



Privacy and Civil Liberties Oversight Board

Report on the Government's Use of the Call Detail Records Program Under the USA Freedom Act

Working to ensure that efforts by the Executive Branch to protect the nation from terrorism appropriately safeguard privacy and civil liberties.

February 2020

Privacy and Civil Liberties Oversight Board • PCLOB.gov • info@pclob.gov

Board Members

Adam I. Klein, Chairman

Jane E. Nitze

Edward W. Felten

Travis LeBlanc

Aditya Bamzai

Table of Contents

(U) Executive Summary	1
I. (U) Introduction	4
II. (U) NSA's Collection of CDRs under the USA Freedom Act	13
III. (U) Operational Use of the USA Freedom Act CDR Program.....	25
IV. (U) Legal Analysis	33
V. (U) Analysis of Privacy Risks.....	53
VI. (U) Statement of Chairman Adam Klein	59
VII. (U) Statement of Board Members Ed Felten and Travis LeBlanc	68
VIII. (U) Statement of Board Members Aditya Bamzai and Jane Nitze	79
(U) Appendix A	86
(U) Appendix B.....	97

(U) Executive Summary

(U) The Privacy and Civil Liberties Oversight Board (the “Board”) presents this report to provide greater transparency and clarity about the collection of phone call detail records (“CDRs”) under the USA Freedom Act. This authority is scheduled to sunset on March 15, 2020.

(U) The Board commenced work on this report in January 2019. Subsequently, in early 2019, NSA suspended its collection of CDRs under the USA Freedom Act. NSA halted the program “after balancing the program’s relative intelligence value, associated costs, and compliance and data-integrity concerns caused by the unique complexities of using these provider-generated business records for intelligence purposes.”¹ The Board proceeded to complete the report, which it offers to enhance the public’s understanding of the program and to assist Congress as it considers the reauthorization of statutory language related to the CDR program.

(U) Program Legality and Operation

(U) The USA Freedom Act amended the Foreign Intelligence Surveillance Act (“FISA”) to expressly bar the government from using its business records collection authority for bulk collection. This prohibition effectively ended the bulk telephony metadata program that the government had operated under the then-existing version of Section 215 of the USA Patriot Act.

(U) At the same time, the USA Freedom Act allows the government to obtain CDRs on a broader basis than other business records authorized for collection under the Act. Put simply, it authorizes the government to collect CDRs within two hops—*e.g.*, a person’s contacts, and those contacts’ contacts—of a specific selection term. Specific selection terms, such as a phone number or International Mobile Equipment Identity number, must be associated with a foreign power engaged in international terrorism and be approved by the FISA court. The Act also provides that CDRs cannot include the contents of any communication; the name, address, or financial information of a subscriber or customer; or cell-site location or global positioning system information. In 2018, the government obtained a relatively low number of FISA court orders—14—and collected a large number of CDRs—more than 434 million, including an unknown number of duplicates, involving 19 million phone numbers.

¹ (U) Letter from Director of National Intelligence Dan Coats to Senators Richard Burr, Lindsey Graham, Mark Warner, and Dianne Feinstein (Aug. 14, 2019).

(U) Findings

- (U) The CDR program was constitutional under settled Supreme Court precedent.
- (U) NSA's collection of two hops of CDR data on an ongoing basis was statutorily authorized.
- (U) The Board found no abuse of the program; nor did it find any instance in which government officials intentionally sought records that they knew were statutorily prohibited.
- (U) NSA acquired landline and wireless phone call records under the USA Freedom Act. The Board found no evidence that NSA received any of the statutorily prohibited categories of information, such as name, address, financial information, cell-site location information, or global positioning system information from providers during the program's operation.
- ~~(TS//NF)~~ NSA did not use this authority to obtain metadata associated with [REDACTED], or [REDACTED].

(U) Program Use and Value

(U) Findings

- (U) NSA typically used the CDR program in response to a terrorist attack or a known terrorist threat. For example, NSA produced intelligence reports that were derived in whole or in part from the USA Freedom Act CDR program in its analysis of the Pulse nightclub shooting in 2016 and the Ohio machete attack in 2016.
- (U) USA Freedom Act CDRs were cited in 15 intelligence reports over the program's four-year operation.
- ~~(S//NF)~~ Of the 15 reports citing USA Freedom Act CDRs, FBI received unique information from two of the intelligence reports. Based on one report, FBI vetted an individual, but, after vetting, determined that no further action was warranted. The second report provided unique information about a telephone number, previously known to US authorities, which led to the opening of a foreign intelligence investigation; [REDACTED]

(U) Data-Integrity Concerns and Compliance Incidents

(U) The program experienced a series of compliance incidents and data-integrity problems, which led NSA to issue about a dozen notices to the FISA court since 2016. After repeatedly discovering anomalies in the data it received, NSA suspended the collection of CDRs in early 2019. NSA subsequently deleted all CDRs collected under the USA Freedom Act.²

(U) Some of the compliance incidents were of types that could have arisen in other intelligence or equivalent law enforcement collection authorities. These include incidents involving information inadvertently omitted from a FISA court application, certain NSA officers who had access to data without required training, and a provider's production of data beyond the end date of an order.

~~(TS//SI//NF)~~ Other incidents raise questions unique to the contours of the USA Freedom Act. Beginning in 2016, NSA identified a series of data-integrity problems related to [REDACTED] and other data errors. In most of these cases, NSA systems unknowingly relied on inaccurate first-hop data to determine which second-hop requests to issue. Additional compliance incidents arose from other data errors, such as overwriting of data fields with incorrect or unrelated data.

(U) These problems, taken together, contributed to NSA's decision to delete the USA Freedom Act CDR data in 2018 and again in 2019, and its decision to eventually suspend the program.

(U) Findings

- (U) Based on a review of the facts, the Board determined that the compliance incidents were inadvertent, not willful.
- (U) NSA took steps to remedy each compliance incident, including notifying appropriate oversight entities, imposing additional limits on data requests, and deleting erroneously obtained data.
- (U) In response to each compliance incident that raised questions about the scope of permitted collection under the statute, NSA chose to follow a narrower, rather than a more expansive, understanding of its authority under the USA Freedom Act.

² (U) Whenever NSA deleted USA Freedom Act CDRs, it did not delete underlying data that had been used in disseminated intelligence reporting or data that was considered "mission management related information." This was consistent with NSA's minimization procedures. See Nov. 2015 Minimization Procedures Used by the National Security Agency in Connection with the Production of CDRs Pursuant to Section 501 of the Foreign Intelligence Surveillance Act, as amended ("NSA Minimization Procedures for CDRs").

I. (U) Introduction

(U) The Privacy and Civil Liberties Oversight Board (the “Board”) presents this report to provide greater transparency and clarity on how the government implemented certain authorities created or extended by the USA Freedom Act. In particular, the report examines collection of phone call detail records (“CDRs”) under the USA Freedom Act, which has proven to be of great public interest. CDRs include some of the information that typically appears on a customer’s phone bill: the date and time of a call, its duration, and the participating phone numbers. CDRs never include the content of phone conversations. The CDRs received under the USA Freedom Act also did not include names, street addresses, financial information, global positioning system information, or cell-site location information.

(U) The Board hopes this report will help Congress, executive branch agencies, and the public understand the government’s use of these authorities and any related privacy and civil liberties concerns, particularly in light of the impending sunset. The Board worked with other government agencies to declassify information to achieve the greatest degree of transparency consistent with the protection of classified or otherwise privileged information. As a result, some of the facts presented in this report are being disclosed to the public for the first time. The Board looks forward to further collaboration with Congress and other executive branch agencies to “ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.”³

A. (U) FISA and the Pre-2015 Bulk Collection Program

(U) Since 1998, the Foreign Intelligence Surveillance Act (“FISA”)⁴ has permitted the government to obtain business records for use in national-security investigations. Under the first iteration of this provision, the government could obtain business records associated with car rentals, storage units, public accommodations, and common carriers.⁵ Any request for business records in an investigation of a US person must be based on a counterterrorism or

³ (U) 42 U.S.C. § 2000ee(c)(2).

