminating the vast majority of the potential targets. Indeed, when one combines the number of actual targeted queries of the Section 215 database with the fact that the information collected and analyzed is fairly limited, the idea that this program has resulted some massive invasion of privacy and civil liberties of Americans is simply belied by the record.[52] Indeed, one might reasonably argue that the use of the metadata to identify and include or exclude potential targets of further surveillance may be one of the least intrusive investigative methods available to the intelligence community and, as such, ought be retained and utilized for that purpose as necessary.

At the same time, one might also argue that the mere fact of the collection and retention by the government of a massive amount of data under the program as it existed before the USA FREEDOM Act raises reasonable concerns about how that data might be utilized or even abused by the government. The fact of the matter, however, is that the historical record—going back nearly two decades—is completely devoid of any legitimate claim of intentional misuse or abuse by the government.[53] To the contrary, as noted above, to the extent there were compliance issues—and there were some significant ones, to be fair—they were all unintentional, self-caught, self-reported, and ultimately corrected by the Executive

---

[52] *See supra* ns. 48-51.

[53] *See, e.g.*, 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* at 9-10 (Jan. 23, 2014) *available online at* <https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf> ("Over the years, a series of compliance issues were brought to the attention of the FISA court by the government. However, none of these compliance issues involved significant intentional misuse of the system. Nor has the Board seen any evidence of bad faith or misconduct on the part of any government officials or agents involved with the program. Rather, the compliance issues were recognized by the FISC — and are recognized by the Board — as a product of the program's technological complexity and vast scope, illustrating the risks inherent in such a program."); see also President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* at 76 (Dec. 12, 2013) *available online at* <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> ("Significantly, and in stark contrast to the pre-FISA era, the Review Group found no evidence of illegality or other abuse of authority for the purpose of targeting domestic political activity."); *see also* Brand, *Separate Statement*, *supra* n. 46, at 212, n. 662 ("As the Board discusses, there have been lapses in compliance with the program's limitations. Most of these violations have been minor and technical. A few have been significant, though apparently unintentional. Compliance problems are always a matter of concern and demonstrate the need for robust oversight. But it is important to remember that the lapses the Board mentions came to light only because the government self-reported violations to the FISC. Those problems were then corrected, under the supervision of the FISC. And these corrective measures and self-reporting occurred before these programs were publicly disclosed. That is, they were identified and fixed not because of the scrutiny brought about by an unlawful leak of classified information, but because existing oversight mechanisms worked.")

Branch.[54]

Moreover, the reality is that not much changed after the implementation of the USA FREEDOM Act, except that: (1) it became harder for the government to get access to the underlying data, because it now had to go to multiple providers to obtain a single series of chained calls; (2) it made the program less effective because the scope of records available to the government became subject to provider decision-making with respect to how much data, if any, they would retain; and (3) it became quite difficult, if not impossible, for the government to correct collection errors—the way it had in the past—because it now relies on the providers to give the government the requested data. And it is this last point that leads to the question of how member of this Committee might think about the NSA's recent decision to terminate the CDR program and why the government nonetheless seeks to retain the authority to restart this program as needed.

If we look at the public record with respect to the challenges that NSA faced on Section 215 in mid-2018, it becomes clear that the challenge was less on NSA's end and more on the *providers* who were supplying the information to NSA under the USA FREEDOM Act. Specifically, at some point in early 2018, NSA analysts "noted technical irregularities in some data *received from telecommunications service providers*….[which] resulted in the production to NSA of some CDRs that NSA was not authorized to receive."[55] And because NSA was unable to "identify and isolate properly produced data," NSA determined that it should not use any of the CDRs and decided, after consulting with DOJ and ODNI, to delete the data.[56] Later descriptions of what followed, and what led to the ultimate decision to terminate the program are likewise instructive: the former DNI, in informing Congress of the Intelligence Community's view that the CDR program and other expiring authorities ought be renewed and made permanent, noted that a key factor informing whether to continue the CDR program was presence of "compliance and data integrity concerns caused by the unique complexities of using these company-generated business records for intelligence purposes."[57] This statement appears to make clear that NSA was not only concerned that the data being provided by the carriers may not have met the legal requirements but also that the data itself may not have been valid for use in intelligence investigations, and that this problem arose in part because of the use of company-generated data.

If this reading of the historical record is correct, then one might wonder whether NSA would have been able to more effectively correct the data issues going forward—as it had done a number of times before when confronted with compliance issues—had it not been mandated, by statute, to not collect and house the data itself. Given this open question—as well the unanimous view of the intelligence professionals before the Committee today that this program ought be reauthorized—Committee may wish to consider providing NSA and ODNI with options under which they might restart the program and provide potential pilot opportunities for NSA to explore how it might collect data in a way that avoids these problems.

---

[54] *Id.*

[55] *See* National Security Agency, *NSA Reports Data Deletion*, *supra* n. 4, at 1 (emphasis added).

[56] *Id*.

[57] *See DNI Coats Letter*, *supra* n. 2 at 1.

IV. Options and Potential Additional Reforms for Consideration

The Committee may wish to consider the following options and potential reforms as it looks to act in the near future on reauthorization of the expiring authorities:

1. With respect to the CDR program, the Committee may wish to consider retaining the existing authority and structure for the program, while requiring NSA to report back to Congress before it restarts the program and to provide the Committee with a detailed explanation of how it intends to meet the statutory requirements going forward.

2. The Committee may also wish to permit NSA to run a short-term pilot CDR program where it once again takes on its pre-USA FREEDOM role of holding a significant subset of the data it needs to do its work—perhaps in a new technology area—to see whether taking on the data itself allows NSA to mitigate the compliance and data integrity issues it experienced under the carrier-based system required by the USA FREEDOM Act.

3. With respect to additional transparency measures, the Committee might consider requiring the FISC to publish a classified and unclassified reporter of all of its opinions, with the latter version redacted to protect sources and methods of intelligence collection, as well as information about the targets of collection, in consultation with the Office of the Director of National Intelligence. Such a reporter would serve to better inform government officials, the government and private sector legal community, and the public about the work of the court and the legal analysis it applies to the issues that come before it in both the classified and unclassified settings.

4. In order to address potential concerns about the ability of the judges of the FISC to operate independently and to keep up with the work of the court from their home districts, the Committee may wish to consider providing the judges of the FISC with direct, regular access to opinions that are issued by their colleagues while in their home districts, either through access in a secure compartmented information facility at the local federal courthouse or at another appropriate government facility in the area.

5. In parallel, the Committee may also wish to consider providing resources to the Administrative Office of the U.S. Courts to ensure that each judge of the FISC has a fully-cleared, term law clerk to assist the judge with their FISA caseload, both while in their home districts as well as while in the Washington area for FISC hearings. If the Committee decides to undertake this reform, the Committee may wish to consider whether the FISC's legal advisors continue to be necessary.

This short list of ideas represents but a partial starting point for Committee to consider as it proceeds forward with the reauthorization process.

Thank you for offering me the opportunity to participate in this important dialogue. I look forward to your questions.