2020

Examining the Anomalies, Explaining the Value: Should the USA FREEDOM Act's Metadata Program be Extended?

Susan Landau

Asaf Lubin

ARTICLE

Examining the Anomalies, Explaining the Value: Should the USA FREEDOM Act's Metadata Program be Extended?

Susan Landau and Asaf Lubin*

* Susan Landau, Bridge Professor in Cyber Security and Policy, Fletcher School of Law & Diplomacy and School of Engineering, Department of Computer Science, Tufts University. Asaf Lubin, Affiliate at the Berkman Klein Center for Internet and Society and a Visiting Fellow at the Information Society Project at Yale Law School; the work was done while Lubin was a Cybersecurity Policy Postdoctoral Research Fellow, Fletcher School of Law and Diplomacy, Tufts University. This research was supported in part by funding from the William and Flora Hewlett Foundation under grant 2018-7277. We greatly appreciate the help provided by Steven M. Bellovin, Matt Blaze, Fred Cate, George Croner, David Crowe, Yves-Alexandre de Montjoye, Tom La Porta, Caroline Lynch, Rebecca "Becky" Richards, and Patrick Traynor. We also thank Anne Boustead, Bryan Cunningham, Jim Dempsey, Sharon Bradford Franklin, Amy Gaudion, Jennifer Grannick, Riana Pffeferkorn, Stuart Shapiro, Robert Sloan, and other participants of the 2019 Annual Privacy Law Scholars Conference for useful comments on an earlier draft.

Abstract

Edward Snowden's disclosure of National Security Agency ("NSA") bulk collection of communications metadata was a highly disturbing shock to the American public. The intelligence community was surprised by the response, as it had largely not anticipated a strong negative public reaction to this surveillance program. Controversy over the bulk metadata collection led to the 2015 passage of the USA FREEDOM Act. The law mandated that the intelligence community would collect the Call Detail Records ("CDR") from telephone service providers in strictly limited ways, not in bulk, and only under order from the Foreign Intelligence Surveillance Court. The new program initially seemed to be working well, although the fact that from 40 court orders in both 2016 and 2017, the NSA collected hundreds of millions of CDRs created public concern. Then in June 2018 the NSA announced it had purged three years' worth of CDRs due to "technical irregularities"; later the agency made clear that it would not seek the program's renewal.

This Article demystifies these situations, analyzing how forty orders might lead to the collection of several million CDRs and providing the first explanation that fits the facts of what might have caused the "technical irregularities" leading to the purge of records. This Article also exposes a rather remarkable lacuna in Congressional oversight: even at the time of the passage of the USA FREEDOM Act a changing terrorist threat environment and changing communications technologies had effectively eliminated value of the CDR collection. We conclude with recommendations on conducting intelligence oversight.

Table of Contents

Introduction

The first of Edward Snowden's disclosures was a Foreign Intelligence Surveillance Court ("FISC") order requiring that Verizon provide the National Security Agency ("NSA") with daily Call Detail Records ("CDRs") for all communications to, from, or within the United States.[1] The order, based on a FISC interpretation of Section 215 of the USA PATRIOT Act of 2001, required Verizon to release all call routing information, including session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity ("IMSI") number, International Mobile station Equipment Identity ("IMEI) number"), trunk identifiers, telephone calling card numbers, and time and duration of calls.[2] The Snowden disclosures and the public controversy that followed led Congress in 2015 to end bulk collection and amend the CDR authorities with the adoption of the USA FREEDOM Act.[3]

The bulk collection program was introduced in 2001 after a failure to recognize that an intercepted call occurred between an Al-Qaeda safe house in Sana, Yemen and a U.S. number.[4] But since then the terrorist threat had changed from a highly centralized, almost corporate structure to a more diffuse recruitment effort exemplified by ISIS. Communication technologies also changed. Both in the United States and around the world, there was a shift from wireline phones to mobiles to smartphones, and phone calls to Internet Protocol ("IP")-based applications. When terrorists use mobile phones for communication, it is for IP-based communications, not for phone calls or short message service ("SMS") texts.

These changes transformed the value of investigative tools provided under the Foreign Intelligence Surveillance Act ("FISA"). Collection of IP-based communications is conducted not under Section 215, but under FISA Section 702, which enables the Intelligence Community ("IC") to target communications of non-U.S. persons reasonably believed to be located outside the United States.[5] Section 702 has become pivotal in tracking and preventing terrorist plots against the United States while the value of Section 215 collection has waned.

---

[1] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/F7BT-SQSZ].

[2] Order at 2, In re Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services Inc. on Behalf of MCI Communication Services, Inc. D/B/A Verizon Business Services, No. BR 13-80 (FISA Ct. Apr. 25, 2013).

[3] Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring (USA FREEDOM) Act, Pub. L. No. 114-23, 129 Stat. 268 (2015).

[4] *See* DOES STATE SPYING MAKE US SAFER?: THE MUNK DEBATE ON MASS SURVEILLANCE 25 (Rudyard Griffiths ed., 2014).

[5] Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 120–21 (2015).

While controversy surrounded the USA FREEDOM Act's passage in 2015, all appeared fine afterwards. Then in June 2018, NSA announced that it had found "technical irregularities" in the CDRs being provided by the telecommunications providers under USA FREEDOM Act[6] and deleted three years' worth of records collected under the program.[7] More was to come. In March 2019, the *Washington Post* disclosed that the NSA had halted collection since at least September 2018;[8] the *Wall Street Journal* reported that the NSA recommended not seeking the program's renewal.[9]

This Article explains why. This Article also explains the high number of CDRs collected under USA FREEDOM Act in 2016, 2017, and 2018, and possible reasons for the purge. This Article also shows how changes in technology and communication methods and the foreign-terrorist threat have sharply lessened the value of the CDR program and made its use largely unnecessary.

Section I begins this Article with a brief history of NSA's telephony metadata and Section 702 programs and the foreign-terrorist threat. Section II examines the few orders for collection of CDRs, but seemingly disproportionately large number of CDRs collected, and the June 2018 purge of three years of collected CDRs. The analysis in this Article, based on the technical aspects of collection, goes a good way towards explaining the reasons behind these. This should move the discussion from concerns regarding overcollection to questions over the program's efficacy—which is where the focus properly belongs. Section III demonstrates how terrorists' utilization of IP-based communications has made the metadata program far less beneficial. Section IV probes Congress's failure to carefully examine the efficacy of the CDR program prior to USA FREEDOM Act's adoption in 2015 and examines what Congress should do. Section V provides a brief conclusion.

The value of investigative tools changes with time and circumstances. While almost all investigative tools can, on occasion, uncover some unknown information, it makes little sense to deploy surveillance tools when they cease to be efficacious. Focusing on Section 215 collection, this Article shows how the program lost usefulness, illuminating the need to carry out efficacy analyses on a

---

[6] *NSA Reports Data Deletion*, IC ON THE RECORD (June 28, 2018), http://icontherecord.tumblr.com/post/175347073998/nsa-reports-data-deletion-june-28-2018 [https://perma.cc/X3DT-F68T].

[7] Charlie Savage, *N.S.A. Purges Hundreds of Millions of Call and Text Records*, N.Y. TIMES (June 29, 2018), https://www.nytimes.com/2018/06/29/us/politics/nsa-call-records-purged.html [https://perma.cc/X9KZ-RHQN].

[8] *See* Ellen Nakashima, *NSA Has Halted a Counterterrorism Program Relying on Phone Records Amid Doubts About its Utility*, WASH. POST (Mar. 5, 2019), https://www.washingtonpost.com/world/national-security/nsa-has-halted-a-counterterrorism-program-relying-on-phone-records-amid-doubts-about-its-utility/2019/03/05/f2d2793e-3f80-11e9-922c-64d6b7840b82_story.html [https://perma.cc/LZP2-L8ZJ].

[9] *See* Dustin Volz & Warren P. Strobel, *NSA Recommends Dropping Phone Surveillance Program*, WALL ST. J. (Apr. 24, 2019), https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247 [https://perma.cc/538R-SRSK].

continuing basis. Collection costs time and resources; increasing the size of the haystack may make it more difficult to find the needle.[10] Collecting all possible data does not necessarily make us safer.

I. The History of NSA's Bulk Collection Programs

A. *The History of the Telephony Metadata Program*

In the lead up to the September 11 attacks, there was a failure to follow up on crucial pieces of evidence that, properly studied, might have prevented those attacks. This included calls made by Mawaf al-Hazmi and Khalid al-Mihdhar (two of Bin-Laden's muscle men personally picked to carry out the 9/11 attack on the Pentagon) to a Yemeni number connected to a safe house for bin Laden's operations.[11] The calls were made from an apartment in San Diego, California.[12] NSA was listening in to the Yemeni end of the call, which was over a satellite phone.[13] Eavesdroppers to satellite calls typically overhear only one end of the communication. Without access to the switch or CDR, NSA did not learn the location of the other end of the call until it was too late.[14]

That was not the only failure. Analysts understood that spectacular attacks were being planned, but as the 9/11 Commission later put it: "When reports did not specify where the attacks were to take place, officials presumed that they would again be overseas."[15] Searching for the communication's other end was thus not a high priority for U.S. signals intelligence. Even if it had been, it is not clear that NSA would have been able to determine the call's origin. As former NSA Director Michael Hayden later noted, "[i]f we had the 215 program at the time, we would have thrown that selector at that mass of American phone bills and phone connection and said, 'Did anybody here talk to this number in Yemen?' and ka-jink! The San Diego number would have popped up."[16]

On October 4, 2001, President George W. Bush directed the Secretary of Defense to undertake a program of collection of telephone and Internet

---

[10] *See* NAT'L RESEARCH COUNCIL, BULK COLLECTION OF SIGNALS INTELLIGENCE: TECHNICAL OPTIONS 54 (2015) [hereinafter National Research Council's Bulk SIGINT Collection Report].
[11] MATTHEW AID, THE SECRET SENTRY: THE UNTOLD HISTORY OF THE NATIONAL SECURITY AGENCY 209–11 (2009).
[12] DOES STATE SPYING MAKE US SAFER: THE MUNK DEBATE ON MASS SURVEILLANCE 25 (Rudyard Griffiths ed., 2014).
[13] The safe house and phone are described in JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING OF AMERICA 7–8 (2008).
[14] DOES STATE SPYING MAKE US SAFER, *supra* note 12, at 25–26.
[15] THE 9/11 COMM'N, FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 257, 263 (2004).
[16] *See Statement for the Record of Robert S. Mueller III, Dir., Fed. Bureau of Investigation, Before the Senate Select Comm. on Intelligence*, FEDERATION OF AMERICAN SCIENTISTS (Feb. 24, 2004), https://fas.org/irp/congress/2003_hr/021103mueller.html [https://perma.cc/3G5L-9CR2]; DOES STATE SPYING MAKE US SAFER, *supra* note 12, at 25–26.

communications, known as STELLAR WIND.[17] The presidential authorization was renewed for over six years, allowing warrantless surveillance of the metadata of American citizens' telephone and email communications, financial transactions, and Internet activity and, under certain restrictions, the content of those communications and transactions.[18]

In December 2005, the *New York Times* broke a story about the warrantless wiretapping program.[19] One telecommunications operator then expressed concern to the government about providing telephony metadata "under Presidential Authority" rather than under court order.[20] The administration moved to change this and in May 2006—as it happened, thirteen days after *USA Today* exposed the existence of the bulk metadata collection program—the FISC signed the first order placing STELLAR WIND's telephony metadata collection under FISA's authorities.[21]

The court relied on an interpretation of the USA PATRIOT Act, which amended FISA Section 501. The original section permitted access under court order to "business records" held by common carriers in the context of foreign intelligence or international terrorism investigations. The amended act allowed the court to compel the production of "any tangible things including books, records, papers, documents, and other items"[22] when necessary for an authorized investigation "against international terrorism or clandestine intelligence activities."[23] To allow for STELLAR WIND's mass collection of communications metadata to be brought

---

[17] *See* OFFICES OF INSPECTORS GEN. OF THE DEP'T OF DEF., ET AL., No. 2009-0013-A, REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 1 (2009), https://oig.justice.gov/reports/2015/PSP-09-18-15-full.pdf [https://perma.cc/QNQ4-BZL8] [hereinafter DOJ Inspector General's 2009 Report].

[18] *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 16 (2014), https://www.pclob.gov/library/702-Report.pdf [https://perma.cc/6CUK-5J3W] [hereinafter PCLOB Section 702 Report].

[19] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Calls Without Orders*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html [https://perma.cc/U54W-R4RW].

[20] OFF. OF THE INSPECTOR GEN. OF THE NAT'L SEC. AGENCY, ST-09-0002, REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, WORKING DRAFT 39–40 (Mar. 24, 2009), https://www.emptywheel.net/wp-content/uploads/2013/06/090324-Draft-NSA-IG-Report.pdf [https://perma.cc/6CCQ-GB8B] (noting comments by NSA General Counsel Vito Potenza that the decision to transition the telephony metadata program to the Business Records provision was due to a private sector company reacting to the *New York Times* story) [hereinafter 2009 NSA Inspector General's PSP Working Draft Report]. This section did not appear in the published version of the report. *See* DOJ Inspector General's 2009 Report, *supra* note 17, at 54–55.

[21] Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at A1.

[22] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861(a)(1)).

[23] Congress amended the authority in 2006 further requiring that there be "reasonable grounds to believe that the tangible objects sought are relevant." USA PATRIOT Act Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106, 120 Stat. 196 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

under Section 215, the FISC adopted an expansive interpretation of "relevant" encompassing non-targeted forms of collection.[24]

Beginning on May 24, 2006, the FISC issued quarterly orders to some U.S. telephone companies directing them to provide NSA with all CDRs "on an ongoing daily basis to the extent practicable."[25]

Only after the Snowden disclosures did the government publicly acknowledge the program. NSA Director Keith Alexander testified to the House Intelligence Committee that information gathered from the Section 215 program provided the U.S. government with "critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world."[26] He later cited 54 cases in which the NSA bulk collection programs "contributed to our understanding, and in many cases helped enable the disruption of terrorist plots."[27] But in December 2013, Director Alexander spoke of only eight events in which Section 215 played a role in disrupting terrorist activity.[28] In 2014, the Privacy and Civil Liberties Oversight Board concluded that the bulk metadata program was useful domestically only once in identifying a previously unknown terrorist suspect (Basaaly Moalin, who materially supported Al-Shabaab, an extremist Somali militia with al-Qaeda ties).[29]

---

[24] *See* Robert Chesney, *Telephony Metadata: Is the Contact-Chaining Program Unsalvageable?*, LAWFARE (Mar. 6, 2019), https://www.lawfareblog.com/telephony-metadata-contact-chaining-program-unsalvageable [https://perma.cc/L7AX-YVAF].

[25] Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism, In re Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 06-05 (FISA Ct. May 23, 2006).

[26] *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids our Adversaries: Hearing Before the H. Permanent Select Comm. On Intelligence*, 113th Cong. (2013), https://www.intel.gov/index.php/ic-on-the-record-database/results/43-hearing-of-the-house-permanent-select-committee-on-intelligence-on-how-disclosed-nsa-programs-protect-americans,-and-why-disclosure-aids-our-adversaries [https://perma.cc/MSD2-NC86].

[27] Gen. Keith Alexander, Remarks at the AFCEA International Cyber Symposium (June 28, 2013), https://www.nsa.gov/news-features/speeches-testimonies/Article/1620137/remarks-by-gen-keith-alexander-commander-us-cyber-command-uscybercom-director-n/ [https://perma.cc/TVB4-LDEG].

[28] *Continued Oversight of U.S. Government Surveillance Authorities: Hearing Before the S. Judiciary Comm.*, 113th Cong. 25 (2013).