⁴ (U) FISA, originally passed in 1978, created a statutory regime regulating the government’s use of certain investigatory techniques for national security purposes. Among other things, FISA created a special court, comprised of Article III judges, to hear government applications to use those techniques. *See* 50 U.S.C. § 1801 *et seq.*

⁵ (U) 50 U.S.C. § 1862(b)(2)(B) (2000).

counterintelligence investigation that is not premised solely on activities protected by the First Amendment.⁶

(U) After the 9/11 attacks, Congress passed the USA Patriot Act,⁷ which revised the business records provision of FISA. Specifically, Section 215 of the USA Patriot Act expanded the business records provision to allow the government to request a FISA court order compelling the production of any “tangible things,” including books, records, papers, and documents that are relevant to an authorized FBI investigation.

(U) Under Section 215, the FISA court authorized the government’s collection of virtually all CDRs held by certain US phone providers.⁸ This collection program was commonly referred to as the “bulk” CDR program.⁹ Approximately every 90 days, the government filed an application with the FISA court requesting an order that providers continue to produce their CDRs to NSA.¹⁰ When the FISA court approved an application, the court issued orders, including secondary orders directly addressed to providers.¹¹ The secondary orders required the providers to produce their CDRs to NSA “on an ongoing daily basis” for the ninety-day duration of the order.¹²

(U) NSA stored these CDRs in a database that trained analysts could access as part of NSA’s counterterrorism mission.¹³ In 2013, NSA stated that the program enabled

⁶ (U) 50 U.S.C. § 1861(a)(1).

⁷ (U) The full name of the USA Patriot Act is the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.” Pub. L. No. 107-56 (2001) (codified as amended at 50 U.S.C. § 1861 *et seq.*).

⁸ (U) 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* (2014) [hereinafter 2014 Board Report], https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf; Amended Memorandum Opinion, *In re application of the Federal Bureau of Investigation for an Order requiring the Production of Tangible Things*, No. BR 13–109 (FISA Ct. Aug. 29, 2013); Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13–158 (FISA Ct. Oct. 11, 2013).

⁹ (U) The phrase “bulk” collection does not appear in FISA; rather, it is commonly used in this context to refer to the collection of large amounts of data that is not limited by a specific selection term or individualized suspicion. *Cf.* Presidential Policy Directive 28 (2014) (defining bulk collection as “collection of large quantities of signals intelligence data . . . which is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)”). Collection of data that is not “bulk,” as commonly understood, may nonetheless result in the government’s acquisition of very large volumes of data.

¹⁰ (U) *See* Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No. BR 06–05, 2–3 (FISA Ct. May 24, 2006) (“CDR Order”).

¹¹ (U) 2014 Board Report at 23.

¹² (U) 2014 Board Report at 23–24.

¹³ (U) 2014 Board Report at 29.

“comprehensive” analysis of telephone communications “that cross different providers and telecommunications networks.”¹⁴ Once in NSA’s database, NSA analysts could “contact chain”¹⁵ or otherwise query the database when authorized under a FISA court order.¹⁶ The FISA court order required that one of twenty-two designated NSA officials determine that there was a reasonable articulable suspicion that the query term was associated with one of the terrorist groups specified on the court’s order.¹⁷ Contact chaining enabled NSA analysts to retrieve CDRs relating to a direct phone contact with a target (the “first hop”), CDRs relating to a direct contact with any of the first-hop numbers (the “second hop”), and CDRs relating to a direct contact with any of the second-hop numbers (the “third hop”), for a total of three hops of contact chaining.¹⁸

(U) For example, hypothetically, in the aftermath of a terrorist attack in Manhattan, an NSA analyst may have learned from FBI’s New York field office that the attacker used a particular phone number. Upon learning this phone number, the NSA analyst could seek approval from one of the twenty-two designated NSA officials by showing that there was a reasonable articulable suspicion that the phone number was associated with a specified terrorist group. If the designated official approved, the NSA analyst could use that phone number to query the database of CDRs produced every day by the providers. The result of the query would identify CDRs relating to direct phone contacts with the attacker (the first hop), CDRs relating to the phone contacts with the attacker’s contacts (the second hop), and CDRs relating to the direct contacts with any second-hop numbers (the third hop). “Some have suggested that if NSA’s [bulk collection] program were in place before 9/11, it could have alerted the government that one of the future airplane hijackers was in the United States, and perhaps have led to the prevention of the attacks.”¹⁹

¹⁴ (U) See Declaration of Teresa H. Shea, Signals Intelligence Director, National Security Agency at 59–60, *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13–3994).

¹⁵ ~~(TS//SI//NF)~~ Contact chaining is a type of analysis in which a [REDACTED] of contacts linking communicants and identifying additional phone numbers. [REDACTED] of potential intelligence interest. The contact-chaining [REDACTED] identifies the first hop of contacts made by a seed number [REDACTED] and builds out further contacts made by the first-hop phone numbers [REDACTED]. Under the bulk program, the government used selectors associated with telephones, such as telephone numbers [REDACTED], to conduct contact chaining. [REDACTED] See 2014 Board Report at 26.

¹⁶ (U) See CDR Order at 5–6; see also 2014 Board Report at 26–31.

¹⁷ (U) See CDR Order at 5–6; see also 2014 Board Report at 27.

¹⁸ (U) Additional information regarding the provenance and operation of NSA’s bulk collection program is available in the 2014 Board Report.

¹⁹ (U) See 2014 Board Report at 153–55.

(U) In 2013, unauthorized disclosures of classified documents by Edward Snowden revealed the nature and scope of the CDR program (among other intelligence activities). The President and House Minority Leader asked the Board to review aspects of the CDR program.²⁰ The President also ordered a separate review group to evaluate the program and consider modifications to its operations.²¹

B. (U) The Board's Section 215 Report

(U) The Board issued its report on the CDR program in 2014 (the "2014 Board Report").²² In that Report, the Board concluded that the program was not authorized by Section 215 of the USA Patriot Act and conflicted with another federal statute, the Electronic Communications Privacy Act.²³

(U) The 2014 Board Report made two major recommendations concerning the CDR program: (1) the US government should discontinue the bulk collection program;²⁴ and (2) to the extent the program continued, the executive branch should add certain privacy safeguards.²⁵ The Report contained an additional ten recommendations for enhancing oversight and transparency.²⁶

(U) In light of these recommendations and the report of the President's review group,²⁷ the President ordered NSA to query the CDRs collected under the CDR program only if (1) a FISA court judge first approved the seed number for such queries based on a judicial finding, or (2) in the case of a true emergency.²⁸ Seed numbers were generally phone numbers, but could

²⁰ (U) See Remarks by the President at a White House Press Conference (Aug. 9, 2013), <http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference>; Letter from Democratic Leader Nancy Pelosi to Chairman David Medine (July 11, 2013), <https://www.pclob.gov/library/Letter-Pelosi.pdf>.

²¹ (U) The White House, *Presidential Memorandum—Reviewing Our Global Signals Intelligence Collection and Communications Technologies* (Aug. 12, 2013), <https://obamawhitehouse.archives.gov/the-press-office/2013/08/12/presidential-memorandum-reviewing-our-global-signals-intelligence-collec>.

²² (U) 2014 Board Report.

²³ (U) 2014 Board Report at 8–10 ("That statute prohibits telephone companies from sharing customer records with the government except in response to specific enumerated circumstances, which do not include Section 215 orders.").

²⁴ (U) 2014 Board Report at 168–72. Two of the five Board Members did not believe the program should be discontinued before an adequate alternative was instituted. See 2014 Board Report at 208–18.

²⁵ (U) 2014 Board Report at 168–72.

²⁶ (U) 2014 Board Report at 173–206.

²⁷ (U) The White House, *Liberty and Security in a Changing World* (Dec. 12, 2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

²⁸ (U) The White House, *Remarks by the President on Review of Signals Intelligence* (Jan. 17, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>;

have also been other unique identifiers, such as an International Mobile Subscriber Identity (“IMSI”) or International Mobile Equipment Identity (“IMEI”) number associated with a SIM card or phone, respectively.²⁹ Additionally, the President limited query results to CDRs within two hops of the query target instead of the previous three.³⁰ In other words, although NSA still received the same CDRs from the same providers, NSA analysts could only retrieve the first two hops.³¹

(U) The Board continued its oversight of the CDR program after releasing its report. Initially, the Board concentrated on reviewing the government’s response to its recommendations, which the Board summarized in its 2015 Recommendations Assessment Report.³² That report concluded that the government had not implemented the Board’s recommendation to end the bulk collection of CDRs.

C. (U) The USA Freedom Act

(U) After hearings and debate, Congress enacted the USA Freedom Act on June 2, 2015. The President signed it into law that day. The Act amended FISA’s provisions governing the collection of business records, imposing new requirements on the government’s collection of and access to CDRs.³³

see also The White House, *Fact Sheet: The Administration’s Proposal for Ending the Section 215 Bulk Telephony Metadata Program* (Mar. 27, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m>.

²⁹ (U) NSA briefing to the Board (Jan. 23, 2019). An IMSI is generally a fifteen digit number used to uniquely identify users on a cellular network. The number is either associated directly with a phone or, more commonly, is put on a small chip, known as a subscriber identification module (“SIM”) card, which is inserted into a cellular phone or similar device. An IMEI is a unique number given to mobile phones; it is typically found behind the battery.

³⁰ (U) The White House, *Remarks by the President on Review of Signals Intelligence* (Jan. 17, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>; *see also* The White House, *Fact Sheet: The Administration’s Proposal for Ending the Section 215 Bulk Telephony Metadata Program* (Mar. 27, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m>.

³¹ (U) The White House, *Remarks by the President on Review of Signals Intelligence* (Jan. 17, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>; *see also* The White House, *Fact Sheet: The Administration’s Proposal for Ending the Section 215 Bulk Telephony Metadata Program* (Mar. 27, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m>.

³² (U) Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report* (Jan. 29, 2015), https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf.

³³ (U) Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114–23, 129 Stat. 268 (2015). Although officially written as the “USA FREEDOM Act,” we have used “USA Freedom Act” for readability. As defined in the USA Freedom Act, “[t]he term ‘call detail

(U) The USA Freedom Act amended Section 215 to expressly bar the government from using FISA’s business records collection authority for bulk collection of CDRs—that is, collection not based on a “specific selection term” (such as a phone number) or individualized suspicion.³⁴ NSA no longer obtains CDRs in bulk from providers.

(U) At the same time, the USA Freedom Act also allowed the government to continue to obtain CDRs on a broader basis than other business records. Specifically, it authorized the government to compel providers to produce both “a first set of call detail records using the specific selection term” and “a second set of call detail records using session-identifying information . . . identified by” the first request.³⁵ Put simply, the USA Freedom Act enabled the government to collect CDRs within two hops of a specific selection term on an ongoing basis.

(U) By statute, a specific selection term must be a term that “specifically identifies an individual, account, or personal device.”³⁶ In practice, NSA does not use names or “accounts” as specific selection terms, and instead uses terms associated with particular electronic devices, such as phone, IMSI, and IMEI numbers.³⁷

(U) To obtain a court order compelling providers to produce CDRs, the USA Freedom Act requires the government to identify a “specific selection term” and demonstrate reasonable articulable suspicion to the FISA court that the term is associated with a foreign power or agent of a foreign power that is engaged in international terrorism or activities in preparation for

record’ (A) means session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call, and (B) does not include (i) the contents . . . of any communication; (ii) the name, address, or financial information of a subscriber or customer; or (iii) cell site location or global positioning system information.” 50 U.S.C. § 1861(k)(3).

³⁴ (U) *See* 50 U.S.C. § 1861(c)(3) (“No order issued under this subsection may authorize the collection of tangible things without the use of a specific selection term that meets the requirements in subsection (b)(2).”); *see also* discussion of “bulk collection” in footnote 9 above.

³⁵ (U) 50 U.S.C. § 1861(c)(2)(F) (“An order under this subsection . . . shall . . . (iii) provide that the Government may require the prompt production of a first set of call detail records using the specific selection term . . . [and] (iv) provide that the Government may require the prompt production of a second set of call detail records using session-identifying information or a telephone calling card number identified by the specific selection term used to produce call detail records under clause (iii)[.]”).

³⁶ (U) 50 U.S.C. § 1861(k)(4)(B) (“For purposes of an application submitted under subsection (b)(2)(C), the term ‘specific selection term’ means a term that specifically identified an individual, account, or personal device.”).

³⁷ (U) 2014 Board Report at 26; NSA Civil Liberties and Privacy Office, *Transparency Report: The USA FREEDOM Act Business Records FISA Implementation* 4 (Jan. 15, 2016); *see also* NSA briefing to the Board (Jan. 23, 2019); Part III(A).

international terrorism.³⁸ The statute includes an emergency exception, which allows the Attorney General to temporarily authorize collection.³⁹

(U) If the FISA court approves a specific selection term, NSA may use that specific selection term to obtain two hops of CDRs.⁴⁰ The technical architecture that NSA created to collect those CDRs from providers is discussed in greater detail below.

(U) The USA Freedom Act also implemented a number of other surveillance reforms and oversight mechanisms. For example, the Act created a panel of cleared amici (technical and legal experts) from whom the FISA court can solicit additional perspectives on matters of privacy and civil liberties, communications technology, and other technical or legal matters presented by its cases.⁴¹ The Act also required that the Director of National Intelligence, in consultation with the Attorney General, conduct a declassification review of each decision by the FISA court that includes a novel and significant interpretation and make publicly available to the greatest extent practicable each decision.⁴² Further, the Act required the Attorney General and Director of National Intelligence to report to Congress the total number of applications approved by the FISA court under the CDR provision each year.⁴³

³⁸ (U) 50 U.S.C. § 1861(b)(2)(C) (“Each application . . . shall include . . . in the case of an application for the production on an ongoing basis of call detail records . . . a statement of facts showing that there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term . . . are relevant to [an investigation to protect against international terrorism]; and there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor[.]”).

³⁹ (U) *See* 50 U.S.C. § 1861(i)(1)(A) (“[T]he Attorney General may require the emergency production of tangible things if the Attorney General reasonably determines that an emergency situation requires the production of tangible things before an order authorizing such production can with due diligence be obtained[.]”). The definition of Attorney General in FISA includes certain senior level officials in the Department of Justice. *See* 50 U.S.C. § 1801(g).

⁴⁰ (U) 50 U.S.C. § 1861(c)(2)(F)(i) (“An order under this subsection . . . shall authorize the production on a daily basis of call detail records for a period not to exceed 180 days[.]”).

⁴¹ (U) 50 U.S.C. § 1803(i)(1) (“The presiding judges of the courts established under subsections (a) and (b) shall, not later than 180 days after June 2, 2015 jointly designate not fewer than 5 individuals to be eligible to serve as amicus curiae, who shall serve pursuant to rules the presiding judges may establish.”).