[29] 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 152–53 (2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf [https://perma.cc/TGY3-F9AV] [hereinafter PCLOB Section 215 Report]. In August 2016, David Anderson, the Independent Reviewer of Terrorism Legislation, reported to the U.K. Parliament on bulk surveillance powers, making the case for the utility of metadata collection programs. Anderson clarified that his finding should not cast doubt on PCLOB's conclusions. There are differences between the Section 215 program and the U.K. authorities, which covers all metadata, not just calls and texts; there are also different terrorism threats facing the United Kingdom and the United States, resulting in a different scale of use. *See* DAVID ANDERSON, Q.C., REPORT OF THE BULK POWERS REVIEW, 2016, Cm. 9326, ¶ 3.50-3.54 (UK),

While the program failed to identify new terrorist suspects or disrupt ongoing terrorist plots, it assisted in triaging in time-sensitive cases, corroborated existing evidence, and allowed for "negative reporting," enabling investigators to focus resources where needed.[30] CDRs were useful in establishing links between suspects and also enabled going "backwards in time," allowing intelligence analysts to study past history of a newly discovered suspect.[31]

Implementing the Section 215 metadata collection program was problematic, however, and problems with the technology resulted in compliance issues in 2006–09.[32] NSA operators had inadvertently violated the FISC's orders, a situation that Director of National Intelligence James Clapper would later describe as a case in which NSA and the FISC simply lacked a shared understanding of how the complex program worked.[33] Repeated compliance issues and misrepresentations resulted in the FISC suspending the program for roughly six months in 2009.[34]

After the Snowden disclosures, President Obama appointed a five-person review committee that studied various aspects of the exposed NSA surveillance programs, concluding that the CDR program should be abandoned.[35] The Privacy and Civil Liberties Oversight Board similarly observed that the program raised serious threats to privacy and civil liberties while showing "only limited value" and should thus come to an end.[36] A 2015 National Academies study determined that there were no technical alternatives that would produce the same information.[37] Meanwhile, ACLU, other civil liberties organizations, and individuals filed

---

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546923/56730_Cm_9326_PRINT.PDF [https://perma.cc/34ZF-ZTMH].

[30] Information collected in this way may also "rule out" a suspect by showing that the number is actually that of a non-suspect (e.g. car mechanic or IT help desk) and thus not worth further investigative time. *See* National Research Council's Bulk SIGINT Collection Report, *supra* note 10, at 42–43.

[31] National Research Council's Bulk SIGINT Collection Report, *supra* note 10, at 51.

[32] For a complete summary of all compliance issues, see Marcy Wheeler, *"Institutional Lack of Candor": A Primer on Recent Unauthorized Activity by the Intelligence Community*, DEMAND PROGRESS (2017), https://s3.amazonaws.com/demandprogress/reports/Institutional_Lack_of_Candor.pdf [https://perma.cc/PX6T-5VJ9].

[33] Press Release, Off. of Dir. Nat'l Intelligence, DNI Clapper Declassified Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (FISA) (Sep. 10, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/927-dni-clapper-declassifies-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act-fisa [https://perma.cc/57HJ-LP8D].

[34] The NSA querying of the bulk CDR collection was halted on March 2, 2009 after the FISC became aware of problems with compliance. *See* In re Production of Tangible Things From [redacted], No. BR 08-13 (FISA Ct. Mar. 2, 2009) (reinstated on September 3, 2009); *see also* In re Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things From [redacted], No. BR 09-13 (FISA Ct. Sept. 3, 2009).

[35] *See* THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD, at xxvi (2014).

[36] *See* PCLOB Section 215 Report, *supra* note 29, at 16.

[37] National Research Council's Bulk SIGINT Collection Report, *supra* note 10.

lawsuits challenging the program's legality.[38] They largely focused on the program's infringement of privacy rights and civil liberties.

In June 2015, Congress passed the USA FREEDOM Act, ending the bulk collection program 180 days after the law's enactment. The vote came less than a month after the U.S. Court of Appeals for the Second Circuit struck down the government's expansive interpretation of Section 215 justifying the metadata collection.[39] The USA FREEDOM Act clarified that the Section 215 program did not authorize bulk collection; the IC would instead rely on providers' own call records in their normal course of business.[40] Under the USA FREEDOM Act, the government is required to seek a FISC order requiring the production of certain CDRs the companies held. The companies would have to build infrastructure to respond, with the technology "likely cost[ing] millions of dollars in the form of reimbursements."[41] The system had to handle iterative querying across multiple providers and was also required to provide CDR information whenever there was a query—even if the data was no longer held in CDR format; building a system to do these tasks correctly is quite complex.

B. *The History of the Section 702 Program*

While this Article's focus is on the telephony metadata program, it is also important to consider Section 702 because its authorities allow for targeting, for foreign intelligence purposes, communications of foreign persons reasonably believed to be located abroad, consistent with the Fourth Amendment. Section 702's origins are in the Terrorist Surveillance Program, launched in the aftermath of 9/11. The Terrorist Surveillance Program operated separately from the program collecting communications metadata about telephone and email in bulk.[42] The President routinely renewed the program for "extraordinary emergency" reasons. Chairs and leading members of Congressional committees and the presiding judge of the FISC were briefed on the program's existence.[43]

This warrantless wiretapping, which allows for collection of content and metadata, was ultimately codified in Section 702 as part of the FISA Amendments Act of 2008 and has been reauthorized twice.[44] Section 702 requires the government

---

[38] *See, e.g.*, Complaint, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 1:13-cv-03994); Complaint, Klayman v. Obama, 142 F. Supp. 3d 172 (D.D.C. 2013) (No. 1:13-cv-00851).
[39] *See* ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).
[40] Bart Forsyth, *Banning Bulk: USA FREEDOM Act and Ending Bulk Collection*, 72 WASH. & LEE L. REV. 1307, 1334–39 (2015).
[41] David S. Kris, *The NSA and the USA FREEDOM Act*, LAWFARE (July 2, 2018), https://www.lawfareblog.com/nsa-and-usa-freedom-act [https://perma.cc/78NG-KZB5].
[42] *See* PCLOB Section 702 Report, *supra* note 18, at 16.
[43] PCLOB Section 702 Report, *supra* note 18, at 16.
[44] PCLOB Section 702 Report, *supra* note 18, at 17; FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631; FISA Amendments Act Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (2018).

to develop certain minimization[45] procedures on the acquisition, retention, use, and dissemination of 702 information, as well as targeting procedures.[46] NSA runs two primary programs under these authorities. The first, PRISM, is focused on Internet collection and does not include telephone calls. The government sends a "selector," such as an email address, to a U.S.-based electronics communications service provider.[47] The provider is then compelled to provide contents of all communications sent to or from that selector. The second program is upstream collection. This includes telephone calls and Internet communications. Such collection involves the compelled assistance of companies controlling the telecommunications "backbone" to release the contents of those communications that transit through their networks to the government.[48]

C. *The Evolution of the Foreign-Terrorist Threat*

In its heyday, Al-Qaeda was a highly centralized foreign terrorist organization with complex command and control structures. Al-Qaeda launched meticulously planned attacks orchestrated by its leadership, with planners in Afghanistan, Yemen, and elsewhere providing detailed instructions to operatives within target nations.[49] Phone calls were the prime form of communication.[50] Thus, the CDR program, focused on contact chaining between known foreign terrorist suspects and their U.S. agents, was quite valuable in discerning plots.

Al-Qaeda leadership's desire to establish a transnational movement, comprising foreign fighters and guided by outward-facing global agendas, posed a new type of terrorism threat. Osama bin Laden had a strong sense of how to run a business. He built this movement along the lines of a multinational corporation with him as CEO.[51] His board oversaw each terrorist attack and ensured attackers

---

[45] There are many aspects to minimization, including destroying inadvertently collected material, segregating Internet transactions that cannot be separated into single, discrete communications, and not moving segregated communications out of the repository if any of the separate communications include only persons in the United States. *See* ERIC HOLDER, ATTORNEY GEN. OF THE UNITED STATES, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITION OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (Oct. 31, 2011), https://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf [https://perma.cc/5MBY-H4JK].

[46] *See* PCLOB Section 215 Report, *supra* note 29, at 16.

[47] PCLOB Section 215 Report, *supra* note 29, at 7.

[48] James Ball, *NSA's Prism Surveillance Program: How it Works and What it Can Do*, THE GUARDIAN (June 8, 2013), https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google [https://perma.cc/JVQ4-ZRDZ].

[49] Bin Laden was in Afghanistan at the time of the planning of the 9/11 attacks, the safe house in Yemen also served as a planning center for attacks. *See* Lawrence Wright, *The Agent*, THE NEW YORKER (July 10, 2006), https://www.newyorker.com/magazine/2006/07/10/the-agent [https://perma.cc/YL4T-XPSY].

[50] *See, e.g.*, MATTHEW AID, THE SECRET SENTRY: THE UNTOLD HISTORY OF THE NATIONAL SECURITY AGENCY 209–11 (2009).

[51] *See* JOHN ROLLINS, CONG. RESEARCH SERV., R41070, AL QAEDA AND AFFILIATES: HISTORICAL PERSPECTIVE, GLOBAL PRESENCE, AND IMPLICATIONS FOR U.S. POLICY, at ii (2011), https://fas.org/sgp/crs/terror/R41070.pdf [https://perma.cc/7JXM-78KZ].

received proper training in Al-Qaeda's training facilities.[52] In light of Al-Qaeda's structure, it is clear why the 2003 U.S. "National Strategy for Combatting Terrorism" concluded that all terrorists "must have a physical base from which to operate."[53] The strategy saw international terrorism as pyramidal. At the top stood highly centralized terrorist organizations with complex command and control structures and leadership.[54]

The wars in Afghanistan and Iraq, targeting of Al-Qaeda's leadership and cutting down its terrorist financing channels, made it increasingly difficult for the organization's higher echelons to maintain the corporate structure.[55] As Al-Qaeda moved to empower more and more junior commanders to operate independently, it risked rogue subordinates and complete breakdown of control. This was exemplified by the Islamic State. To support the undertaking of a worldwide caliphate, the Islamic State launched an online propaganda campaign aimed at attracting foreign fighters. Al-Qaeda's model had been to attract fighters, then radicalize them upon their arrival. ISIS successfully used a "media mix of graphic violence and attractive ideals" to attract recruits who then arrived already partially radicalized, drawing the largest number of foreign fighters compared to any other terrorist group in history. [56] Online radicalization enabled terrorist clickbait, which could provide remote training as well as encourage recruits to commit terrorist attacks. Radicalized online, perpetrators carried out these one-off attacks alone or in a small partnership, without prior direction and control from ISIS-affiliated leaders.

The gradual demise of ISIS in Syria and Iraq in the latter half of 2010s led to a steady return of foreign terrorist fighters in Europe, intensifying a new kind of domestic terrorist threat. The U.S. foreign-terrorist threat is different; the current peril from returning foreign fighters is limited thus far.[57] In 1994, the United States outlawed foreign fighting in support of terrorism,[58] much earlier than many other nations.[59] It is hard for American foreign fighters to return and thus potentially reengage in terrorist activity. Compared to thousands of Europeans who went to

---

[52] *See id.*

[53] THE WHITE HOUSE, NATIONAL STRATEGY FOR COMBATTING TERRORISM 6 (2003), https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf [https://perma.cc/ZFY2-7WCF].

[54] *Id*.

[55] Jason Burke, *Think Again: Al Qaeda*, FOREIGN POL'Y (Oct. 27, 2009), https://foreignpolicy.com/2009/10/27/think-again-al-qaeda-4/ [https://perma.cc/44GE-BJ3N].

[56] T. HAMID AL-BAYATI, A NEW COUNTERTERRORISM STRATEGY: WHY THE WORLD FAILED TO STOP AL QAEDA AND ISIS/ISIL, AND HOW TO DEFEAT TERRORISTS 110–11 (2017).

[57] *See* ALEXANDER MELEAGROU-HITCHENS, SEAMUS HUGHES & BENNETT CLIFFORD, GEORGE WASHINGTON PROGRAM ON EXTREMISM, THE TRAVELERS: AMERICAN JIHADISTS IN SYRIA AND IRAQ 8–9 (2018), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/TravelersAmericanJihadistsinSyriaandIraq.pdf [https://perma.cc/8CKN-CEZC].

[58] *See* 18 U.S.C. §§ 959, 2339B (2012).

[59] *See generally Treatment of Foreign Fighters in Selected Jurisdictions*, LAW LIBRARY OF CONGRESS, https://www.loc.gov/law/help/foreign-fighters/country-surveys.php [https://perma.cc/VA9B-HBQX] (last visited Apr. 14, 2020).

Iraq and Syria to join ISIS, only about 300 Americans are said to have done the same.[60] The physical distance between the United States and the conflict also limited the threat from veteran jihadis. Those seeking to return into the United States to carry attacks undergo tight border restrictions and the scrutiny of airport security. U.S. Customs and Border Protection authorities vet physical entry into the United States; afterwards, domestic law enforcement is likely to monitor returnees after entry into the country.[61] Such monitoring is unlikely to rely on Section 215, entry into the United States of a foreign terrorist fighter would constitute sufficient suspicion to justify a traditional FISA warrant.

Since 2014, when the caliphate was formally declared, radicalized homegrown lone wolves have run eight deadly attacks in the United States.[62] In all cases, attacks were conducted by individuals plugged into an "interactive ecosystem" of propaganda and crowd-sourced jihad.[63] Examining terrorist attacks committed on U.S. soil between 2003–17, counterterrorism expert Christopher Wright found that "the average cell size of those involved in these attacks is 1.2, with the most frequent number involved in the attack being 1."[64] Terrorists were not in significant contact with handlers from ISIS or other terrorist organizations. As Federal Bureau of Investigation ("FBI") Director Christopher Wray observed:

> The FBI assesses HVEs [homegrown violent extremists] are the greatest terrorism threat to the Homeland. These individuals are global jihad-inspired individuals who are in the U.S., have been radicalized primarily in the U.S., and are not receiving individualized directions from FTOs [foreign terrorist organizations]. . . . This is a significant transformation from the terrorist threat our Nation faced a decade ago.[65]

The evolution in the threat environment dramatically changes which intelligence tools provide the greatest value. Current domestic terrorist attacks within the United States are not directed, they are instigated. Domestic terrorists do not leave behind a trail of telephony metadata breadcrumbs for the IC to follow

---

[60] *See* MELEAGROU-HITCHENS ET. AL., *supra* note 57, at 5.
[61] *See* Christopher J. Wright, *Islamist Terror in America*, *in* TERRORISM IN AMERICA 96, 109–10 (Robin M. Valeri & Kevin Borgeson eds., 2018).
[62] *See* Peter Bergen & David Sterman, *Terrorism in America After 9/11*, NEW AMERICA (Sep. 10, 2018), https://www.newamerica.org/in-depth/terrorism-in-america/part-i-overview-terrorism-cases-2001-today/ [https://perma.cc/VM4U-M2ED] [hereinafter New America Report] (for a complete analysis of all of these attacks, see therein at page 5).
[63] *ISIS Radicalization: Countering Terrorist Radicalization & Recruitment on the Internet & Social Media: Hearing Before the Permanent Subcomm. on Investigations of the S. Comm. Of Homeland Security*, 114th Cong. 5 (2016), https://www.hsgac.senate.gov/imo/media/doc/Bergen%20Testimony_PSI%202016-07-06.pdf [https://perma.cc/X57G-NFQ8] (submitted testimony of Peter Bergen, Vice President, New America Foundation).
[64] *See* Wright, *supra* note 61.
[65] *Threats to the Homeland: Before the S. Comm. on Homeland Security and Governmental Affairs*, 115th Cong. 2–3 (2018) (statement of Christopher Wray, Dir., Fed. Bureau of Investigation).

because they are not in touch with any handlers—and certainly not by telephone. Although the Section 215 program could once be used to map links between actors in the United States and terrorist organizations outside the nation's borders, the likelihood that querying the USA FREEDOM Act ("UFA") CDR program will identify Internet-incited lone wolves is slim. Such a tool does not provide investigative information on the operations of these homegrown violent extremists.

II. Issues Arise with the Use of The USA FREEDOM Act

At first it appeared that the transition to the UFA greatly improved the CDR collection. Former NSA Deputy Director Rick Ledgett explained that the UFA "transferred the compliance burden from NSA, which had to maintain the universe of call data, to the telecommunications providers, who only had to give NSA those contacts responsive to an authorized query."[66] The change gave the agency access to additional providers and more data.[67] Then two issues raised concerns. The first was the scale—151 million CDRs collected in 2016 and 534 million in 2017—which seemed high given the 40 orders issued each year.[68] The second was NSA's June 2018 announcement that it was purging three years of records. This Article examines how 40 targets might lead to collecting hundreds of millions of CDRs in a single year and what might have led to the 2018 purge of records.[69] Necessarily speculative, this discussion is nevertheless well grounded in the facts as they are known.

A. *Collecting CDRs*

Following the Snowden disclosures, the IC began a multi-pronged effort for transparency. In that spirit, NSA published an overview of the architecture used by

---

[66] Telephone interview by Susan Landau with Rick Ledgett, Former N.S.A. Deputy Dir. (Apr. 19, 2019).

[67] *Id*. It appears that post-UFA, the agency had access to most of the major providers.