⁴² (U) 50 U.S.C. § 1872(a) (“[T]he Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review . . . that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term ‘specific selection term’, and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.”).

⁴³ (U) *See* 50 U.S.C. § 1861(b)(4) (“In April of each year, the Attorney General shall submit to the House and Senate Committees on the Judiciary and the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence a report setting forth with respect to the preceding calendar year . . . the total number of

D. (U) Effects of the Impending Sunset

(U) Unless reauthorized, several provisions extended or amended by the USA Freedom Act will expire, or “sunset,” on March 15, 2020.

(U) Most notably, NSA’s explicit statutory authority to obtain two-hop CDRs associated with an approved specific selection term will expire. In addition, the explicit prohibition on using the business records provision to collect records that are not based on a specific selection term will expire. The resulting statute would not explicitly authorize the government to collect business records beyond one degree of separation from the target, but it would not explicitly bar it from doing so either.⁴⁴

(U) A sunset would also significantly curtail the broader, “traditional” FISA business records authority, which would revert to its pre-9/11 text. Before 9/11, the statute was limited to “records” from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. Consequently, the government would no longer be authorized to seek broader business records productions from other, non-enumerated entities.

(U) The evidentiary standard required to compel production of these records would also become more stringent. Specifically, the standard would shift from a showing that the records sought are “relevant to an authorized investigation”—the current standard—to requiring “specific and articulable facts giving reason to believe that the person to whom the record pertains is a foreign power or agent of a foreign power.”⁴⁵

(U) Finally, the USA Freedom Act extended the sunsets of two other FISA provisions: the lone wolf and roving wiretap authorities.⁴⁶ Without congressional action, these authorities will also expire on March 15, 2020.⁴⁷

applications described in section 1861(b)(2)(C) of this title made for orders approving requests for the production of call detail records.”).

⁴⁴ (U) 50 U.S.C. § 1862 (2000).

⁴⁵ (U) 50 U.S.C. § 1861(b)(2)(A), (c)(1); 50 U.S.C. § 1862(b)(2)(B) (2000).

⁴⁶ (U) Under the lone wolf authority, the government can obtain a FISA court order for electronic surveillance of a non-US person upon a showing of probable cause that such person is engaged in international terrorism or activities in preparation for international terrorism without having to show that the non-US person is doing so on behalf of a foreign power. The government has never used this broadened definition operationally. The roving wiretap authority modified FISA to permit the government to seek a FISA court order to conduct electronic surveillance without having to specify the entities from whom technical assistance will be required. This authority enables continued surveillance should an individual switch from one provider to another.

⁴⁷ (U) Some provisions of the USA Freedom Act are not subject to sunset. These provisions include the new oversight and transparency mechanisms described above.

E. (U) The Board's Continuing Oversight of CDR Collection

(U) The Board's oversight of the government's CDR collection continued after passage of the USA Freedom Act. In 2016, the Board reviewed the government's response to the 2014 Board Report recommendations and issued a second recommendations assessment report.⁴⁸ In that report, the Board found that the government had addressed most of its recommendations.⁴⁹

(U) Since then, NSA has provided the Board with regular written and oral notifications about significant developments in the operation of the CDR program. The Board received multiple in-person briefings from relevant government agencies and received responses to written and oral questions, as well as document requests. Additionally, the Board hosted a public forum in May 2019 to hear from a range of experts on the USA Freedom Act.⁵⁰ The discussion focused on the history and implementation of the Act, present challenges, and the path ahead. The panelists included academics, former government officials, and representatives from non-governmental organizations. The Board appreciates the time and observations contributed by the participants.

⁴⁸ (U) Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report* (Feb. 5, 2016), https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf.

⁴⁹ (U) Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report*, 1 (Feb. 5, 2016), https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf.

⁵⁰ (U) Public Forum of the Privacy and Civil Liberties Oversight Board To Examine the USA Freedom Act, Telephone Records Program (May 31, 2019), <http://www.pclob.gov>.

II. (U) NSA's Collection of CDRs under the USA Freedom Act

(U) NSA worked with telephony providers to create a technical architecture to collect and use CDRs under the USA Freedom Act.⁵¹ This included technical processes and infrastructure to use approved specific selection terms to obtain, analyze, and control access to the CDRs. NSA released an unclassified description of this architecture in January 2016.⁵² The architecture remained essentially constant throughout the life of the program until NSA began dismantling it in the summer of 2019, after the program was suspended.⁵³

(U) Some of these technical processes were developed to ensure compliance with the minimization procedures approved by the FISA court in 2015, when the program began. The procedures governed NSA's handling, retention, and dissemination of the CDRs obtained from providers under the USA Freedom Act. For example, the minimization procedures required an initial review of records to confirm that the CDRs were generally responsive to the court's order, mandated specific storage standards, and imposed rules for sharing US person information.⁵⁴

A. (U) Program Architecture Used to Collect CDRs under the USA Freedom Act

(U) Under the USA Freedom Act, CDRs could be collected and used in emergency situations (a terrorist attack or an imminent threat) or in day-to-day counterterrorism investigations. In the immediate aftermath of a terrorist attack, collection of USA Freedom Act CDRs may have occurred as an emergency authorization, which had to be approved by the Attorney General.⁵⁵ To seek an emergency authorization, NSA personnel would collaborate with FBI counterparts to prepare the proposed authorization for the Attorney General's review.⁵⁶ Only after the Attorney General approved the request could the government direct the providers

⁵¹ (U) *See* 50 U.S.C. § 1861(j) ("The Government shall compensate a person for reasonable expenses incurred for producing tangible things or providing information, facilities, or assistance in accordance with an order issued with respect to an application . . . or an emergency production . . . or otherwise providing technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.").

⁵² (U) NSA Civil Liberties and Privacy Office, *Transparency Report: The USA FREEDOM Act Business Records FISA Implementation* (Jan. 15, 2016) ("NSA USA Freedom Act Transparency Report").

⁵³ (U) NSA Notice to the Board (Aug. 30, 2019).

⁵⁴ (U) NSA Minimization Procedures for CDRs.

⁵⁵ (U) 50 U.S.C. § 1861(i); *see also* NSA briefing to the Board (May 23, 2019).

⁵⁶ (U) 50 U.S.C. § 1861(i); *see also* NSA briefing to the Board (May 23, 2019).

to produce CDRs associated with the approved specific selection terms. Even in an emergency, this effort could have taken many hours.⁵⁷ Under the statute, the government must seek FISA court approval for any emergency authorization approved by the Attorney General within seven days.⁵⁸ Therefore, almost immediately after the Attorney General's approval, the government would begin preparing its filings to the FISA court to ratify the emergency authorization with a FISA court order.⁵⁹

(U) If CDRs were sought in a non-emergency scenario, NSA and FBI would prepare the specific selection terms and supporting evidence as described above, but typically over a longer time period. Attorneys from the Department of Justice would work with NSA and FBI personnel to draft FISA court filings that described the specific selection terms and explained the reasonable articulable suspicion that the terms are associated with a foreign power engaged in international terrorism.⁶⁰ This drafting process often took days or weeks,⁶¹ and the FISA court could have reviewed the application for several days before denying or approving it.⁶² In parallel with that legal process, NSA analysts could have continued to conduct contact-chaining analysis using data available under NSA's other legal authorities.

1. (U) Obtaining CDRs

~~(TS//NF)~~ NSA acquired landline and wireless CDRs under the USA Freedom Act.⁶³ NSA did not use the program to obtain CDRs associated with [REDACTED]⁶⁴ Nor did the CDR program collect metadata associated with [REDACTED]⁶⁵.

⁵⁷ (U) NSA briefing to the Board (May 23, 2019).

⁵⁸ (U) 50 U.S.C. § 1861(i)(3); *see also* NSA briefing to the Board (May 23, 2019).

⁵⁹ (U) 50 U.S.C. § 1861(i)(3); *see also* NSA briefing to the Board (May 23, 2019).

⁶⁰ (U) 50 U.S.C. § 1861(b)(2)(B); *see also* NSA briefing to the Board (May 23, 2019).

⁶¹ (U) NSA briefing to the Board (May 23, 2019); FBI briefing to the Board (June 19, 2019).

⁶² (U) NSA briefing to the Board (May 23, 2019).

⁶³ (U) NSA briefing to the Board (Jan. 23, 2019).

⁶⁴ ~~(S//NF)~~ NSA briefing to the Board (Jan. 23, 2019). [REDACTED]

[REDACTED] *See* FBI and DOJ briefing to the Board (Mar. 12, 2019). [REDACTED]

⁶⁵ [REDACTED]

~~(S//NF)~~ Once the FISA court approved a specific selection term under the USA Freedom Act, NSA did not immediately send the specific selection term to providers and request corresponding CDRs. Instead, NSA first queried for contacts with the specific selection term in the [REDACTED] an internal repository containing metadata previously collected by NSA.⁶⁶ These queries were governed by NSA's policies and procedures, including the NSA's Attorney General-approved Supplemental Procedures Governing Communications Metadata Analysis ("SPCMA").⁶⁷ SPCMA allows identifiers associated with both non-US persons and US persons to be used to query phone metadata and electronic communications metadata that NSA already obtained through other lawful collection methods. By doing so, NSA was able to find first-hop contacts in telephone metadata already in its own holdings, such as intercepted telephone communications metadata collected pursuant to FISA or Executive Order 12333.⁶⁸

(U//~~FOUO~~) After it queried the internal metadata repository, NSA included the specific selection terms and direct contacts found through the searches in its holdings when it sought further records from the providers.⁶⁹ The system for sending specific selection terms and direct contacts to the providers and for receiving CDRs in return was referred to as [REDACTED] which we refer to here as "System 1."⁷⁰ System 1 marked the specific selection term and direct contacts for internal record-keeping.⁷¹

(U) The providers received the specific selection terms and direct contacts and searched for any responsive CDRs showing contacts between these numbers and others. Those records were produced to NSA in a standardized format that had about 50 fields per record.⁷² The fields included information such as the call participants' phone numbers, unique device identifiers of participants (if applicable), and the date, time, and duration of the call.⁷³ Each record also contained information about the legal authority under which it was obtained, including a code indicating the specific FISA court order.⁷⁴ Under the USA Freedom Act, CDRs could not include the contents of any communication, the name, address, or financial information

⁶⁶ (U) NSA briefing to the Board (Mar. 26, 2019).

⁶⁷ See Department of Defense, *Supplemental Procedures Governing Communications Metadata Analysis*, <https://www.dni.gov/files/documents/0909DoD%20Supplemental%20Procedures%0220080314.pdf>.

⁶⁸ (U) See NSA USA Freedom Act Transparency Report at 5–6; see also NSA briefing to the Board (Mar. 26, 2019).

⁶⁹ (U) See NSA USA Freedom Act Transparency Report at 7; NSA briefing to the Board (Jan. 23, 2019).

⁷⁰ (U) NSA briefing to the Board (Jan. 23, 2019).

⁷¹ (U) NSA briefing to the Board (Mar. 26, 2019).

⁷² (U) NSA briefing to the Board (Mar. 26, 2019). The full list of fields is attached as Appendix B.

⁷³ (U) See NSA USA Freedom Act Transparency Report at 4; NSA briefing to the Board (Mar. 26, 2019).

⁷⁴ (U) NSA briefing to the Board (Mar. 26, 2019).

of a subscriber or customer, or cell-site location or global positioning system information.⁷⁵ NSA represents that, since the start of the program in November 2015, it never received any prohibited categories of information from providers under the program.⁷⁶

(U) NSA then used System 1 to check the validity of CDRs produced by the providers. Among other things, the system checked the code indicating the FISA court order to ensure the collection occurred pursuant to a valid order.⁷⁷ This step did not allow NSA to verify that the CDR accurately described a phone call that had in fact occurred, or that the data did not contain errors.⁷⁸ Rather, NSA used this validation effort to ensure that the CDR fields were plausible—that is, it sought to detect when, on its face, a CDR could not have been a valid response to the specific selection term. For example, if a field should have a date, NSA systems confirmed there was a valid and appropriate date in that field. In other fields, NSA systems checked for a particular number of digits or a particular formatting, with the goal of ensuring the CDRs were properly formatted and not facially incorrect.⁷⁹ If one of these validation checks failed—for example, a field that should have a date did not have one—the records were held for review by technical personnel to identify the nature of the anomaly.⁸⁰ This prevented NSA analysts from accessing certain types of potentially unauthorized or incorrect CDRs.

(U) If the CDRs from the provider passed the validation steps, they were passed by System 1 into other repositories, including the internal metadata repository, where they could be accessed by NSA analysts.⁸¹ NSA regularly checked its internal repository to obtain further CDRs. Related CDRs associated with a specific selection term (first-hop CDRs) were automatically distributed to the other providers to obtain second-hop records.⁸² Similarly, first-

⁷⁵ (U) 50 U.S.C. § 1861(k)(3)(B) (“The term ‘call detail record’ . . . does not include the contents . . . of any communication; the name, address, or financial information of a subscriber or customer; or cell site location or global positioning system information.”).

⁷⁶ (U) NSA briefing to the Board (May 23, 2019).

⁷⁷ (U) *See* NSA USA Freedom Act Transparency Report at 14 (“NSA’s minimization procedures . . . require the Agency to inspect CDRs received from a provider through manual and/or automated means to confirm that the CDRs are responsive to the FISC’s production order.”); NSA briefing to the Board (Mar. 26, 2019).

⁷⁸ (U) The system did not enable NSA to verify the accuracy of the records maintained by the providers themselves—a reason it took years to discover the data-integrity issues discussed in Part II(B) of this report. *See* NSA USA Freedom Act Transparency Report at 14 (“NSA plays no role in ensuring that the provider-generated CDRs accurately reflect the calling events that occurred over the provider’s infrastructure[.]”); NSA briefing to the Board (May 23, 2019).

⁷⁹ (U) *See* NSA USA Freedom Act Transparency Report at 5; NSA briefing to the Board (Mar. 26, 2019).