[68] *See* OFF. OF DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: CALENDAR YEAR 2017, at 33–35 (2018), https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf [https://perma.cc/4QWB-BM35] [hereinafter Statistical Transparency Report 2017]; OFF. OF DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: CALENDAR YEAR 2018, at 27–31 (2019), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf [https://perma.cc/Z9CN-PY3R] [hereinafter Statistical Transparency Report 2018] (repeating those numbers for 2016 and 2017 and discussing the 2018 purge).

[69] The NSA transparency reports define a target as "the individual person, group, entity composed of multiple individuals, or foreign power that uses the selector such as a telephone number." *See* Statistical Transparency Report 2018, *supra* note 68, at 6. Each FISC order correlates with a selector or selectors and not with a target. The number of orders is typically the same as the number of targets but need not be. If two different targets were using the same selector, they would be covered under a single order. Thus in 2016, while 40 CDR orders were issued, 42 targets were actually covered under these orders. In 2017, the number of orders and the number of targets were identical. *See* Statistical Transparency Report 2018, *supra* note 68, at 27.

the USA FREEDOM Act for CDR collection.[70] Collection is based on selectors such as an IMEI number, a 15-digit number that identifies a particular device[71] or phone number.[72] To explain the role these identifiers play in collection, we start with how the phone network works.

Though landline and mobile phone networks operate seamlessly together, the naming convention—what a phone number means—is different for landline and mobile telephones. In traditional landline phones, the phone number delineates the end location of the "twisted pair" of wires that connect the phone to the telephone's central office. The central office is where the phone subscriber's line is connected to switching equipment that enables local calls and connections to long-distance carriers.[73] The twisted pair defines a phone's address—its number—in an apartment, an office (including a particular desk), etc. It is a physical location. By contrast, a mobile phone number does not directly delineate a fixed physical location. Instead fancy footwork within the mobile network, working with the landline network with which it interoperates, connects a mobile number with the phone's current physical location.

For a landline—also known as a wireline phone—the phone number does not identify the phone; a landline phone moved to a new location and plugged into the wall has a different number.[74] By contrast, a mobile phone "owns" its phone number—the IMSI,[75] carried on the device's SIM card—and a mobile phone that moves keeps its number. Changing ownership of a landline number is harder than changing ownership of a mobile number. Replace a mobile's SIM card and you have a different IMSI[76]—but not a different IMEI[77]—while a landline device, the account owner, and phone number have a relatively permanent relationship.

---

[70] *See* NSA CIVIL LIBERTIES AND PRIVACY OFF., TRANSPARENCY REPORT: THE USA FREEDOM ACT BUSINESS RECORDS FISA IMPLEMENTATION 5 (2016), https://fas.org/irp/nsa/ufa-2016.pdf [https://perma.cc/7K7J-CCAY] [hereinafter Records FISA Implementation Report].

[71] Because the IMEI number is tied to a particular device, the number is useful in preventing the use of stolen phones, thus reducing incentive for theft.

[72] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT 1 (2020), https://www.pclob.gov/library/PCLOB%20USA%20Freedom%20Act%20Report%20(Unclassified).pdf [https://perma.cc/PE6Z-JMV3].

[73] Local number portability (LNP)—the ability of a subscriber to switch to another carrier—complicates this picture; some signaling messages contain carrier and physical line identification information instead of phone numbers.

[74] VoIP phones—phones that places voice calls over an IP network—are more like mobile phones, in that they carry their own identity with them.

[75] The IMSI has three fields: country code, mobile network code, and the mobile subscription identification number. *See* ITU-T, TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, INTERNATIONAL TELECOMMUNICATION UNION, SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION, AND HUMAN FACTORS, RECOMMENDATION E.212 (2016).

[76] This is based on the three fields that form the IMSI (country code, mobile network code, and the mobile subscription identification number).

[77] This is because the IMEI is tied to the device.

A mobile phone has two addresses: the MS-ISDN and the IMSI number. The MS-ISDN is the external identifier—the number a user gives when we ask for their cell number. The IMSI is the phone's identity on its "home" network and is not shared except when the phone roams (more on this shortly). The MS-ISDN/IMSI pair delineates the phone itself, not its location.

Delivering calls to mobile devices results in the use of multiple identifiers: IMSI, the phone number or account, and IMEI. This variety of mobile phone identifiers provides investigators with interesting capabilities. While it is understood that mobile phones check into their cell towers with the IMSI as the user roams—that is, after all, how the phone alerts the network that "I am here; route calls to me"—it is less well known that CDRs also collect phones' IMEIs.[78] This information can be quite useful. Hussain Osman, a terrorist involved in the July 21, 2005, bomb attacks in London, fled to Rome having bought a new SIM card for his phone.[79] The phone had a new IMSI, but still had the same IMEI. Authorities tracked Osman to his brother's apartment via the records his cell phone left through the network as he traveled.[80]

When the NSA becomes aware of a selector of interest, the agency checks its archives to cross-reference it with other selectors (e.g., an MS-ISDN, an IMSI, an IMEI number). These archives, however, are limited. They contain phone records NSA acquired from previous searches under UFA and other authorities, but do not include metadata NSA obtained through Section 215 of the USA PATRIOT Act prior to the passage of the USA FREEDOM Act[81] nor data purged in the 2018 incident. For example, NSA determines whether it has records showing a particular phone, for example named through its IMEI, already in the archives as connected to a particular MS-ISDN, IMSI, etc. This is not about "hops"—which numbers have been called by a particular number—it is about which phones or numbers have used (or been used with) which numbers or phones. This step is accounted for in the dashed green arrow that points in both directions between Phases 1 and 2 of *Figure 1*.

Phase 1 of the NSA CDR collection process involves obtaining FISC approval that there is "reasonable and articulable suspicion" ("RAS") that a specific selector (or a set of associated selectors) is "associated with a foreign power, or an agent of a foreign power, engaged in international terrorism or activities in preparation therefore."[82]

---

[78] *See* Statistical Transparency Report 2018, *supra* note 68, at 30.
[79] *Tracking a Suspect by Mobile Phone*, BBC NEWS (Aug. 3, 2005), http://news.bbc.co.uk/2/hi/technology/4738219.stm [https://perma.cc/RM9K-4YWH].
[80] Heather Timmons, *London Suspect Betrayed by His Cellphone*, N.Y. TIMES (Aug. 2, 2005), https://www.nytimes.com/2005/08/02/world/europe/london-suspect-betrayed-by-his-cellphone.html [https://perma.cc/62XQ-83EG].
[81] *See* Records FISA Implementation Report, *supra* note 70, at 5.
[82] Records FISA Implementation Report, *supra* note 70, at 13.

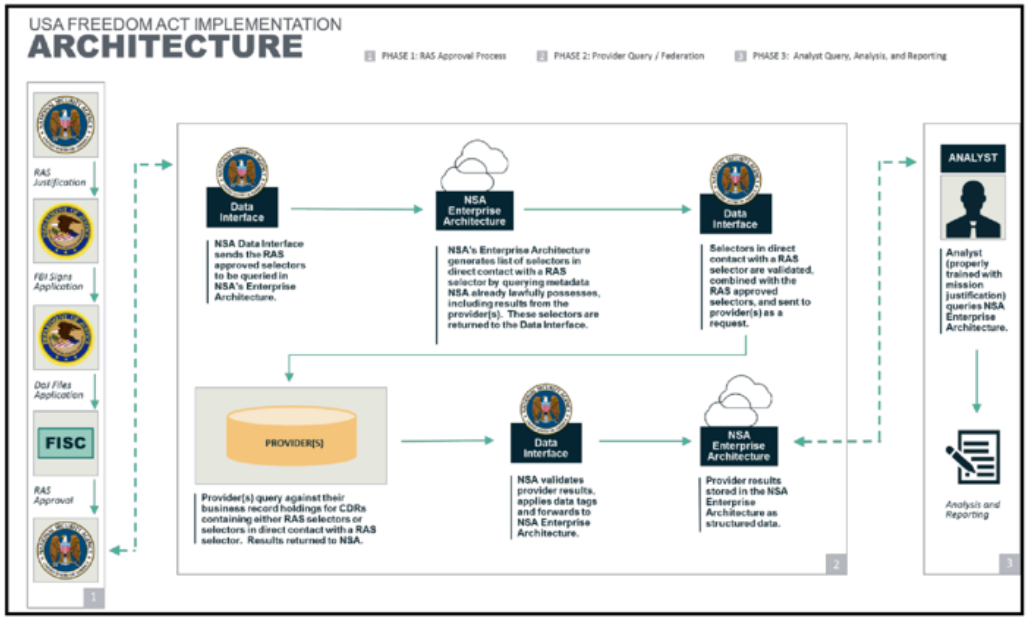

Figure 1: Architecture for USA FREEDOM Act Business Records FISA Implementation[83]

Phase 2 of the process involves querying the providers and NSA's own archives for metadata within one hop and then two hops of the FISC-approved selector.[84] Under the USA FREEDOM Act, the one-hop, two-hop steps are done automatically. This process is repeated periodically for the duration of the FISC order so as to capture new CDRs within a two-hop maximum from a FISC-approved selector.[85] NSA validates the result, storing it within a system called the NSA Enterprise Architecture.[86]

Phase 3 is NSA's processing and analysis of the collected information. This stage is outside the realm of the technical side of collection and this Article does not examine it.

B. *Answering the "Easy" Question: If There Are Only 40 Orders Each Year, Why Are So Many CDRs Collected?*

Per the USA FREEDOM Act, the Office of the Director of National Intelligence ("ODNI") has released annual statistical transparency reports. The reports for 2016 and 2017 show a total of 40 orders in each calendar year for CDRs issued pursuant to applications under the business records provision.[87] The estimated number of CDRs arising from those 40 orders was high. ODNI suggested that duplication occurs because different telecommunications companies produce

[83] Records FISA Implementation Report, *supra* note 70, at 5.
[84] Records FISA Implementation Report, *supra* note 70, at 6.
[85] Records FISA Implementation Report, *supra* note 70, at 6.
[86] Records FISA Implementation Report, *supra* note 70, at 5.
[87] *See* Statistical Transparency Report 2018, *supra* note 68, at 28.

CDRs for the same call event.[88] With multiple selectors possible for each call, the number of possible CDRs could result in many records for a single call. This part examines how the CDR collection works in an effort to explain what appear to be surprising statistics: an average of 3.75 million CDRs per order in 2016 and 13.3 million per order in 2017.

For simplicity of analysis, this part starts with the scenario that NSA supplied:

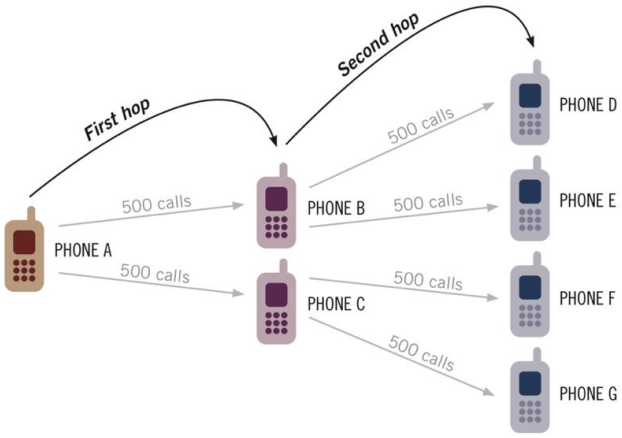

Figure 2: NSA Call Event Hop Scenario and Method of Counting[89]

NSA discovers a selector for which the agency seeks a FISC order. Before applying for an order, NSA checks the archive to determine if the selector is in the archive. Suppose that the selector is not in the archive. Following the example provided in Figure *2*, if Phone A has made 500 calls each to Phones B and C, these calls are likely to be recorded twice, once from A's side and once from B or C's side. This yields two CDRs per call, one per carrier. If Phone A is outside the United States, NSA might not receive the CDR held by the foreign carrier. Thus, after the first hop, NSA has likely received between 1,000 and 2,000 records arising from the 500 calls (for the purpose of this argument, assume 1,000). The CDRs returned other potential selectors with the original one. For example, if the original selector is an IMEI, then the CDRs will return an IMSI, account number, and perhaps a calling card number used—*not hopped to*—by that IMEI. If NSA believes it could demonstrate to the FISC that the target used the new selectors associated with the IMEI, the agency would presumably request the associated selectors be added to the original order. That provides a potential of 4 associated selectors multiplied by 1,000 calls being generated during the first hop, generating 4,000 CDRs. Incoming communications also create CDRs. Assuming as many incoming calls as outgoing calls—a reasonable assumption for consumer, non-marketing, non-fraud numbers—this means the total number of CDRs arising from the first hop is 8,000.

---

[88] *See* Records FISA Implementation Report, *supra* note 70, at 9.
[89] *See* Statistical Transparency Report 2018, *supra* note 68, at 29.

Phones B and C also give rise to selectors. According to the NSA Transparency report, "selectors in direct contact with a RAS selector are validated, combined with the RAS approved selectors and sent to the provider(s) as a request."[90] One can expect up to 8 selectors from phones B and C. As shown in Figure 2, phones D, E, F, and G receive 500 calls each. There are 2 phones (B and C) with 4 selectors per phone, making 1,000 calls per phone and generating 2 CDRs per call, for a total of 16,000 CDRs being generated from outgoing calls on the second hop.[91] Again, assuming that A receives the same number of incoming second-hop calls as it makes, this creates a total of 32,000 CDRs from the incoming plus outgoing second-hop calls. Thus starting with phone A calling 2 phones (B and C), and phones B and C calling phones D and E, and F and G, respectively, there are up to 40,000 CDRs generated from the first and second hops from A (this is from 8,000 + 32,000). Note that implicit in this calculation is the assumption that D, E, F, and G are not communicating directly with A. That is not a reasonable assumption in analyzing social networks—your two close friends or family members are likely to also know, and perhaps call, each other—but the targets against whom NSA is collecting communicate differently.

So far, the sum of CDRs collected is solely for a 180-day period of the court order. The order allows the collection of CDRs "going back in time." That is, while collection by the government may only occur during the 150-day period, the law permits collection of *all* CDRs the telephone company has associated with that selector. Because CDRs are the basis for business planning on telephone use, companies may hold CDRs for a number of years. We estimate the companies NSA queries retain three years' worth of records.[92] Instead of 180 days' worth of CDRs, there are likely six times that, or 240,000 CDRs returned. This substantial number remains well below the 3.75 million per order that would explain the numbers NSA has reported.

We do not know to what degree the example NSA provided is representative of actual terrorist behavior. The 2005 assassination of former Lebanese Prime Minister Rafik Hariri can provide insights. Hariri had resigned as Prime Minister on October 20, 2004, intending to participate in regional elections six months later. Instead he was assassinated on February 14, 2005, by a truck bomb that detonated as his motorcade passed by.[93]

---

[90] *See* Records FISA Implementation Report, *supra* note 70, at 5.

[91] We are assuming that D, E, F, and G are inside the United States, and thus each call nets 2 CDRs.

[92] *See, e.g.*, *Cell Phone Location Tracking Request Response – Cell Phone Company Data Retention Chart*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart [https://perma.cc/47FF-89U8] (last visited Apr. 5, 2020) (containing DEP'T OF JUSTICE, RETENTION PERIODS OF MAJOR CELLULAR SERVICE PROVIDERS (Aug. 2010)). We are assuming that user calling patterns did not change substantially over the three-year period. In fact, calling patterns do change, but not sufficiently to change our estimates.

[93] Ronen Bergman, *The Hezbollah Connection*, N.Y. TIMES (Feb. 10, 2015), https://www.nytimes.com/2015/02/15/magazine/the-hezbollah-connection.html [https://perma.cc/9P6X-4YY7].

The attack involved extensive planning. Examining Lebanese cell phone records from the time of Hariri's resignation as prime minister in October 20, 2004, to his assassination on February 14, 2005, investigators discovered interesting calling patterns. The assassination "team" had different cells: the "green" group had 18 phones, the "blue," 15; the "yellow," 13; and the "red," 8.[94] The green group appeared to be the operational center of the team.[95] This group's leader only spoke with two deputies and always only on green phones.[96] These deputies, using phones belonging to the other color groups, would then call a leader of the other color group. A leader of the blue or yellow groups would call a member of the green group on a green phone but communicate with blue or yellow group members on a blue or yellow phone. Members of the group avoided using their "work" phones for personal communications, instead they typically carried an additional personal phone from which they made personal calls. Thus, deputies of the green group and leaders of the various color groups carried at least three phones.[97]

Let us focus first on the personal phone. The purpose of plotters having a personal phone to make calls was to prevent identifying the individuals in the plot. Journalist Ronen Bergman reported: "[P]rosecutors say that same purple phone was always in the same place as the green command-group phone that Merhi [the plotter who ran the cover operation] carried."[98] From the point of view of counting CDRs, these personal phones are important. Unlike those used in the plot, these phones were used as phones to call or text a family member, to order furniture, or to arrange to meet for dinner.

For simplicity, we assume a 100-day period for the phones rather than the 117 days between October 20 and February 14 (the phones stopped working after the assassination). Consider the CDRs from the calls of the leader of the blue group, B. We can assume that B spoke with the green deputy, G, once or twice a day during the 100 days of the plot's planning and execution. We assume that using his blue phone, B spoke with other members of the blue group twice a day. This combination of devices means that there were at least nine potential selectors associated with the blue leader: three IMEIs, three IMSIs, three accounts (so as to keep records of the three phones—green phone, blue phone, and personal phone—separate). But there may have been more (e.g., possible calling card numbers for the two "official" phones).

The next step is to count the number of anticipated CDRs that would result from the first hop of the call emanating from the leader of the blue group. Say, on average, that B had 1.5 incoming and outgoing calls, combined, per day with G. That would give a total of 900 CDRs over the period (3 selectors for the green phone x 1.5 calls per day x 100 days x 2 CDRs per call, assuming this time that both carriers are domestic carriers). B also had 3,000 CDRs arising from calls with

---

[94] *Id.*
[95] *Id.*
[96] *Id.*
[97] *See id.*
[98] *Id.*

the blue group (3 selectors and 5 calls daily to his group of 15 on the blue phone, for a total of 3 x 5 x 100 days x 2 CDRs per call). Finally, B used his personal phone for friends and family. Assuming five calls a day, that would work out to 3,000 CDRs (3 selectors x 5 calls/day x 100 days x 2 CDRs/call). Further assuming that the friends and family phone results in calls to 30 different numbers over the 100-day period, a high but not unreasonable estimate, the total is 6,900 first-hop CDRs over the 100-day period.

We can expect many more CDRs from the second hop and the compounding effect of the number of B's contacts. There are three sets of second hops. These emanate from G, the members of the blue group, and B's friends and family. We examine each in turn.

Assuming that between calls to and from the green group's leader and calls to and from the leaders of the various color groups, G made five calls a day, this contributed 3,000 CDRs (3 selectors x 5 calls/day x 100 days x 2 CDRs per call) on a combination of his green and blue phones. G made calls on his personal phone; as with B's personal phone, assuming that these constituted 3,000 CDRs (3 selectors x 5 calls/day x 100 days x 2 CDRs/call), the contribution of CDRs generated from the second-hop communications emanating from G is 6,000.

There are fifteen members of the blue group. We conservatively assume that aside from B, members of the blue group carry a blue one and a personal one. If we assume that members of the blue group made 4 calls a day within the group, there are 36,000 CDRs (15 people x 3 selectors per person x 4 calls/day x 100 days x 2 CDRs per call). The contribution of the personal phones of the fifteen members of the blue group is 3,000 CDRs per person x 15 people, or 45,000 CDRs over the 100 days. Thus, the total CDR second-hop contribution from the blue group is 81,000 CDRs.

Finally, there are "friends and family" of the blue deputy. This creates the substantial expansion of CDR records. In a 100-day period, B's 30 "friends and family" each may have had three selectors and made about 500 calls during the period. Accordingly, that is an additional contribution of 90,000 CDRs (30 people x 3 selectors/person x 5 calls/day x 100 days x 2 CDRs per call). Summing up, this adds up to 171,000 CDRs from the second hop or a total of about 177,000 CDRs from the first two hops.

The calculation for 177,000 CDRs was for a 100-day period. Extending the same calling patterns to a 180-day period (the length that a FISC order permits), the length of time of a FISC Section 215 order, that would come to 318,600. That is still not 3.75 million CDRs per order that NSA reported for 2016. Indeed, it is under a tenth of the number of CDRs per order that NSA reported for 2016.

The calculations above made assumptions here about how the phones are used—how many calls are made per day and how many different numbers are called—but the assumptions are reasonable. In fact, the assumptions may lead to

underestimates of the number of CDRs produced from calls by the various phones. If one imagines that one of B's "friends and family" calls is to a popular number—a doctor's office, for example—the growth in CDRs from the second hop is much higher. The earlier CDR collection program carried out under the USA PATRIOT Act employed a master "defeat" list to "block the ingest of, or purge already ingested unwanted information."[99]

High-volume identifiers such as telemarketers are problematic because they indiscriminately "touch" many users, amplifying the collateral reach of the NSA when caught in a hop. There are three steps to handling the CDRs: collection, query, and dissemination.[100] While there are privacy interests in all three—even the perception that one's CDRs may be collected can create a chilling effect—a collected CDR that is never examined, and thus never disseminated, impinges on privacy less than one that is.

NSA's UFA implementation performs the second hop automatically. If a high-volume number directly connects with a selector belonging to a target, NSA collects the CDRs between the high-volume identifier and its connections. CDRs related to high-volume identifiers are just dead ends. As such, NSA has little interest in collecting them. But since these high-volume identifiers shift frequently, NSA cannot necessarily identify a high-volume identifier before the second hop, for it is the second hop that reveals the high-volume nature of the identifiers.

A declassified 2014 FISC opinion states:

> An authorized technician may access the [Business Records] metadata to ascertain those identifiers that may be high volume identifiers [such as telemarketers]. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories).[101]

As the FISC opinion indicates, it appears that NSA then determines which are high-volume identifiers. It is likely safe to assume that those CDRs involving the high-volume identifiers are not examined—and certainly not disseminated.

While the terrorists who carried out the Hariri assassination do not appear to have shifted between different SIM cards, phones, and accounts for the same communication channels (as opposed to using different phones for different

---

[99] *See* LEGISLATIVE AFFAIRS OFF., MEMORANDUM FOR STAFF DIRECTOR OF THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE FROM NSA DEPUTY ASSOCIATED DIRECTOR 2 (June 29, 2009).

[100] National Research Council's Bulk SIGINT Collection Report, *supra* note 10, at 29.

[101] *See* In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 14-67, at 6 (FISA Ct. Mar. 28, 2014).

subgroups of the plot), many terrorists do so. The NSA program, CO-TRAVELER, uses mobile phone data to track users in real time. For this reason, CO-TRAVELER is of particular use in discovering people in close proximity to an individual.[102] CO-TRAVELER can also be used to discover whether a target is using a burner phone. Each discovery of this sort increases the number of selectors associated with a particular target. For example, if the initial selector is an IMEI, it might be associated with two different IMSIs. These, in turn, might be associated with two different IMEIs and three different calling card numbers. If a single target is using these different IMEIs, IMSIs, and calling card numbers, then the collection would fall under a single order.[103] If the people with whom the target is communicating are doing the same, then the number of CDRs grows exponentially even for a two-hop collection.

The Hariri assassination involved many members of a highly structured terrorist organization planning over many months and may not be representative of the cases of radicalized lone wolves being investigated today. But the lessons from the Hariri case, in conjunction with *Figure 2*, can guide our understanding. If a target is using a phone to call only two other numbers, then it is likely that, just as in the Hariri case, the target also has a phone from which he makes personal calls to various parties. The collection from the two hops emanating from the target's "terrorist phone" may result in 24,000 CDRs; how many CDRs may come from the terrorist's personal phone?

Calculating this number requires knowing the median number of unique numbers a person may connect to over a 180-day period and the median number of times they do so (this Article uses "median" since the average number is heavily skewed upwards by the number of outgoing calls made by calling centers, robocalls, and the like). Determining these numbers is quite challenging.

First and foremost is the rate of change of communications technologies. For at least sixty years, the telephone was the preferred method of electronic communication. Communications technologies now change in a matter of years, if not months. Because IP-based messaging applications—e.g., iMessage, WhatsApp, Messenger—are often limited to a single platform, adoption of technologies can occur in Internet time. Widespread use may occur in a matter of months.

Telephone companies have precise data about use of voice calls and text. However, given their general unwillingness to share that information publicly, there are gaps in the literature regarding text and voice usage. While there is information

---

[102] *See* NAT'L SECURITY AGENCY, SUMMARY OF DNR AND DNI CO-TRAVEL ANALYTICS (2012), https://www.documentcloud.org/documents/888734-cotraveler-tracking-redacted.html [https://perma.cc/4RMQ-RQEY].
[103] Records FISA Implementation Report, *supra* note 70, at 8.

on mean and median use of text by Americans,[104] minutes of voice call use annually by Americans,[105] and U.S. teens' use of SMS,[106] studies fail to show how many unique people Americans call or text in a month, what the mean and median usage of phone calls are, and what those numbers are once spammers and robocallers are removed from the data set. This Article has made reasonable estimates about available data and used these estimates to provide some educated guesses on usage.

These estimates include CDRs for telephone calls and SMS.[107] Sometimes "texting" is used to denote both SMS and text messaging applications such as iMessage and WhatsApp, but text messaging applications are IP-based communications.[108] It appears that IP-based messaging applications are not collected under Section 215 authorities, an issue discussed in Section III.C.1. Let us explain our assumptions.

To calculate the number of CDRs generated by the use of a personal phone, it is necessary to ascertain the median number of calls plus SMS texts a person might make daily and the number of "unique" connections for those communications—the number of different outgoing numbers used for these calls plus SMS texts. According to the Pew Research Center, in 2010, among adults who used mobile phones for calls and SMS texts, the daily median for receiving and making calls was five, and the daily median for receiving and sending texts was ten.[109] These numbers were notably higher for young people; 18- to 24-year-olds had a mean of 110 texts per day and a median of 50; 25- to 34-year-olds showed a mean of 49 and a median of 20 texts daily.[110] A similar Pew study in 2015 echoed high use of texts by young adults.[111] CTIA, an industry association, observed that

---

[104] *See* Aaron Smith, *How Americans Use Text Messaging*, PEW RESEARCH CTR. (Sept. 19, 2011), https://www.pewinternet.org/2011/09/19/how-americans-use-text-messaging/ [https://perma.cc/PT9Z-FW29].

[105] *See* FED. COMMC'N COMM'N, TWENTIETH WIRELESS COMPETITION REPORT 72 (2017), https://www.fcc.gov/document/fcc-releases-20th-wireless-competition-report-0 [https://perma.cc/9A6T-UV93].

[106] *See* Amanda Lenhart & Dana Page, *Teens, Social Media & Technology Overview*, PEW RESEARCH CTR. (Apr. 9, 2015), https://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/ [https://perma.cc/B724-8JVT].

[107] *See* Charlie Savage, *Disputed N.S.A. Phone Program Is Shut Down, Aide Says*, N.Y. TIMES (Mar. 4, 2019), https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html [https://perma.cc/6BYD-ZQBR] (in March 2019 the *New York Times* reported that SMS CDRs are collected under the USA FREEDOM Act). The statement regarding collection of log data pertaining to texts was confirmed in an email exchange with one of the authors on March 8, 2019. Laura Donohue has written that the current government interpretation of UFA could include texting metadata. *See* LAURA DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 53 (2018).

[108] iMessage is actually a multiprotocol application. *See infra* Section III.A.

[109] Smith, *supra* note 104.

[110] Smith, *supra* note 104.

[111] *See* Aaron Smith & Dana Page, *U.S. Smartphone Use in 2015*, PEW RESEARCH CTR. (Apr. 1, 2015), https://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/ [https://perma.cc/V6A8-SACR].

in 2016, Americans sent and received 1.99 trillion texts (combined SMS and MMS multimedia texts sent via the cellular network) yearly,[112] or approximately 22 daily.

The last number needed before calculating is the median or mean number of unique contacts for users within a fixed time period. That number is not readily available for the U.S. population, but a 2013 study of users of a Chinese telecom provider found the number of unique outgoing contacts for phone calls to be rather surprising: 245 over a two-part, four-month period in 2010 (June 28, 2010–July 24, 2010 and October 1, 2010–December 31, 2010, with some unexplained missing days).[113] The fact that the number is just for phone calls means that it underestimates calls plus SMS texts. Researchers first sifted the telecom data so that the study considered only the 100,000 most active cellphone users—that is, those with the largest number of outgoing calls. They then filtered the data to eliminate users conducting robocalls, telecom sales, or telecom frauds (such users are recognizable by a high number of outgoing calls and almost no incoming ones). Thus, 245 denotes communications between people who know each other at some level, not sales calls or otherwise inflated numbers.

We are ready to calculate the number of CDRs resulting from A's personal phone. We do this twice, providing a low estimate using conservative estimates of how many calls and SMS are sent to how many unique contacts and a high estimate using more generous numbers. We remind the reader of the greater use of the telephone network—calls plus SMS—by young people. As we discuss at greater length in Section III.A, the most serious foreign-influenced terrorist threat in the United States arises from home-grown violent extremists; their ages almost inevitably lie in the 18-to-34 range.

Because the targets are within this demographic group, when doing estimates, it is reasonable to base numbers on the higher use this age range enjoys. Even when we estimate conservatively, we can assume that A makes and receives at least ten calls or SMS texts daily, and, over the first 30 days of the 180-day order, contacts at least 10 unique numbers (3 family members, 2 people from work, and 5 others from a combination of friends). The period of collection is 180 days.[114]

The number of CDRs generated during the first hop of A's personal phone is 7,200 (4 selectors of A's phone x 10 daily incoming and outgoing communications x 180 days). By assuming that the calls from B and C are domestic, we can assume that NSA will collect twice as many CDRs from B and C's first

---

[112] *See* CTIA, THE STATE OF WIRELESS 2018, at 7 (July 10, 2018), https://api.ctia.org/wp-content/uploads/2018/07/CTIA_State-of-Wireless-2018_0710.pdf [https://perma.cc/Q3F2-RHB6]. Other trade magazine estimates were much higher. *See, e.g.*, Kenneth Burke, *How Many Texts Do People Send Every Day (2018)?*, TEXT REQUEST (May 18, 2018), https://www.textrequest.com/blog/how-many-texts-people-send-per-day/ [https://perma.cc/73BF-68YD].

[113] *See* Zhi-Qiang Jiang, Wen-Jie Xie, Ming-Xia Li, Boris Podobnik, Wei-Xing Zhou & H. Eugene Stanley, *Calling Patterns in Human Communication Dynamics*, 110 PNAS 1600, 1603 (2013).

[114] A renewal counts as a new order. *See* Statistical Transparency Report 2018, *supra* note 68, at 7.

hops. That is, the above will be multiplied by 2 CDRs per call, for a total of 14,400 CDRs on the first hop of their personal phones (these form the second hop from A's device).

A's second hop on her personal phone will create larger numbers. Each of the ten unique outgoing contacts will generate their own set of CDRs. In our conservative estimate, we will assume A does not connect with these contacts until day 30 of the 180-day period. The number of CDRs in the second hop of A's personal phone is 120,000 CDRs over the time period (10 contacts x 4 selectors each x 10 communications a day x 150 days x 2 CDRs per communication). Combined with the 7,200 records contributed by A's first hop, and the 14,400 records contributed by the first hops of B and C, we have 156,000 CDRs for the time period, a number that is far from the average number of 3.75 million CDRs per target that NSA reported collecting.

Let us now try this using more generous estimates on A, B, and C's use of their phones. We assume that A, an NSA target, is in the age range of heavy use of calls and SMS, of which she does forty a day (a conservative number). Recall the 2010 study found gregarious users contacted 245 unique numbers in a three-month period. We underestimate this figure and assume that the U.S. user only contacts 50 unique numbers in the 180-day period. During the first hop of A's personal phone, the related CDR collection will be 4 selectors of A's phone x 80 daily incoming *and* outgoing communications x 180 days, or 57,600 CDRs. B and C will also create 115,200 CDRs on their first hop (A's second hop) since, as before, their calls are assumed to be domestic and will thus generate two domestic CDRs per call.

A's second hop will produce a much larger number of CDRs. We will assume that A's contacts are similarly gregarious and do a combination of eighty calls or SMS texts incoming and outgoing per day. We estimate that A's 50 outgoing contacts will produce CDRs from 4 selectors each x 80 communications a day x 180 days x 2 CDRs, or 5,760,000 CDRs over the time period. Combined with the 56,400 records x 3 contributed by the first hops of each of A, B, and C, we have 6,048,000 CDRs for the time period, a number that is 1.6 times as much the 3.75 million CDRs that NSA reported.