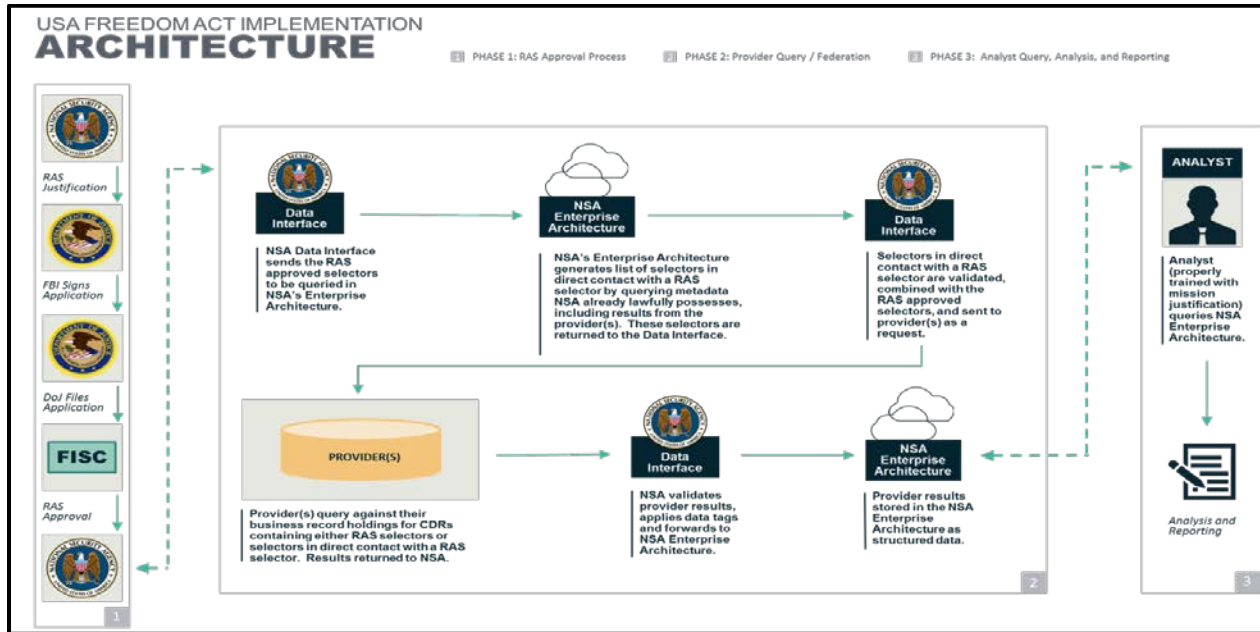
⁸⁰ (U) *See* NSA USA Freedom Act Transparency Report at 5; NSA briefing to the Board (Mar. 26, 2019).

⁸¹ (U) *See* NSA USA Freedom Act Transparency Report at 5–8; NSA briefing to the Board (Jan. 23, 2019).

⁸² (U) *See* NSA USA Freedom Act Transparency Report at 5–8; NSA briefing to the Board (Jan. 23, 2019).

hop numbers derived from NSA's metadata collection were sent to providers to enable them to return any second-hop results.⁸³ The providers sent any responsive CDRs, including historical records, back to NSA on an ongoing, automated basis for the life of the order.⁸⁴ In other words, NSA was able to obtain a second hop of CDRs by sending providers the first-hop contacts it found in its internal repository. Thus, at any given point, the providers were only returning a single hop of data.

(U)



(U)

(U) This resulted in an iterative process whereby new CDRs from any provider or new contacts from NSA's own metadata collection could result in additional responsive CDRs being produced to NSA automatically for counterterrorism analysis. For example, if two weeks into an order one provider produced to NSA CDRs showing that a specific selection term contacted another number, NSA would automatically transmit that new number to the providers as a first-hop contact. With the new contact added, other providers might identify new responsive second-hop CDRs that they would then produce to NSA. Likewise, if NSA found contacts between the specific selection term and another individual via its Executive Order 12333 collection, the other individual's number could be sent to each of the providers as a first-hop contact.⁸⁵ Finally, it

⁸³ (U) See NSA USA Freedom Act Transparency Report at 5–8; NSA briefing to the Board (Jan. 23, 2019).

⁸⁴ (U) See NSA USA Freedom Act Transparency Report at 5–8; NSA briefing to the Board (Jan. 23, 2019).

⁸⁵ (U) See NSA USA Freedom Act Transparency Report at 5–8.

was also possible for second-hop contacts to become first-hop contacts if they directly contacted a FISA court-approved⁸⁶ specific selection term. Because that individual would now be a first-hop contact, NSA could seek CDRs for its contacts from all providers.

2. (U) Analyzing CDRs

(U) When NSA received valid CDRs, they were processed and placed into its repository.⁸⁷ NSA repositories are subject to access controls and cannot be directly reviewed by NSA analysts. Rather, NSA analysts use software interfaces that validate what data they are authorized to access, and return information from a repository in response to the analysts' queries.⁸⁸

(U/~~FOUO~~) To view metadata records, NSA analysts use general metadata viewing tools, including [REDACTED], which we refer to here as Tool 1. Tool 1 enables NSA analysts to query one or more datasets to which they have access, including multiple types of NSA metadata records.⁸⁹ Primarily using Tool 1, NSA analysts can input different terms which they reasonably expect to return foreign intelligence information and query those terms against several different pools of metadata.⁹⁰

(U) Prior to the passage of the USA Freedom Act, CDRs were maintained in such a way that NSA analysts could not query CDRs collected under the former CDR program alongside other metadata records collected by NSA in Tool 1.⁹¹ NSA later determined that it could use a single tool, Tool 1, it had earlier produced to search all metadata records the analyst was authorized to review, though this was not caused by the passage of the USA Freedom Act.⁹² Tool 1 allowed an analyst to search against all available metadata and to use all query terms at once, saving time and providing insights that might otherwise be difficult to uncover.⁹³

(U) Using this tool to query different types of metadata, while operationally efficient, had an anomalous side-effect for NSA's efforts to count metadata query terms. A simple example illustrates the anomaly: A query in Tool 1 about an email address and a US phone number could automatically ping against CDRs obtained under the USA Freedom Act. This would count as

⁸⁶ (U) Or Attorney General-approved under the emergency provision. *See* 50 U.S.C. § 1861(i).

⁸⁷ (U) *See* NSA USA Freedom Act Transparency Report at 5–8; NSA briefing to the Board (Mar. 26, 2019).

⁸⁸ (U) NSA briefing to the Board (May 23, 2019).

⁸⁹ (U) NSA briefing to the Board (May 23, 2019).

⁹⁰ (U) NSA briefing to the Board (May 23, 2019).

⁹¹ (U) NSA briefing to the Board (May 23, 2019).

⁹² (U) NSA briefing to the Board (May 23, 2019).

⁹³ (U) NSA briefing to the Board (May 23, 2019).

two query terms of USA Freedom Act CDRs even though using an email address as a query term in Tool 1 would never return USA Freedom Act CDRs.⁹⁴ (Those CDRs did not include email addresses or other unique online identifiers.⁹⁵) As a result, the reported number of USA Freedom Act CDR query terms⁹⁶ included terms that, by their nature, could never have returned those CDRs.

(U) Using Tool 1 for its operational benefits produced ancillary benefits for oversight and compliance. The minimization procedures that apply to USA Freedom Act CDRs address the handling, retention, and dissemination of CDRs, but do not regulate querying.⁹⁷ Thus, NSA was not required to track—and did not need to have a particularized foreign intelligence justification for running—US person queries of CDR program data. However, Tool 1 is designed to automatically require analysts to justify and track US person queries and requires a foreign intelligence purpose for each query run in order to comply with NSA’s other procedures. Using Tool 1 effectively imposed these requirements as a matter of practice on the CDR program.⁹⁸

~~(S//NF)~~ When an analyst ran a query that returned CDRs, the analyst would naturally want to know additional information about the individuals involved, even to the point of identifying communicants if possible. However, [REDACTED] with identifying information as they entered its repositories. For example, it did not [REDACTED] to the CDR produced by the provide [REDACTED]

[REDACTED]⁹⁹ For example, an NSA analyst could have Tool 1 indicate whether any CDRs were associated with an NSA target of foreign-intelligence interest.¹⁰⁰ An NSA analyst could also ask Tool 1 to display certain [REDACTED] the contact in the query results, [REDACTED]

101

⁹⁴ (U) NSA briefing to the Board (Mar. 26, 2019).

⁹⁵ (U) NSA briefing to the Board (Mar. 26, 2019).

⁹⁶ (U) Office of the Director of National Intelligence, *Statistical Transparency Report Regarding the Use of National Security Authorities: Calendar Year 2018*, 28 (Apr. 2019) (“2018 Statistical Transparency Report”), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf.

⁹⁷ (U) See NSA Minimization Procedures for CDRs.

⁹⁸ (U) NSA briefing to the Board (Mar. 26, 2019).