Our numbers changed strikingly between the two estimates due to our estimate of the fifty unique outgoing contacts in a thirty-day period. The number of CDRs NSA collects appear to be high for a somewhat different reason. In 2019, NSA reported the number of unique identifiers from the 2018 CDR program: 19,372,544 phone numbers associated with 7,285,362 IMSIs and 5,305,578 IMEIs.[115] This works out to 1,761,140 phones, 662,305 IMSIs, and 482,325 IMEIs reached within two hops of a target (there were only 11 targets in 2018[116]). Even if A is highly gregarious and uses multiple phones and SIM cards—and A's contacts

[115] *See* Statistical Transparency Report 2018, *supra* note 68, at 31.
[116] *See* Statistical Transparency Report 2018, *supra* note 68, at 28.

behave similarly—we cannot account for such large numbers. But, as NSA has explained, "CDRs provided to the government include call events with business entities, such as calls for marketing purposes."[117] Telemarketers make an enormous number of outgoing calls; this could easily explain the anomalously large number of unique identifiers reported in the 2018 Transparency Report. This also explains the anomaly of nineteen million phone numbers associated with over seven million IMSIs and over five million IMEIs. The discrepancy between these number—nineteen million phone numbers but just seven million IMSIs and five million IMEIs—is almost certainly due to spoofed telephone numbers, a scheme often employed by telemarketers.[118]

The 250% growth of the CDR collection between 2016 and 2017 may have a simple answer: NSA had more data to compare in 2017 than it did in 2016. NSA CDR collection in 2016 queried metadata that the agency had collected under other authorities; queries in 2017 were also compared against the CDRs NSA had acquired in 2016, some undoubtedly containing selectors "associated" with a selector for which NSA was seeking FISC approval. It would not take a high number of such matches to drive the collection from 151 million in 2016 to 534 million in 2017.

C. *Answering the "Hard" Question: What Went Wrong?*

The "math problem" around the large number of CDRs produced was not the sole fly in the ointment. On May 23, 2018, NSA began deleting all CDRs acquired since 2015 under its UFA-amended FISA authorities. NSA announced that it was:

> [D]eleting the CDRs because several months ago 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. Because it was infeasible to identify and isolate properly produced data, NSA concluded that it should not use any of the CDRs.[119]

This statement is an enigma wrapped inside a mystery.[120] What were the irregularities? Why was it "infeasible to identify and isolate properly produced

---

[117] *See* Statistical Transparency Report 2018, *supra* note 68, at 30.
[118] *See, e.g.*, *Be Alert for 'Spoofed' Local Phone Numbers*, OFFICE OF MINNESOTA STATE ATTORNEY GENERAL, https://www.ag.state.mn.us/Consumer/Publications/SpoofingLocalNumbers.asp [https://perma.cc/2AWS-G76W] (last visited Apr. 6, 2020).
[119] *NSA Reports Data Deletion*, *supra* note 6.
[120] The original quote, "I cannot forecast to you the action of Russia. It is a riddle, wrapped in a mystery, inside an enigma; but perhaps there is a key. That key is Russian national interest," is attributed to Winston Churchill. *See* WINSTON S. CHURCHILL: HIS COMPLETE SPEECHES, 1897–1963 6161 (Robert Rhodes James ed., vol. 6, 1974).

data"? Significant speculation arose, including that NSA had been receiving location data.[121]

We believe that the problem lies with data from Mobile Switching Centers ("MSC"), which is where calls from mobile devices enter the Public Switched Telephone Network ("PSTN"). This explanation fits both NSA's public statements about the data purge and what Rebecca Richards, Civil Liberties and Privacy Officer of the NSA, told us: "[the] record on its face did not look like it had a problem, but a comparison with other records [showed] it had a problem"; she added that analysts "[couldn't] on the face identify a problem" with the CDRs.[122]

Using a phone is such a mundane aspect of daily life that few consider how the network tracks a user across the globe, enabling real-time conversation regardless of whether the speakers are using landlines, satellite phones, mobile devices, or, most recently, IP-based devices. While this increasingly complex system may make a connection, the network does not always correctly report the connection ends. This requires understanding some technicalities of telephone networks.

The phone network developed at a time when it was impossible to put any complexity into the end-user devices—the phones—themselves; instead, switches handled the complexity of connecting calls. First run by human operators,[123] they are now controlled by software. AT&T led the effort to develop "Common Channel interoffice signaling," the international version of which is CCITT Signaling System 6, adopted in 1975.[124] This system separates the call's management—the signaling that initiates and ends a call—from its communications channel. By the mid 1990s, both began being replaced by Signaling System 7 ("SS#7"), which handles international roaming.[125]

We start with the simplest version of phone networks: the PSTN used for landlines. It is easy to imagine that the phone number is the name of the phone at a particular location, but it is actually a program "to build a path to the phone."[126] When the receiver on a landline is picked up, this sends a signal to the local phone exchange. This exchange, called a central office, then generates a dial tone.

---

[121] Marcy Wheeler, *Lawfare "Breaks" News: NSA Hasn't Restarted the Section 215 CDR Function*, EMPTYWHEEL BLOG (Mar. 4, 2019), https://www.emptywheel.net/2019/03/04/lawfare-breaks-news-nsa-hasnt-restarted-the-section-215-cdr-function/ [https://perma.cc/3LV9-RYLT].
[122] Telephone interview by Susan Landau and Asaf Lubin with Rebecca "Becky" Richards, NSA Civil Liberties and Privacy Officer (Oct. 31, 2018).
[123] A.E. JOEL, JR. ET AL., BELL TELEPHONE LABS, A HISTORY OF ENGINEERING AND SCIENCE IN THE BELL SYSTEM: SWITCHING TECHNOLOGY (1925-1975) 7 (G. E. Schindler, Jr. ed., 1982).
[124] *Id.* at 321.
[125] ITU-T, TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, INTERNATIONAL TELECOMMUNICATION UNION, SPECIFICATIONS OF SIGNALING SYSTEM No. 7, Q 700 (Mar. 1993).
[126] Van Jacobson, *A New Way to Look at Networking*, at 8:48min (Aug. 30, 2006), https://www.youtube.com/watch?v=oCZMoY3q2uM.

Once a number has been dialed, switches in the central office (the nearest phone office) determine how to route the call. As one of us explained in an earlier work, in a landline:

> [i]f the call is local . . . then the switches at the central office need to determine which trunk line, or communications channel, should use to route the call to an appropriate intermediate telephone exchange. This new exchange repeats the process, but this time connects to the recipient's local exchange . . . . The local exchange determines if the recipient's line is free; if so, it 'rings' the line. If the recipient answers, her receiver closes a circuit to the local exchange, which establishes the call. The speakers have a fixed circuit for the call, the one that was created during the call set up.[127]

Long distance—or, more precisely, calls made to outside an area code—and international calls work similarly; for instance, the "1" of a long-distance number signals the local switch to connect to the switch used by the caller's long-distance carrier. The carrier's switches connect to the local exchange for the call's recipient. From there on, everything works as before: the local exchange checks if the recipient's line is free, rings the line, and establishes a communications circuit if someone answers the other end. The country code and area code (outside of the United States and Canada, this is instead the country code and city code) similarly connect to the appropriate exchanges.

Telephone networks are "backwards compatible"; old phone systems must work even as new ones are introduced. Thus, the stolid black rotary telephone that sends analogue dialing pulses to the phone network must be accommodated—even though switching technology began the move to digital more than forty years ago. Similarly, the cellular network interoperates with the landline system, requiring some fancy footwork to make this happen.[128]

The first aspect of this interoperability is the Mobile Switching Center ("MSC"), the cellular network's equivalent of the central office.[129] Information about a mobile user is stored in a Home Location Register, an enormous database

---

[127] SUSAN LANDAU, SURVEILLANCE OR SECURITY: THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES 16 (2011).

[128] Different companies and nations built their systems—phones, equipment, and networks—to different standards. For the early generations of mobile phones, devices supplied by different companies worked on different radio systems, e.g., in 2000 in the United States, Sprint and Verizon used CDMA while AT&T and T-Mobile used GSM (the standard preferred in much of the rest of the world). By the fourth generation of mobile phones, the carriers settled on a single standard, LTE, and the problem went away (except for those phones in areas with only 2G and 3G networks). *See, e.g.*, Sascha Segan, *CDMA vs. GSM: What's the Difference?*, PC NEWS AND ANALYSIS (May 24, 2019), https://www.pcmag.com/news/cdma-vs-gsm-whats-the-difference [https://perma.cc/Y3VL-CDLW]; *see also* PATRICK TRAYNOR ET AL., SECURITY FOR TELECOMMUNICATIONS NETWORKS, 36–40 (2008).

[129] *See, e.g.*, GUNNAR HEINE, GSM NETWORKS: PROTOCOLS, TERMINOLOGY, AND IMPLEMENTATION 34–37 (1998); TRAYNOR, *supra* note 128, at 26, 29.

containing the mobile phone information for hundreds of thousands of subscribers.[130] Assignment to a Home Location Register is dependent on the SIM card and is based on the IMSI number.[131] The Home Location Register stores subscriber information including the services to which the user is entitled.[132]

As a user roams, if her phone is turned on, it signals "I'm here, I'm here" and passes its IMSI and IMEI on to the visited cellular network;[133] this is "registration."[134] The local Base Transceiver Station picks up the signal[135] and sends the registration information to a Base Station Controller, which may control tens to hundreds of Base Transceiver Stations.[136] The BSC allocates radio frequencies and assigns roaming phones to appropriate Base Tranceiver Stations.[137] The MSC connects the cellular network and the PSTN, with which it communicates via SS#7.

The MSC checks to see if the subscriber is in its Home Location Register. If not, the MSC queries its Visiting Location Register, a database that stores user information while the user is roaming within the area of the associated MSC, to determine whether the phone is registered.[138] If it is, the phone is now ready to go; if it is not, using SS#7, the visited MSC connects to the phone's Home Location Register to determine to which services the roaming subscriber is entitled. There may be no business agreement between the subscriber's network and the one in which she is roaming or the user may not have arranged for service in the roaming location. In that case, the user cannot receive or make calls.

If the subscriber is entitled to service, the visited MSC informs the visitor's Home Location Register of the cluster of cells by which the visitor is currently served and updates this information approximately every thirty minutes (this is how the Home Location Register knows where the user is and thus where to route calls). The MSC constructs a temporary ID, the Temporary Mobile Subscriber Identity ("TMSI"), for the user; this serves to protect the subscriber's IMSI against eavesdroppers who might be trying to track the caller over the air interface between the phone and the tower.[139] Depending on the cell provider, the TMSI can change

---

[130] HEINE, *supra* note 129, at 6, 32–33; TRAYNOR, *supra* note 128, at 27–28.
[131] TRAYNOR, *supra* note 128, at 27.
[132] ITU-T, TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU, INTERNATIONAL TELECOMMUNICATION UNION, PUBLIC LAND MOBILE NETWORKS: LOCATION REGISTRATION PROCEDURES, RECOMMENDATION Q. 1003.
[133] The IMEI is included to prevent the use of cloned phones. *See, e.g.*, HEINE, *supra* note 129, at 7.
[134] TRAYNOR, *supra* note 128, at 46–48.
[135] The BTS may be a cell tower that simply sends and receives communications between mobile devices and the cellular network. It may also be more complex—for example, encrypting the communications to and from the device.
[136] HEINE, *supra* note 129, at 5–6, 25–28.
[137] HEINE, *supra* note 129, at 108.
[138] TRAYNOR, *supra* note 128, at 29, 47.
[139] TRAYNOR, *supra* note 128, at 68–69.

frequently (e.g., after every call) or much less so (e.g., after several days).[140] The TMSI is conveyed to the Base Station Controller and Base Transceiver Station—*but no farther*. In particular, the visitor's home MSC and Home Location Register never learn the TMSI. The registration message and location update messages between the MSCs, Home Location Register, and Visitor Location Register use the IMSI as the roaming phone's identifying number.[141]

Suppose Bob in the United States dials Alice, whose Home Location Register is in New York but who is currently in Paris. Bob calls using Alice's MS-ISDN, the number he has for Alice's mobile. Alice's MS-ISDN has been set up to work on either system. The SS#7 signaling channel routes the call to Alice's home MSC, which queries Alice's Home Location Register about reaching Alice. Alice's Home Location Register does a conversion from Alice's MS-ISDN to Alice's IMSI; for the rest of the communication, only Alice's IMSI will be used (and not her MS-ISDN). With Alice's IMSI as identifier, Alice's Home Location Register checks with the MSC that Alice has been visiting: is Alice still there?

If yes, the visited MSC sends Alice's Home Location Register a number to connect to Alice. This is not the TMSI assigned to Alice; instead, the visited MSC sends a Mobile Station Roaming Number (MSRN) created just for this call.[142] The MSRN has the same format as Alice's MS-ISDN—country code followed by area code[143] followed by "office code" (the MSC) followed by a four-digit "line number." Alice's Home Location Register must use the MSRN within ten seconds; otherwise the period of validity for the MSRN elapses.

Alice's home MSC connects the call between Alice and Bob using Alice's MSRN and Bob's number, which may well be Bob's MS-ISDN. Why is Bob's MS-ISDN used—and, more particularly—included in the connection? It may be that Alice wants Caller ID, making Bob's MS-ISDN necessary. When the call signaling reaches Paris, the MSC completes the call using Alice's IMSI (which it has associated with the 10-second MSRN it sent to New York). Alice and Bob start chatting.

Consider what CDR information is being stored at the MSCs. The New York MSC knows Alice's MS-ISDN, Alice's MSRN, and Bob's MS-ISDN. The New York MSC can keep the records in a number of ways: in terms of Alice's MS-ISDN and Bob's MS-ISDN, in terms of MSRN used for the call and Bob's MS-ISDN, or in terms of both Alice's MS-ISDN and the MSRN used for the call from Bob to Alice. The Paris MSC knows Alice's IMSI and probably Bob's MS-ISDN (whether it does depends on whether the New York MSC has forwarded it), but is not given Alice's MS-ISDN on an incoming call. The critical point is that whatever

---

[140] How often the TMSI changes varies by carrier; the information is typically found within proprietary documentation of the carriers.
[141] ITU-T, *supra* note 132, § 3.3.8.
[142] TRAYNOR, *supra* note 128, at 47–48.
[143] This is actually the area code in the integrated North America numbering plan, which includes Canada, the United States, and a number of Caribbean islands. It is the city code elsewhere.

CDR the Paris MSC creates for the call from Bob to Alice does not include Alice's MS-ISDN, for Paris does not know it.

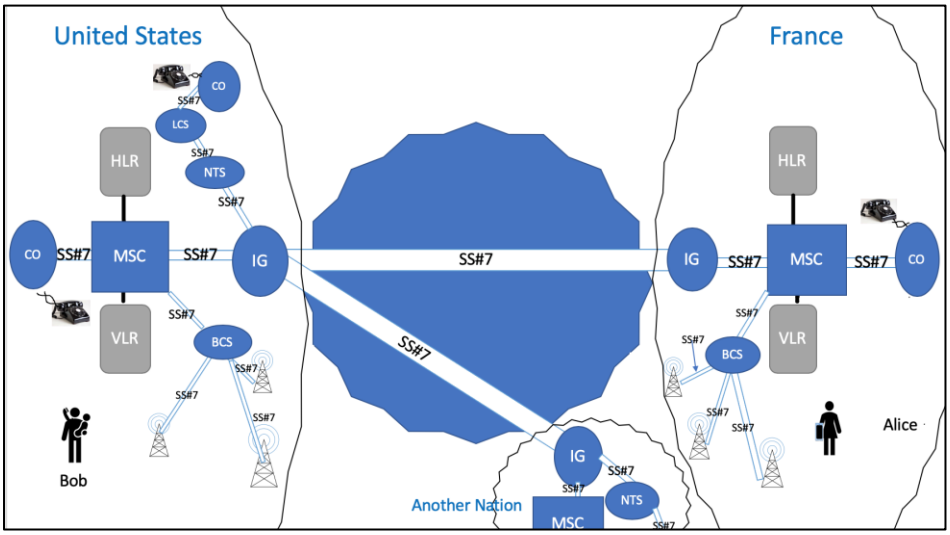

Figure 3: International Mobile Calling: Showing Switches and Connections[144]

In other words, no one place in the network has full information about which number is connecting to which; each MSC has only partial information, albeit *sufficient partial information* to enable the connection. CDRs collected in one place (e.g., the New York MSC) may well show different numbers connecting in a different place (e.g., the Paris MSC). If the CDR collected is showing an incorrect number, subsequent CDRs will be collected against the wrong number, but that the record held an incorrect number will not be obvious from the CDR itself.

Recall Richards's comment that, "[the] record on its face did not look like it had a problem, but a comparison with other records [showed] it had a problem."[145] An incorrect CDR stemming from the fact that different parts of the network know different pieces of the connection would explain why comparing the records with other records demonstrated a problem. Our explanation fits with Richards's statement that the record looked fine "on its face." It also fits the issue that an incorrect record happens sometimes, not all the time or even frequently. Other explanations proffered for the problem with collection, including that some

[144] We include International Gateways ("IG"), National Transit Switches ("NTS"), Local Transit Switches ("LTS"), and local network's Central Offices ("CO") in this diagram; these are all part of the phone network. In the interest of diagram simplicity, we do not have all possible configurations (including the connections between "Another Nation" and France).

[145] Telephone interview by Susan Landau and Asaf Lubin with Rebecca "Becky" Richards, NSA Civil Liberties and Privacy Officer (Oct. 31, 2018).

CDRs included location information, would not look fine "on its face."[146] Our analysis fits the known facts and how switching technology works.

A critical nuance may be what NSA said, namely that it was infeasible to isolate properly produced data. The agency did not say it was impossible to do so and refused to answer why when asked. It seems very likely that the program ended because it no longer had much value.

III. The Effectiveness of the CDR Program in Light of the Changing Communications Environment

We now examine how foreign-inspired terrorists have operated within the United States over the past five years and show how the evolution in foreign terrorist communication has shifted the way the IC conducts counterterrorism investigations.

A. *How Methods of Communications Have Evolved*

Over the last two decades, we have seen a dramatic change in electronic communications, one that continues to evolve at an unprecedented rate. Three particular changes stand out: (1) worldwide adoption of cellular communication in the 2000s; (2) use of mobile and SMS-text inside the United States; and (3) the subsequent move to smartphones and IP-based communications.

Worldwide adoption of mobile communications took off between 2000 and 2010. In Yemen, for example, the number of mobile phone subscriptions grew from fewer than 1 in 500 people in 2000 to 47 in 100 in 2010.[147] A similar trend occurred in other countries of importance to U.S. counter-terrorism intelligence operations. In 2000, the number of subscriptions per 100 people stood at zero in Afghanistan, Iraq, and Libya.[148] By 2010, those numbers had shifted significantly to 35 in 100, 55 in 100, and 177 in 100, respectively.[149] With few exceptions, the rest of the developing world saw similarly rapid growth.

With this new technology, the signaling message is picked up along with the call. The missed connection between Yemen and San Diego in 2001 by U.S.

---

[146] The Privacy and Civil Liberties Oversight Board confirmed this: "[W]hen receiving CDRs from providers, NSA's validation checks could detect if a provider had accidentally sent additional data fields forbidden by the statute, such as subscriber name or cell-site location information." PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE GOVERNMENT'S USE OF THE CALL DETAIL RECORDS PROGRAM UNDER THE USA FREEDOM ACT 48 (Feb. 2020), https://www.pclob.gov/library/PCLOB%20USA%20Freedom%20Act%20Report%20(Unclassified).pdf [https://perma.cc/XXP2-96EM] [hereinafter Government's Use of the CDRs].

[147] *Mobile Cellular Subscriptions (per 100 people)*, WORLD BANK, https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=AF-IQ-LY&veiw=chart [https://perma.cc/RUZ6-VHHA] (last visited Apr. 30, 2020).

[148] *Id.*

[149] *Id*. The number for Libya is correct; some people have more than one mobile cellular subscription.

intelligence was an artifact of an old switching technology. The new infrastructure included phone technology that, *had it been in use in 2001*, would have revealed the number of the other end of the communication calling the Al-Qaeda safe house in Sana.

The United States also experienced the growth of cell-phone technology during the period between 2000 and 2010. Cellular subscriptions grew from 62% of the population in 2002 to 85% by 2010, while voice calls over the phone network declined.[150] The shift continued into the 2010s, with texting becoming the preferred means of communications for those aged 18 to 34.[151] Use of social media created virtual communities and networks and the last decade has seen a move towards IP-based applications. In 2010, such applications were largely on the desktop, but smartphones have enabled people to stay connected at all times—while waiting for lunch, before a movie, in a taxi—thereby increasing the number of daily IP-based communications and user-generated content.

By 2016, smartphones and tablet devices surpassed desktop computers as the primary means of going online.[152] As of 2019, 81% of all American owned a smartphone, with "roughly one-in-five American adults [being] 'smartphone-only' Internet users."[153] The transition to IP-based communications significantly increases the amount and type of data generated; at the same time a changing technological landscape decreases the value of CDRs. Use of voice calls is dropping; the wireless trade association, CTIA, reports a decrease in number of minutes of use between 2015 and 2016,[154] and that trend is continuing. Federal Communications Commission ("FCC") Commissioner Michael O'Rielly reports: "Many of the legacy wireless cellphone functions are being overtaken by Internet apps, such as Skype, FaceTime, WhatsApp and Facebook messenger."[155] Consider the following two examples.

The messaging app iMessage contacts an Apple server whenever a new phone number is used.[156] The server then determines whether to route through Apple's iMessaging system as an IP-communication or over the public-switched telephone network as an SMS text. If the communication is IP-based, then the user will see blue bubbles; if it is an SMS text, the user will see green ones. Apple collects metadata around those queries, recording each number or IP address, date,

---

[150] *Mobile Fact Sheet*, PEW RESEARCH CENTER (June 12, 2019), https://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/LKV8-8RZN].
[151] *See* RICHARD K. MILLER & KELLI WASHINGTON, CONSUMER USE OF THE INTERNET AND MOBILE WEB 2018–2019, at 196–98 (4th ed. 2019).
[152] *Id.*
[153] *See Mobile Fact Sheet*, *supra* note 150.
[154] FED. COMMC'N COMM'N, *supra* note 105, at 72.
[155] FED. COMMC'N COMM'N, *supra* note 105, at 92.
[156] *See Legal Process Guidelines: Government and Law Enforcement within the United States*, APPLE 12, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/XS83-589P] (last visited Apr. 7, 2020).

and time of the communication.[157] Apple stores this information for 30 days.[158] Apple is headquartered and registered in the United States and is thus subject to the jurisdiction of U.S. courts. Thus, the company could be presented with "pen register" or "trap and trace" court orders seeking to acquire this metadata. The CDR program could only be useful in collecting metadata around the "green" messaging, which go over the PSTN network. The blue bubbles represent IP-based communications that are therefore outside of the telephony CDR collection (this limitation appears to be a decision of the IC rather than a legal requirement; see Section III.c.1).

On the other end of the spectrum are applications such as Telegram, which allows for "secret chats" that are end-to-end encrypted so that only the sender and receiver can read the message. The secret chats leave no information, support self-destruction (the message is deleted from the recipient's device after a fixed time), and do not allow the recipient to forward the message (nothing prevents the recipients from retyping and sending of course).[159] Messages are not stored on Telegram's cloud and can only be accessed on their devices of origin.[160] Telegram stores the user phone's contact lists on its server. This challenge of collection against Telegram is not only technological, but also jurisdictional, as the company operates from Dubai.[161]

These examples highlight how evolving IP-based applications make CDR collection less useful.

B. *How Terrorist Methods of Communications Have Evolved*

A useful example to consider is that of the perpetrators of the Garland Texas shooting. On May 3, 2015, Elton Simpson and Nadir Soofi opened fire outside the Garland Curtis Culwell Center, which was hosting an exhibit of images mocking the prophet Muhammad.[162] Both attackers were promptly shot and killed by an off-duty police officer guarding the center.[163] ISIS later claimed responsibility for this attack.[164] But there are no indications that ISIS members had actually instructed the

---

[157] *See id.*
[158] Sam Biddle, *Apple Logs Your iMessage Contacts and May Share Them with Police*, THE INTERCEPT (Sept. 28, 2016), https://theintercept.com/2016/09/28/apple-logs-your-imessage-contacts-and-may-share-them-with-police/ [https://perma.cc/83FP-CCVN].
[159] *See Telegram FAQ*, TELEGRAM, https://telegram.org/faq#q-how-is-telegram-different-from-whatsapp [https://perma.cc/8T4H-F9FK] (last visited Apr. 7, 2020).
[160] *Id.*
[161] *Telegram FAQ, Where is Telegram Based?*, TELEGRAM, https://www.telegram.org/faq#q-where-is-telegram-based [https://perma.cc/N5KS-JBFT] (last visited Apr. 7, 2020).
[162] Adam Goldman & Matt Berman, *FBI Had Known About Suspected Texas Shooter for Years*, WASH. POST (May 4, 2015), https://www.washingtonpost.com/news/post-nation/wp/2015/05/04/fbi-had-known-about-suspected-texas-shooter-for-years/ [https://perma.cc/MQ8J-AGXK].
[163] *Id.*
[164] Evan Perez et al., *Texas Attacker Had Private Conversations with Known Terrorists*, CNN (May 7, 2015), https://www.cnn.com/2015/05/07/politics/fbi-warning-elton-simpson-cartoon-event-attack/index.html [https://perma.cc/K8ZK-VTXX].

perpetrators to carry out the attack or provided them with material support beyond mere encouragement and inspiration over social media and encrypted messaging apps.[165]

In the days before the attack, Mohammed Abdullahi Hassan, an American in Somalia who had been contributing to ISIS's online radicalization efforts, tweeted a link to the exhibit calling on jihadists to follow the example set by the Charlie Hebdo shooters.[166] Simpson responded to Hassan's tweet by suggesting "if there were jihadists like that in the U.S., people would not draw Mohammed."[167]

In March 2015, Simpson had begun corresponding with ISIS recruiter Junaid Hussain.[168] The men started on Twitter, then switched to SureSpot, an open source end-to-end encrypted messaging application.[169] Hussain seemingly showed early knowledge of an impending strike and would later boast about the fact that through his communications with Simpson he "helped direct the attack."[170]

The Simpson case exemplifies what has become the typical process of radicalization through online communication undertaken by most homegrown domestic terrorists in the United States. Social media is traditionally the launching pad for this process. At the height of the caliphate, in 2014, the ISIS social media wing ran at least 46,000 Twitter accounts, with 20% of all followers of these accounts designating English as their primary language.[171] ISIS relied on intermediaries, some of whom operated from within the United States and connected ISIS radicalizers with Americans showing potential interest in carrying out attacks on U.S. soil.[172] As the Simpson case highlights, a mere response or retweet could be enough for ISIS to focus attention on a specific individual with an eye towards recruitment. Once an initial correspondence begins, communications usually transition from the public platform to an encrypted messaging app.

---

[165] *Id*.
[166] Sean Holstege & Matthew Casey, *Elton Simpson's Low, Isolated Descent Into ISIS, Jihad*, AZ CENTRAL (May 9, 2015), https://www.azcentral.com/story/news/local/phoenix/2015/05/09/slow-isolated-descent-jihad-phoenix-resident-elton-simpson-texas-shooting/27060211/ [https://perma.cc/F3EU-885J].
[167] *Id*.
[168] Del Quentin Wilber, *Here's How the FBI Tracked Down a Tech-Savvy Terrorist Recruiter for the Islamic State*, L.A. TIMES (Apr. 13, 2017), https://www.latimes.com/politics/la-fg-islamic-state-recruiter-20170406-story.html [https://perma.cc/EV8F-UUCA].
[169] *Id*.
[170] *See* Nafees Hamid, *The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain*, 11(4) CTCSENTINEL 34, 35 (2018).
[171] *See* Robin Maria Valeri, *From Declarations to Deeds: Terrorist Propaganda and the Spread of Hate and Terrorism Through Cyberspace*, *in* TERRORISM IN AMERICA, 147, 153–54 (Kevin Borgeson & Robin Valeri eds., 2018).
[172] Press Release, U.S. Dep't of Justice, Jalil Ibn Ameer Aziz Sentenced for Conspiracy to Provide Material Support and Resources to a Designated Foreign Terrorist Organization and Transmitting a Communication Containing a Threat to Injure (Dec. 20, 2017), https://www.justice.gov/opa/pr/jalil-ibn-ameer-aziz-sentenced-conspiracy-provide-material-support-and-resources-designated [https://perma.cc/5S6Y-SBC6].

ISIS has relied heavily on apps such as WhatsApp, Surespot, Viber, Telegram, and Signal.[173] Telegram channels allow for mass propagation of news from the caliphate to targeted audiences, which becomes useful when Twitter accounts become vulnerable to stricter takedown efforts.[174] Some apps are not only end-to-end encrypted, but also provide users with the ability to send messages with a self-destruct timer. ISIS recruiters attend to communications security. Hussain, for example, would ask potential recruits to switch from Kik to Surespot; Kik did not offer end-to-end encryption, while SureSpot did.[175] Erick Jamal Hendricks, another online ISIS recruiter, tried various techniques to avoid detection. For example, he frequently changed his online handles on messaging apps and placed spaces between letters in texts.[176]

Recruiters are open to experimenting with new apps that might provide greater security. Beginning in mid-December 2018, ISIS-linked media groups suggested using RocketChat, an open-source messaging system for mobile and desktop systems.[177] In December 2018 an ISIS-related organization published a technical manual that demonstrated how to install and anonymously use RocketChat.[178]

In addition to social media and encrypted communications with recruiters, homegrown terrorists rely on the Internet to conduct research for their attacks. Zale Thompson, the hatchet-wielding man who attacked several police officers in Queens, NY in 2014 visited at least 277 sites connected to Al-Qaeda, ISIS, or jihad, in the nine months leading to the attack.[179] Faisal Mohammad visited multiple ISIS and other extremist websites in the weeks prior to stabbing people at the University of California, Merced.[180] Online research often leads to the identification of certain training materials published in jihadi magazines such as *Inspire* and *Dabiq*.[181]

---

[173] *See* MALCOLM NANCE & CHRIS SAMPSON, HACKING ISIS: HOW TO DESTROY THE CYBER JIHAD 176 (2017).
[174] *Id.* at 177.
[175] *See* Hamid, *supra* note 170, at 34.
[176] *See* Eric Heisig, *Undercover FBI Agent Testified He was Unaware of Plans for 2015 ISIS-Inspired Attack in Texas*, CLEVELAND NEWS (Mar. 9, 2018), https://www.cleveland.com/court-justice/2018/03/undercover_fbi_agent_testified.html [https://perma.cc/5AVV-6FG5].
[177] Rita Katz, *A Growing Frontier for Terrorist Groups: Unsuspecting Chat Apps*, WIRED (Jan. 9, 2019), https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps/ [https://perma.cc/U7DX-6C2A].
[178] *Id*.
[179] James Gordon Meek and Josh Margolin, *NYC Ax Attacker Was Consumed by Desire to Strike U.S. Authority Figures, Police Say*, ABC NEWS (Nov. 3, 2014), https://abcnews.go.com/US/nyc-ax-attacker-consumed-desire-strike-us-authority/story?id=26664787 [https://perma.cc/7ZJY-RBU3].
[180] Press Release, FBI Sacramento Press Office, Update on Investigation at University of California, Merced (Mar. 17, 2016), https://www.fbi.gov/contact-us/field-offices/sacramento/news/press-releases/update-on-investigation-at-university-of-california-merced [https://perma.cc/A9FW-BBNR].
[181] *See e.g.*, Zolan Kanno-Youngs & Scott Calvert, *After New York Attack, Investigators Ask: Should ISIS Material Be Online?*, WALL ST. J. (Dec. 15, 2017), https://www.wsj.com/articles/investigators-

In late 2018, FBI Director Wray described some of the investigatory challenges of such attacks:

> We, along with our law enforcement partners, face significant challenges in identifying and disrupting homegrown violent extremists. This is due, in part, to their lack of a direct connection with a foreign terrorist organization, an ability to rapidly mobilize, and the use of encrypted communications. In recent years, prolific use of social media by foreign terrorist organizations has greatly increased their ability to disseminate their messages. We have also been confronting a surge in terrorist propaganda and training available via the Internet and social media. Due to online recruitment and indoctrination, foreign terrorist organizations are no longer dependent on finding ways to get terrorist operatives into the United States to recruit and carry out acts of terrorism. Terrorists in ungoverned spaces – both physical and cyber – readily disseminate propaganda and training materials to attract easily influenced individuals around the world to their cause. They motivate these individuals to act at home or encourage them to travel.[182]

The IC faces a new challenge trying to prevent attacks by violent-prone individuals who follow an online radical template. These lone-wolf attackers might not be capable of joining a terrorist organization, but they answer ISIS's call to carry out attacks deep in the heart of western societies.