⁹⁹ (U) NSA briefing to the Board (May 23, 2019).

¹⁰⁰ (U) NSA briefing to the Board (May 23, 2019).

¹⁰¹ (U) NSA briefing to the Board (May 23, 2019).

3. (U) Access Controls, Logs, and Data Deletion

(U) Access to NSA systems that contained USA Freedom Act information was controlled.¹⁰² NSA systems are built to ensure that only users with a valid mission need and appropriate training are allowed to access stored foreign intelligence information.¹⁰³ For back-end systems not accessible to analysts, including System 1, only particular authorized users can access those systems or files.¹⁰⁴ Thus, a pool of analysts had the training and authority to query CDR program records in Tool 1, and a smaller number of technical personnel were able to view records that arrived in System 1, including those that failed NSA's initial validation check.¹⁰⁵

(U) Subject to certain exceptions, NSA minimization procedures required NSA to eventually destroy records obtained under the USA Freedom Act.¹⁰⁶ The minimization procedures required NSA to promptly destroy records that were determined not to contain foreign intelligence information.¹⁰⁷ No CDRs were destroyed under this provision.¹⁰⁸ Records collected under the program were otherwise scheduled to be destroyed after five years.¹⁰⁹ This was to be accomplished by deleting them from the internal metadata repository and any other pertinent systems. However, some residual information would remain, such as documentation that a provider had produced CDRs.¹¹⁰ Additionally, the minimization procedures allowed NSA to retain CDRs that were the basis of an approved dissemination—that is, intelligence reporting circulated to other agencies.¹¹¹ In practice, NSA deleted all USA Freedom Act CDRs in 2018 and again in 2019; however, CDRs that were used in intelligence reporting were not deleted, though those records were no longer available in the internal metadata repository.¹¹²

B. (U) Compliance and Data-Integrity Challenges

(U) Between early 2016 and mid-2019, the government filed approximately a dozen notices to the FISA court regarding compliance and data-integrity issues experienced while

¹⁰² (U) NSA briefing to the Board (Jan. 23, 2019).

¹⁰³ (U) NSA briefing to the Board (Jan. 23, 2019).

¹⁰⁴ (U) NSA briefing to the Board (Jan. 23, 2019).

¹⁰⁵ (U) NSA briefing to the Board (Mar. 26, 2019).

¹⁰⁶ (U) NSA Minimization Procedures for CDRs.

¹⁰⁷ (U) NSA Minimization Procedures for CDRs at 7.

¹⁰⁸ (U) NSA briefing to the Board (May 23, 2019).

¹⁰⁹ (U) NSA Minimization Procedures for CDRs at 7.

¹¹⁰ (U) NSA briefing to the Board (Jan. 23, 2019).

¹¹¹ (U) NSA Minimization Procedures for CDRs.

¹¹² (U) *See* note 2.

operating the USA Freedom Act CDR program. A classified appendix describes these incidents in more detail.

1. (U) General Compliance Matters

(U) Some of the notices filed with the FISA court, which are described in this section, dealt with compliance incidents which could occur when using other intelligence or equivalent law enforcement collection authorities and were the result of two types of government error and one type of provider error.

a. (U) Omitted Information from FISA Application

(U) In one instance, the same day the FISA court approved the government's application under the USA Freedom Act, FBI informed NSA that it possessed intelligence which called into question facts the government relied on in its application.¹¹³ FBI attributed its failure to share this intelligence with NSA and the Department of Justice to an internal oversight.¹¹⁴ NSA asked the providers to stop producing CDRs for certain specific selection terms affected by the omissions and asked the providers to continue production for the specific selection term that was not affected by the omissions and continued to meet the statutory requirements.

b. (U) Overproduction

~~(S//NF)~~ Three days after a valid FISA court order expired, a provider transmitted [REDACTED] CDRs associated with the expired order to NSA. Upon receiving the files, NSA's automated initial review in System 1 determined that the CDRs should not have been produced and, as a result, ensured that NSA analysts did not gain access to the files. NSA destroyed all CDRs erroneously transmitted by the provider within a few days.

c. (U) Training Compliance Incidents

(U) NSA discovered that a number of NSA personnel were unintentionally granted access to USA Freedom Act CDRs even though the personnel did not have training required by the minimization procedures. NSA confirmed that this issue was caused by human error. Among other corrective steps, NSA revoked access credentials for personnel. In light of this incident, NSA sped up its efforts to shift from manual verification of training toward automated verification. Additionally, NSA analysts improperly shared CDR information via email with NSA analysts who had not had the formal USA Freedom Act training. In this instance, NSA

¹¹³ (U) Government Notice to the FISA court ¶ 2 (May 24, 2016).

¹¹⁴ (U) Prior to the filing of the application, a foreign partner provided additional information about the target to FBI. Due to an FBI analyst's annual leave, that additional information was not included in the application. FBI briefing to Board staff (Oct. 22, 2019); Government Notice to the FISA court (May 24, 2016).

recalled the improperly shared CDR information. No additional improper access occurred during the duration of the program.

2. (U) Data-Integrity Issues

(U) Beginning in 2017 and continuing until the program's suspension in 2019, NSA sought to diagnose and overcome complex data-integrity issues in the CDRs produced by phone companies, which implicated a large number of records.¹¹⁵ The government's notices to the FISA court described these issues. This section summarizes NSA's repeated discovery of anomalies in the data it received and the agency's response to these incidents.

a. (U) Production of Inaccurate First-Hop Numbers

~~(TS//SI//NF)~~ In the first data-integrity incident, a provider produced inaccurate first-hop numbers to NSA in a subset of CDRs. The provider's system had been incorrectly populating terminating numbers (the field for a number used by the party receiving a call) with [REDACTED]

While System 1 was designed to detect data which may not be authorized for collection, these non-responsive [REDACTED] similarly to data regularly accepted by System 1. Accordingly, the system did not reject the data and instead requested second-hop records using the erroneous first-hop response. As a consequence, NSA requested records numbers "one hop" away from the [REDACTED].

~~(TS//SI//NF)~~ While investigating this incident, the provider identified a separate incident: [REDACTED] records incorrectly produced to NSA as a result of a [REDACTED]. This error was separate from the errors related to the [REDACTED].

~~(TS//SI//NF)~~ The provider implemented a technical solution to prevent incorrect CDRs from being delivered to NSA. NSA identified and purged CDRs that contained these [REDACTED] terminating numbers. NSA did not identify any incorrect CDRs that were used in an application to the FISA court or as the source of reporting.

b. ~~(TS//SI//NF)~~ Production of Inaccurate Data Associated with [REDACTED]

~~(TS//SI//NF)~~ In another data-integrity incident, a provider produced to NSA almost [REDACTED] CDRs with inaccurate data. The inaccurate data was populated by the provider's CDR production system, which assembles the data into CDRs, [REDACTED]. Specifically, when [REDACTED]. These inaccurate CDRs were created by the provider's CDR production system over a two year period.

¹¹⁵ (U) This large number of records reflected a fraction of one percent of the overall collection.

(U) The same day it identified the problem, NSA stopped issuing new requests to the provider for data and also stopped processing data received from the provider into its repositories. This ensured analysts stopped receiving access to new inaccurate CDRs. NSA informed its analysts of the inaccurate information produced by the provider and cautioned them not to rely on CDRs from the affected time period. The provider ultimately implemented a technical solution to its system to prevent delivery of inaccurate records to NSA.