C. *How Investigative Methods Have Evolved in Light of the New Communications Environment*

1. The Decline in the Utility of CDRs

As the Privacy and Civil Liberties Oversight Board ("PCLOB") noted in 2014, the Section 215 CDR program "is not utilized in a vacuum."[183] The move towards IP-based communication by terrorists, including social media and encrypted communications, highlights the reasons for the reduction in efficacy of traditional CDRs. The USA Freedom Act's value can only be understood when compared to capabilities other legal authorities provide to the IC; this includes

---

looking-at-how-nyc-terror-suspect-found-radical-islam-online-1513339201 [https://perma.cc/CV28-VWY5]; Adam Nagourney et al., *Neighbor of San Bernardino Attackers Faces Terrorism Charges*, N.Y. TIMES (Dec. 17, 2015), https://www.nytimes.com/2015/12/18/us/san-bernardino-enrique-marquez-charges-justice-department.html [https://perma.cc/2P9T-ZYKE]; Richard Valdmanis, *Boston Bomb Suspect Influenced by Al Qaeda: Expert Witness*, REUTERS (Mar. 23, 2015), https://www.reuters.com/article/us-boston-bombings-trial/boston-bomb-suspect-influenced-by-al-qaeda-expert-witness-idUSKBN0MJ0Z620150323 [https://perma.cc/QSK9-27BA].

[182] Wray, *supra* note 65, at 2–3.

[183] *See* PCLOB Section 215 Report, *supra* note 29, at 144.

signals intelligence NSA captures under Section 702, Executive Order 12333,[184] and traditional wiretaps. To this growing menu, one might add more traditional FBI techniques: 48% of all lone-wolf attackers in the United States are monitored by FBI informants, 26% are implicated through a tip from family or community members, while 9% come through a tip from the general public.[185]

Former PCLOB Executive Director Sharon Bradford Franklin has argued that, based on the language of the law, the CDR program could encompass metadata from encrypted messaging apps.[186] There is no public information on this, but we do not believe it is occurring. Our rationale is based on practicality. In 2011, the NSA discontinued a program to collect metadata from email communications "for operational and resource reasons."[187] The USA FREEDOM Act program is quite stringent—notably more so than the authorities under which the CDR program was working in 2011. IP-based communications applications are far more complex than PSTN-based ones—and they are constantly changing. Applying the USA FREEDOM Act to IP-based communications would require specific authorizations for every protocol and app. In a world of ever-changing IP-based communications—new ones developed seemingly weekly—obtaining FISC approval for each new application is complex and time consuming.

It seems far more likely that Section 702's authorities for the collection of the metadata and content of Internet communications offer far greater flexibility in addressing these pressing needs. This is also the view of independent journalist Marcy Wheeler.[188] Note, though, that there is not a direct trade of 702 authorities for those of 215. Targets under Section 702 cannot include U.S. persons or people located in the US, while they can under Section 215.

The Section 215 CDR program in its current structure thus seems to provide a decreasing value in the investigation of international terrorism. Indeed, in 2019, the NSA told the Privacy and Civil Liberties Board that "traditional telephony data, like that obtained under the CDR program, was unlikely to show a terrorist's

---

[184] *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *amended by* Exec. Order No. 13,470, 3 C.F.R. 218 (2009), *reprinted as amended in* 50 U.S.C. § 3001 app. at 418–27 (Supp. 1 2013). President Ronald Reagan signed Executive Order 12333 in 1981; it created a framework for foreign intelligence collection activities, including electronic surveillance conducted outside the United States as well incidental electronic surveillance collection against U.S. persons. Note that EO 12333 has been updated since 1981. *See also* Donahue, *supra* note 5, at 144–47.

[185] *See* Wright, *supra* note 61, at 113; *see also* New America Report, *supra* note 62.

[186] *See* 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), https://www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records/ [https://perma.cc/QWU9-MSAT].

[187] *See* Glenn Greenwald & Spencer Ackerman, *NSA Collected US Email Records in Bulk for More Than Two Years under Obama*, THE GUARDIAN (Jun. 27, 2013), https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama [https://perma.cc/JW86-6FW7].

[188] *See* Marcy Wheeler, *Surveillance Whack-A-Mole, Section 215 to Section 702 Edition*, EMPTYWHEEL BLOG (Mar. 6, 2019), https://www.emptywheel.net/2019/03/06/surveillance-whack-a-mole-section-215-to-section-702-edition/ [https://perma.cc/K9BJ-LZEA].

complete social network because it did not account for other modes of communication."[189]

What intelligence gaps would be created if the program is not renewed? Two important aspects of the CDR program come to mind. First, the program allows for the storage of CDRs around specific seeds meeting a RAS threshold of potential ties to international terrorism. As the National Academies study on bulk collection concluded:

> If past events become interesting in the present, because intelligence-gathering priorities change to include detection of new kinds of threats or because of new events such as the discovery that an individual is a terrorist, historical events and the context they provide will be available for analysis only if they were previously collected.[190]

Second, Section 215 has a "second hop" feature allowing investigators to move from the known target to other entities across a chain. This feature of the Section 215 program does not currently exist under either Section 702 authorities or traditional FISA warrants.

It is impossible to know, based solely on publicly available information, whether the loss of these two features of the Section 215 program would create a national-security risk. But given the declining value of the program, and the apparent fact that NSA has chosen to suspend it, this seems unlikely. The 2020 Privacy and Civil Liberties Oversight Board report on the USA FREEDOM Act program included NSA's statement that "an intelligence program of similar duration and cost would be expected to produce thousands or tens of thousands of reports."[191] Instead the CDR program produced only 15 reports over several years.[192]

Congress, in its intelligence oversight capacity, should ask if there is any reason to expect the numbers to be different in the future. However, for two different reasons, that seems highly unlikely. Of the 15 reports, "11 duplicated information that was already present in FBI files;"[193] two others had information that FBI had received from other sources.[194] And second, as already noted, terrorists communicate by multiple methods; the NSA observed that the CDR collection is unlikely to unveil the terrorist's full social network.[195]

---

[189] *See* Government's Use of the CDRs, *supra* note 146, at 27 n.126.
[190] *See* National Research Council's Bulk SIGINT Collection Report, *supra* note 10, at 9.
[191] *See* Government's Use of the CDRs, *supra* note 146, at 28.
[192] *See* Government's Use of the CDRs, *supra* note 146, at 62.
[193] *See* Government's Use of the CDRs, *supra* note 146, at 31.
[194] Government's Use of the CDRs, *supra* note 146, at 31.
[195] *See* Government's Use of the CDRs, *supra* note 146, at 27.

2. The Increased Value of Section 702 Authorities

The move towards social media and other forms of IP communications has not only reduced the value of the Section 215 metadata program; it also increased the value of Section 702's authorities. As previously discussed, between PRISM and upstream collection, NSA can compel the assistance of U.S.-based electronics communications service providers and companies that control the telecommunication "backbone." These companies release to the NSA both the contents and metadata around communications of foreign persons who are reasonably believed to be located abroad.

The IC has made the value of Section 702 clear. PCLOB noted that as of 2014, "over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted."[196] IC leadership has repeatedly affirmed that Section 702 now provides "critical foreign intelligence that cannot practicably be obtained through other methods."[197] In a Congressional hearing in June 2017, then NSA Director Admiral Michael Rogers said that the 702 collection is "more and more impactful for us. It generates more and more value."[198] Former Director of the National Counterterrorism Center Matthew Olsen concurred:

> Against this backdrop of a dynamic and lethal terrorism threat posed by ISIS, the ability of the United States to conduct surveillance under Section 702 is vital to our security. Through the surveillance of communications under this authority, the government gains information that is often unavailable from other sources about the identities of terrorists, their networks, and their plans and capabilities. This surveillance allows the government to peer inside highly secretive terrorist organizations that are difficult to penetrate and to obtain unvarnished intelligence about how these groups operate and seek to carry out attacks, often long before plots are executed... Moreover, the flexibility of Section 702 collection, according to the PCLOB, enables the government to maintain

---

[196] *See* PCLOB Section 702 Report, *supra* note 18, at 10.

[197] *FISA Amendments Act: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 9 (2016) (joint unclassified statement of Robert S. Litt, Gen. Counsel of the Office of the Dir. of Nat'l Intelligence, Stuart J. Evans, Dep. Asst. Att'y Gen. for Intelligence, U.S. Dep't of Justice, Michael B. Steinbach, Ass. Dir. Counterterrorism Div., Federal Bureau of Investigation & Jon Darby, Chief of Analysis and Production, Signals Intelligence Directorate, Nat'l Sec. Agency), https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2016/02/17/508_compliant_02-02-16_fbi_litt_evans_steinbach_darby_joint_testimony_from_february_2_2016_hearing_re_fisa_amendments_act.pdf [https://perma.cc/FHX8-6MPQ].

[198] *FISA Legislation: Hearing Before the Select Comm. on Intelligence*, 115th Cong. 41 (2017) (statement of Admiral Michael Rogers, Dir., Nat'l Sec. Agency, Commander, U.S. Cyber Command), https://www.intelligence.senate.gov/sites/default/files/hearings/S.%20Hrg.%20115-84.pdf [https://perma.cc/3FYQ-HTPD].

> coverage on particular individuals as they add or switch their modes of communications.[199]

The IC has publicized cases in which Section 702 was used in thwarting the ISIS terrorist threat. ISIS recruiter Shawn Parson was an active member of ISIS's English-speaking media effort, using social media to encourage terrorist attacks against specific U.S. soft targets.[200] The IC used Section 702 to determine members of Parson's propaganda network.[201] This was used to prevent ISIS recruitment efforts, ultimately leading to the 2015 drone that killed both Parson and Junaid Hussain.[202] The IC relied almost exclusively on Section 702 to monitor the communications of his close associate, Abdulrahman Mustafa al-Qaduli (known as Hajji Iman), who was at one point considered ISIS's second in command.[203] Iman was killed during an operation in March 2016.[204]

While encryption may prevent U.S. government agencies from reading the communications, use of messaging apps allows for significant intelligence to be gleaned from the communications metadata. SureSpot, for example, stores usernames, friend and block relationships, time stamps on messages, and the total number of messages and images sent by a user.[205]

Based in Colorado, SureSpot is under U.S. jurisdiction, but not all companies supplying IP-based messaging applications are. RocketChat, for example, was produced by a Brazilian company and Telegram is now based in Dubai. The ability of investigators to compel these companies to release metadata depends on either collaboration with local law enforcement or on voluntary disclosures made by the companies. Nonetheless, with the majority of social media

---

[199] *The FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties: Hearing Before the S. Comm. on the Judiciary*, 115th Cong. 3–4 (2017) (statement of Matthew G. Olsen, Former Dir., Nat'l Counterterrorism Ctr., Former Gen. Counsel, Nat'l Sec. Agency), https://www.judiciary.senate.gov/imo/media/doc/06-27-17%20Olsen%20Testimony.pdf [https://perma.cc/RT3K-D5YJ]. *See also* PCLOB Section 702 Report, *supra* note 18, at 107; *Reauthorization of FISA*: *Hearing Before the S. Comm. on the Judiciary*, 115th Cong. 3 (2017) (joint statement for the record of Bradley Brooker, Acting Gen. Counsel ODNI, Stuart Evans, Dep. Asst. Att'y Gen. for Intelligence, U.S. Dep't of Justice, Paul Morris, Dep. Gen. Counsel for Operations, Nat'l Sec. Agency, and Carl Ghattas, Exec. Asst. Dir. Nat'l Sec., Fed. Bureau of Investigation), https://www.judiciary.senate.gov/imo/media/doc/06-27-17%20Brooker-Evans-Morris-Ghattas%20Joint%20Testimony.pdf [https://perma.cc/EMW5-L9EW].

[200] *See* OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, GUIDE TO SECTION 702 VALUE EXAMPLES 4 (Dec. 5, 2017), https://www.dni.gov/files/documents/icotr/Updated-Guide-to-Section-702-Value-Examples---Dec-2017-FINAL.pdf [https://perma.cc/T2XD-DJX3] [hereinafter Guide to Section 702 Value Examples].

[201] *Id*.

[202] *Id*.

[203] *See id.* at 2–3.

[204] *Id*.

[205] *Data and Threat Analysis*, SURESPOT ENCRYPTED MESSENGER, https://www.surespot.me/documents/threat.html [https://perma.cc/3EL8-GBA4] (last visited Mar. 25, 2020).

platforms operating from U.S. soil, the jurisdictional issues pose less of an immediate risk to Section 702's efficacy.

Section 702 serves other purposes beyond addressing the contemporary terrorist threat to the United States. It has been utilized on multiple occasions as a source of counterterrorism intelligence to foreign governments[206] and has been useful in addressing the emerging threat of cyber terrorism and state-sponsored cyber-attacks. As the potential for a cyber terrorist attack continues to mount, Section 702 will continue to be a useful counter-terrorism surveillance tool long into the future.

The various ways in which Section 702 has been used to tackle the contemporary foreign terrorist challenges highlight the shortcomings of the Section 215 program. Section 702 authorities correspond far better with the ways in which terrorists communicate in the post-smartphone, post-IP-communication era and are far more effective in thwarting terrorist plots and identifying new terrorist targets than Section 215 authorities.[207]

IV. Properly Framing the Issues

We began with three questions: Why, with only 40 targets, did NSA collect so many CDRs? What was the technical problem that caused the agency to purge three years of CDR records in May 2019? Is the CDR program efficacious as a counterterrorism investigative tool? Two questions remain: What would have helped Congress understand in 2015 that the time for the CDR collection had passed? What should Congress do now?

A. *Why Didn't Congress Know in 2015 that the CDR Collection was No Longer Useful?*

When Edward Snowden disclosed the CDR program in June 2013, President Obama felt compelled to explain what it was about: "When it comes to telephone calls, nobody is listening to your telephone calls."[208] Many in the government who knew of the bulk metadata collection assumed the public would have no problem with it. The President's initial public statements on the program reflected that assumption. But already in 2013, a time when the words "communications metadata" were not particularly well known, the public understood that call histories reveal a significant amount of personal information about an individual. The public's immediate response to the bulk collection

---

[206] *See* Guide to Section 702 Value Examples, *supra* note 200, at 1–2.
[207] *Cf.* PCLOB Section 702 Report, *supra* note 18, at 107. This contrasts PCLOB Section 215 Report, *supra* note 29, at 146.
[208] THE WHITE HOUSE, OFFICE OF THE PRESS SEC'Y, STATEMENT BY THE PRESIDENT (Jun. 7, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president [https://perma.cc/4PEW-BREF].

program was strongly negative. Congress took notice, focusing largely on the program's infringement of privacy rights and civil liberties.

While the President's Review Committee and PCLOB considered efficacy, that issue was not on Congress's radar. Yet understanding efficacy—the goals of a surveillance program and how well it achieves them—is essential to striking a balance between privacy and civil liberties on the one hand, and public safety and security on the other. Unlike the more expansive concerns over the balance between privacy and security, questions of efficacy are not philosophical or constitutional; they are rooted in pragmatism. These are descriptive rather than normative questions. Using analysis of various different types—understanding the changes in communications technologies, the trends in their use, the changes in foreign terrorist organizations, and the resulting changes in how those groups "direct" attacks on the U.S—we have shown that the CDR collection has not been efficacious and *that it is unlikely to be so in the future*. This analysis demolishes the argument for continuing the program.

This Article's value lies in the analysis explaining why the CDR collection authority is no longer useful in combatting foreign-instigated domestic terrorism; that is why the Article is largely analytical rather than prescriptive. Our analysis makes clear that, at the time the act passed, the value of the CDR collection had already waned. During the course of our research, one of us asked former NSA Deputy Director Chris Inglis about this conclusion. Inglis concurred, saying, "There is some truth to it."[209]

Indeed, ODNI has been public about this for some time. Consider how ODNI described Section 702. Well before the Snowden revelations surfaced, in a letter dated May 4, 2012, then-Director of Legislative Affairs at ODNI Kathleen Turner and Assistant Attorney General Ronald Weich wrote the Senate Select Committee on Intelligence highlighting the increasing importance of Section 702 over all other FISA authorities, describing the 702 powers as a "critical tool in the Government's efforts to acquire foreign intelligence necessary to protect the nation's security."[210] The two suggested reauthorization was a "top legislative priority of the intelligence community."[211] In the wake of the 2017 sunsetting of the Section 702 program, and prior to its reauthorization, NSA's General Counsel Glenn Gerstell argued, "Section 702 represents one of NSA's most important intelligence surveillance authorities, and it provides tremendous value in the

---

[209] Telephone interview by Susan Landau with Chris Inglis, former Dep. Dir., Nat'l Sec. Agency (March 4, 2019).
[210] Letter from Kathleen Turner, Dir. of Legis. Affairs, Office of the Dir. of Nat'l Intelligence, and Ronald Weich, Assistant Att'y Gen., Office of Legis. Affairs, U.S. Dep't of Justice to Sen. Dianne Feinstein and Sen. Saxby Chambers of the Select Comm. on Intelligence (May 4, 2012), https://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf [https://perma.cc/JU6L-NWUF].
[211] *Id.*

nation's fight against foreign terrorists."[212] He explained, "a failure to reauthorize Section 702 would place the U.S. at a perilous disadvantage, hindering our ability to identify and respond to threats against the nation and our allies."[213]

Compare this powerful language to the pallid statements made concerning the bulk telephony metadata program prior to the 2015 enactment of the USA FREEDOM Act and introduction of a constrained CDR program. When called to showcase successful uses of the program, members of the IC would often bundle its use with the Section 702 authorities, referring to them together as the "bulk collection programs."[214] For example, in defending the Section 215 metadata program, NSA Director Keith Alexander argued that these bulk collection programs as a unitary whole "contributed to our understanding, and in many cases helped enable the disruption of terrorist plots."[215] Attorney General Loretta Lynch and Director of National Intelligence James Clapper wrote to Congress, citing Section 215 alongside FISA pen registers and National Security Letters as providing "essential operational capabilities" and arguing that, in the absence of authorizing legislation that would keep all programs running, the IC would lose "important intelligence authorities."[216]

This was misleading. The Justice Department's Inspector General's report, released a few weeks prior to the USA FREEDOM Act's authorization vote in Congress, had reached the very opposite conclusion about the bulk metadata collection. It noted that the majority of interviews conducted with FBI agents, "did not identify any major case developments that resulted from use of the records obtained in response to Section 215 orders."[217] But NSA continued to publicly endorse the program's value.

---

[212] Glenn S. Gerstell, Gen. Counsel, Nat'l Sec. Agency, Judicial Oversight of Section 702 of the Foreign Intelligence Surveillance, Presented to The Robert S. Strauss Ctr. for Intern'l Sec. & L. & The Univ. of Tex. Sch. of L., Austin, Texas (Sep. 14, 2017), https://icontherecord.tumblr.com/post/176443831313/judicial-oversight-of-section-702-of-the-foreign [https://perma.cc/3UPN-56YR].

[213] *Id.*

[214] See *supra* notes 25, 26 and accompanying text (NSA Director Keith Alexander would cite to both the both Section 215 and 702, as the two "bulk collection programs", whenever asked to defend the former's usefulness to the IC).

[215] Gen. Keith Alexander, Commander, U.S. Cyber Command, Dir., Nat'l Sec. Agency, Chief, Central Sec. Service, Remarks at AFCEA Int'l Cyber Symposium (Jun. 28, 2013), https://www.nsa.gov/news-features/speeches-testimonies/Article/1620137/remarks-by-gen-keith-alexander-commander-us-cyber-command-uscybercom-director-n/ [https://perma.cc/MM7W-LC2G].

[216] Letter from Att'y Gen. Loretta E. Lynch and Dir. of Nat'l Intelligence James R. Clapper to Sen. Patrick J. Leahy and Mike S. Lee (May 11, 2015), https://www.leahy.senate.gov/imo/media/doc/5-12-15%20AG.DNI%20Response.pdf [https://perma.cc/ZG27-E5WS].

[217] OFFICE OF THE INSPECTOR GENERAL, U.S. DEPARTMENT OF JUSTICE, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS: ASSESSMENT OF PROGRESS IN IMPLEMENTING RECOMMENDATIONS AND EXAMINATION OF USE IN 2007 THROUGH 2009, at 44 (2015), https://oig.justice.gov/reports/2015/o1505.pdf#page=1 [https://perma.cc/23T4-XB6N].

There are two possible explanations for this. One may have been political pressure. A former official said that following the disclosures, "There was a great desire to circle the wagons. If Snowden hadn't revealed [the metadata program], NSA probably would have dumped it on their own."[218] Another may have been the program's peripheral value in supporting investigations. As Inglis explained, "If you could get [the metadata program] under control, it was still useful. [But] zero tolerance is the real driver here."[219] Avoiding all domestic terrorist attacks is a worthy goal, yet it seems implausible in the face of the current wave of jihadist-inspired homegrown attacks.

To anyone carefully reading the tea leaves, it was clear by the mid-2010s that members of the IC saw diminishing returns from the CDR program.

That Congress reauthorized the program anyway underscores several failures. First, the IC did not publicly clarify that the CDR program which was already of waning value, and this value was likely only to decrease further. Second, Congress failed to ask the right questions. In debating the USA FREEDOM Act, Congress focused on the civil liberties and privacy risks of the previous program, but it did not carefully examine issues of efficacy. And yet the information behind the arguments in this Article—the revolution in communications technologies, trends in their use, and transitions in how foreign terrorist organizations operate—were in the public domain. The IC understood how the future was trending; Congress did not. The lesson is clear. In intelligence oversight, study the trees, but never lose sight of the forest.

Technological changes now occur not at the speed of the Industrial Revolution, spanning a century, but at Internet speed, spanning just months. Understanding the import of these changes and anticipating future changes are necessary to considering the future of USA FREEDOM Act—and all other U.S. intelligence programs. Congress must have the resources it needs to ask the right questions and properly exercise its mandate as an intelligence oversight body. This does not seem to be the case at present. The Congressional Research Service reports that the intelligence committees have approximately the same number of staff as they did in 1987,[220] even though their challenges have grown far more complex. Access issues compound the staff resources challenge. Only congressional staffers who staff certain committees (such as Intelligence, Foreign Services, Armed Services, and Homeland Security) can get TS/SCI clearances.[221] Members of

---

[218] Ellen Nakashima, *Repeated Mistakes in Phone Record Collection Led NSA to Shutter Controversial Program*, WASH. POST (Jun. 26, 2019), https://www.washingtonpost.com/world/national-security/repeated-mistakes-in-phone-record-collection-led-nsa-to-shutter-controversial-program/2019/06/25/f256ba6c-93ca-11e9-b570-6416efdc0803_story.html [https://perma.cc/BFX3-QGFC].

[219] Telephone interview by Susan Landau with Chris Inglis, former Dep. Dir., Nat'l Sec. Agency (Dec. 19, 2018).

[220] *See* R. ERIC PETERSEN & AMBER H. WILHELM, CONG. RESEARCH SERV., R43946, SENATE STAFF LEVELS IN MEMBER, COMMITTEE, LEADERSHIP, AND OTHER OFFICES, 1977-2016, at 9–11 (2016), https://fas.org/sgp/crs/misc/R43946.pdf [https://perma.cc/4G6V-NK4D].

[221] These would be TS/SCI—Top Secret/Sensitive Compartmented Information—clearances.

Congress not on those particular committees cannot obtain full TS/SCI clearances for their staff, constraining their own ability to fully review classified information about collection.

The issue extends well beyond the intelligence committees. Sufficient expertise in new and emerging technologies and the implications of their use must be available to Congress so that legislation reflects technological realities of the future. Laws must be made for the world that is coming, and without access to technical expertise, Congress cannot govern wisely or well. Since the dismantling of the Office of Technology Assessment ("OTA") in 1995, Congress lacks internal bodies chartered to develop objective and authoritative analysis of complex scientific and technical issues. The introduction of designated funds for reviving the OTA into the 2020 spending bill might signal a shift in the right direction.[222]

B. *What Should Congress Do?*

In early March 2019, Luke Murry, national security adviser for House Minority Leader Kevin McCarthy, confirmed on the *Lawfare* podcast that collection under the CDR program had not taken place over the previous past six months. Murry suggested that the Administration may not seek to renew the UFA authorities undergirding the program.[223] Since then other members of the IC have come out against renewing the program; the Administration seems to have adopted the opposite view.[224] Regardless of what the Administration and IC ultimately decide to do, Congress should use the law's renewal as an opportunity to review the last three years of the program. Doing so gives an opportunity to examine three important issues.

First, Congress should examine programmatic shortcomings associated with its review and reauthorization process of intelligence authorities by asking questions, including:

1. Was the CDR program useful to the IC in the period of 2015–18 under the USA FREEDOM Act? What metrics were used to make this judgement?[225]

---

[222] *See* Press Release, H. Comm. on Appropriations, Appropriations Committee Releases Fiscal Year 2020 Legislative Branch Funding Bill (Apr. 30, 2019), https://appropriations.house.gov/news/press-releases/appropriations-committee-releases-fiscal-year-2020-legislative-branch-funding [https://perma.cc/ZM6R-MXK7].

[223] *See* Chesney, *supra* note 24.

[224] *See supra* notes 8, 9 and accompanying text.

[225] A 2018 report written by the Inspector General of the Intelligence Community concluded that "the IC did not have a formal process to assess the importance of information obtained using Section 215 authority." OFFICE OF THE INSPECTOR GENERAL OF THE INTELLIGENCE COMMUNITY, INS-2016-003, UNCLASSIFIED SUMMARY OF ASSESSMENT OF INTELLIGENCE COMMUNITY FOREIGN INTELLIGENCE SURVEILLANCE ACT TITLE V INFORMATION 3 (2016), https://int.nyt.com/data/documenthelper/1527-nsa-freedom-act-ig-reports-acl/8f5c47c23b1a63129136/optimized/full.pdf#page=1 [https://perma.cc/Z63E-MH6Q].

2. If not, could the IC have anticipated this in 2015 given the changes in communications technologies and organizational structure of foreign-based terrorist groups?
3. The 2015 National Academies study on technical alternatives for Bulk Signals Intelligence Collection observed that bulk collection was the only way to go back in history.[226] Does the abandonment of the program mean that use is no longer important? Could that have been anticipated in 2015?
4. What questions should Congress have asked in 2014 and 2015 that it failed to ask?
5. What changes could Congress implement in the way it conducts its intelligence oversight work to ensure these questions would be raised in the future?

One possible answer to the last question could involve shifting the focus of congressional hearings. As Tommy Ross notes, the "most mundane aspects of intelligence work—how agencies are organized, how personnel are recruited and developed, how programs are administered and executed, and how resources are budgeted and allocated" are critical for intelligence oversight.[227] As technology grows more complicated and intelligence capabilities become more pervasive, those engaging in oversight also need to understand each program's value in a changing threat environment. To the extent that the writing was already on the wall in 2015, Congress must ask itself how it renewed a controversial program under such public and legislative scrutiny without deeply examining efficacy. How can we avoid repeating this mistake in the future?

One looming issue is the growing importance of Section 702 in investigating cases of foreign-inspired U.S. domestic terrorism. Changes in U.S. domestic terrorism, specifically the rise of right-wing terrorism, could have wide ramifications here. The United States wrestled with the proper balance of investigations and civil liberties in the 1970s; striking this balance has grown harder as a result of new technologies. Congress cannot afford to ignore these concerns.

Second, many unanswered questions remain around the June 2018 purge and the broader usefulness of the program.[228] Answering these on the record—even in a closed hearing with answers redacted prior to publication—should be part of the public disclosure process that the IC has undertaken in the years since the

---

[226] National Research Council's Bulk SIGINT Collection Report, *supra* note 10, at 9.

[227] Tommy Ross, former Senior Advisor at both the House and Senate Intelligence Committees, observed "the committees rarely conduct hearings dedicated to oversight of these issues beyond routine budget hearings." Tommy Ross, *At a Crossroads, Part II: No More Shadows: The Future of Intelligence Oversight in Congress*, WAR ON THE ROCKS (May 16, 2018), https://warontherocks.com/2018/05/at-a-crossroads-part-ii-no-more-shadows-the-future-of-intelligence-oversight-in-congress/ [https://perma.cc/2DN6-2BLT].

[228] *See, e.g.*, Letter from Sen. Ron Wyden and Rand Paul to the Hon. Robert P. Storch, Inspector Gen. of the Nat'l Sec. Agency (Aug. 2, 2018), https://www.wyden.senate.gov/imo/media/doc/Storch%20Letter%2008.02.18.pdf [https://perma.cc/E3GH-RQD3].

Snowden disclosures. Congressional intelligence oversight committees should determine answers to the following:

6. What problem triggered the CDR purge? What controls did NSA put in place to prevent similar problems from arising in the future?
7. Did the purge of three years' worth of CDRs impact the ability to effectively conduct international terrorist investigations?

Finally, Congress needs to decide what to do with the CDR collection authority. It has three options. First, it may seek to sidestep potential controversies around reauthorization by adopting a blanket or "clean" extension of all the powers listed under the "business records" provision of FISA, with no amendments or changes.[229] Such an extension could be done with or without a new sunset clause, the latter approach seems to be favored by the White House.[230] While a straight reauthorization will keep the CDR authority on the books, it would not compel the government to operate the program. This would allow the IC to re-launch the program in the future, if technological shifts were ever to make it efficacious. This approach would also ensure that the same oversight checks introduced in UFA would remain operative should the program ever restart.

A second option would be to allow the authorities to expire. Professor Robert Chesney has advised against this, noting that much more than just the CDR authority would be lost.[231] For starters, three provisions of the USA PATRIOT Act—the roving wiretap provision, the lone wolf provision, and the full Section 215 "business records" provision (not just its current CDR program)—would sunset in December 2019.[232] Because Section 215 authorizes FISA court orders for business records separate from the CDR program for both counter-terrorism and counter-intelligence investigations, this provision will revert back to its pre-2001 USA PATRIOT Act form if Congress opts for complete expiration. The 1998 version of the business records provision excluded many categories subject to governmental reach and limited collection to records belonging to an alleged "agent of a foreign power."[233] Reverting to this version would weaken the FBI's ability to gather intelligence in a wide range of national security investigations.

If that is not enough, in the absence of the authorities created by UFA, nothing would stop a future president from reinstating bulk collection through an executive order (something that is currently prevented by the introduction of a "specific selection term" ("SST") under UFA). Expiration would also eliminate UFA's protections for FISC-order recipients and congressional reporting

---

[229] USA PATRIOT Act, Pub. L. 107-56, § 215, 115 Stat. 271, 287 (2001).
[230] *See* Nakashima, *supra* note 8.
[231] *See* Chesney, *supra* note 24.
[232] The law was extended until March 15, 2020 in the Further Continuing Appropriations Act of 2020 and Further Health Extenders Act of 2019, Section 1703 (a). As of this writing (April 2, 2020), it has not been extended.
[233] *See* Chesney, *supra* note 24.

requirements. For these reasons we do not recommend simply letting the authorities expire.

A third approach could be for Congress to tailor an amendment to the authorities that does not throw the baby out with the bath water. That said, the concerns that Caroline Lynch, former Chief Counsel to the House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, raised in her statement to PCLOB carry great weight:

> 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 the 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 Amendment Act reauthorization debate."[234]

We nonetheless believe that Congress should end the Section 215 program. To do so without damaging other authorities, Congress would need to carefully craft an amendment ending UFA's authorization for collecting CDRs on an ongoing basis, while retaining safeguards such as the requirement that all Section 215 applications include an SST as the basis for the production. Such an amendment would allow the government to continue to rely on Section 215 to collect business records without permitting a return to bulk collection.

The bottom line for a program, any program, should be efficacy—even more so when the program may violate privacy or civil rights. Press reports indicate that NSA has already recommended that the White House officially end the CDR collection program.[235] Thus our proposal is in line with the reported interests of the IC. We further recommend that the reauthorization of an amended Section 215 be subject to a sunset. In light of the rapid developments in telecommunications and terrorism discussed above, we argue that sunsets for foreign surveillance authorities be shortened and not exceed two-year time periods.

---

[234] *See* 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, 9 (May 31, 2019) (on file with the authors).
[235] *See* Volz & Strobel, *supra* note 9.

V. Conclusion

Whatever Congress ultimately decides to do with the specific CDR authority, the lessons from this episode should be understood within their broader context. As terrorists find new ways to organize themselves and plot attacks against the United States, and as technology continues to redefine our means of communication, the relative value of individual intelligence programs will evolve. A counterterrorism program that plays a critical role today may not be useful tomorrow. Intelligence oversight bodies must be alert to those changes, routinely and systematically reviewing the efficacy of each program under their supervision. Otherwise, we allow authorities that are neither necessary nor wise, and in so doing, protect neither our security nor our liberty.