~~(S//NF)~~ Subsequent internal NSA investigations discovered that prior to the discovery of the data-integrity issue, some inaccurate CDRs were used to support four applications to the FISA court seeking USA Freedom Act authorization [REDACTED]. On April 11, 2018, the government filed a notice informing the FISA court of the inaccurate information produced by this provider. The government also notified the FISA court of the four applications that relied on the inaccurate information. NSA deleted CDRs acquired as a result of these four applications and recalled one disseminated intelligence report generated based on the inaccurate CDRs.

c. (U) Expanding Accuracy Concerns Lead NSA to Delete CDRs

~~(TS//SI//NF)~~ In connection with its investigation into the provider's production of inaccurate data associated with [REDACTED], NSA searched for similar anomalous data from the other providers and found a number of questionable CDRs. In one instance, NSA brought the possibility of inaccurate CDRs to the attention of the provider. That provider confirmed that it also produced CDRs with inaccurate data in [REDACTED] situations. In addition, the provider had also reported to NSA a separate tranche of inaccurate CDRs. Those CDRs included fields which had been overwritten with unrelated data.

(U) By May 2018, NSA realized that the providers could not identify for NSA all the affected records, and NSA had no way to independently determine which records contained inaccurate information. Thus, NSA did not have a viable way to remove the affected records and retain unaffected records. In response, NSA initiated the deletion of all data produced under the USA Freedom Act by providers.¹¹⁶ NSA also successfully revalidated all reports produced by NSA by that time and confirmed they did not rely upon inaccurate CDRs produced in error by the providers. NSA issued a public statement regarding its deletion of USA Freedom Act CDRs.¹¹⁷

¹¹⁶ (U) In September 2018, NSA's Office of the Inspector General identified a small number of USA Freedom Act "data objects" derived from CDRs that should have been deleted but were not, based upon NSA's mistaken assumption regarding the technical configurations for a single SIGINT repository. By October 15, 2018, NSA had also deleted this data. See NSA Office of the Inspector General, *Semi-Annual Report to Congress: 1 October 2018 to 31 March 2019*, 13 (Jan. 2019), <https://oig.nsa.gov>.

¹¹⁷ (U) Government Notice to the FISA court ¶ 7 (June 4, 2018); see also NSA Press Release, *NSA Reports Data Deletion*, PA-010-18 (June 28, 2018).

d. (U) Additional Compliance Issues and Concerns

~~(S//NF)~~ Later in 2018, NSA noticed a larger than expected number of data values in specific fields of CDRs from one provider. The provider discovered that it had produced more [REDACTED] CDRs with incorrect data associated with authorized specific selection terms. Working with this provider, NSA was unable to rectify the inaccurate data problem.

~~(TS//SI//NF)~~ Further discussion with this provider, and with the other providers, led NSA to gain a better appreciation for how all providers maintain their business records in [REDACTED]. The government maintains that CDRs created by all providers in [REDACTED] are valid session identifying information under the statute because [REDACTED] with the specific selection term and are included in CDRs showing a contact and/or connection with the Court-authorized specific selection term. The government informed the FISA court of this position. The FISA court did not explicitly address this issue in any orders or hearings.

e. (U) Suspension of the Program

~~(S//NF)~~ NSA allowed its last FISA court order issued under the USA Freedom Act to expire in early 2019.¹¹⁸ Since then, NSA has not requested any CDRs from providers. On [REDACTED] [REDACTED] NSA informed the Board that it would begin dismantling the System 1 architecture and would reallocate any remaining funds to other intelligence programs.¹¹⁹ NSA's decision to end its collection of CDRs under the USA Freedom Act, delete previously acquired records, and decommission the technical architecture created to effectuate it, was "made after balancing the program's relative intelligence value, associated costs, and compliance and data-integrity concerns caused by the unique complexities of using these provider-generated business records for intelligence purposes."¹²⁰ NSA subsequently deleted data collected under the USA Freedom Act.¹²¹

¹¹⁸ (U) NSA Notice to the Board (Apr. 17, 2019).

¹¹⁹ (U) NSA oral notice to Board Executive Director, Lynn Parker Dupree.

¹²⁰ (U) Letter from Director of National Intelligence Dan Coats to Senators Richard Burr, Lindsey Graham, Mark Warner, and Dianne Feinstein (Aug. 14, 2019).

¹²¹ (U) NSA Notice to the Board (Aug. 5, 2019).

III. (U) Operational Use of the USA Freedom Act CDR Program

(U) This section describes how an NSA analyst would use the CDR program to assist his or her counterterrorism mission; how the CDR program provided analytic material for intelligence reporting since 2015; and how FBI used NSA's intelligence reporting in its counterterrorism and investigative efforts.

A. (U) How NSA Analysts Used the USA Freedom Act CDR Program

(U) As part of its signals intelligence mission, NSA collects foreign intelligence from communications and information systems to support intelligence needs across the government.¹²² To answer terrorism-related requests, NSA maintains an office of counterterrorism within its operations directorate.¹²³ That office brings all lawful authorities and intelligence relationships to bear in its collection and analysis of signals intelligence, providing valuable insight into the terrorist threats to the country.¹²⁴

(U) When a new terrorism threat is discovered or a terrorist attack occurs, NSA's office of counterterrorism uses all its legal authorities to collect and analyze intelligence.¹²⁵ Its analysis informs policymakers and law enforcement about the threat and aids in their decision-making processes.¹²⁶ Time is of the essence in the immediate aftermath of an attack or when an imminent threat is discovered, so NSA analysts routinely leverage intelligence relationships and utilize a broad array of authorities to obtain and access the highest quality information they can, as quickly as they can.¹²⁷

~~(S//NF)~~ For example, hypothetically, if a terrorist attack occurred in New York City, an NSA analyst would seek information from an FBI analyst liaison [REDACTED]. The FBI analyst would attempt to ensure that any information relating to the attack in FBI's possession that could legally be shared with NSA was quickly relayed to NSA. Likewise, NSA would pass any pertinent intelligence to FBI, subject to applicable legal

¹²² (U) NSA briefing to the Board (May 23, 2019).

¹²³ (U) NSA briefing to the Board (May 23, 2019).

¹²⁴ (U) NSA briefing to the Board (May 23, 2019).

¹²⁵ (U) NSA briefing to the Board (May 23, 2019).

¹²⁶ (U) NSA briefing to the Board (May 23, 2019).

¹²⁷ (U) NSA briefing to the Board (May 23, 2019).

restrictions. On the other hand, if a terrorist attack were to occur at a US embassy abroad, an NSA analyst would seek information held by NSA's foreign partners.

(U) When reaching out to its intelligence partners, NSA would be particularly interested in any specific selection terms related to the attack or attackers.¹²⁸ Without such leads, including specific selection terms shared by partners or discovered by NSA, it is harder for NSA analysts to query its intelligence repositories, conduct metadata analysis, and employ other analytic techniques.¹²⁹

(U) Once NSA obtains information about the attack and attacker, an analyst would search NSA's intelligence repositories to find information previously collected under NSA's various legal authorities, such as Executive Order 12333 or FISA.¹³⁰ The results of these queries could, for example, help the analyst conduct contact chaining to better understand the attacker's contacts and communications.

(U) The NSA analyst might also work with FBI and the Department of Justice to seek authority to collect CDRs under the USA Freedom Act.¹³¹ If approved, the analyst could use the resulting CDRs to reveal connections between the attacker and other individuals in the United States or abroad.¹³² The analyst would write a report describing any foreign intelligence findings (or, in some cases, simply listing phone numbers or other identifiers associated with the attacker). That information could then be disseminated, pursuant to the minimization procedures, to other government agencies involved in counterterrorism, including FBI.

B. (U) USA Freedom Act CDRs in Intelligence Reporting

(U) The number of orders the government sought under the CDR program has declined sharply since its inception. From 2016 to 2018, the government received 94 FISA court orders under the USA Freedom Act CDR provision.¹³³ In 2018, the government received 14 FISA court orders, a steep drop from the two prior years.¹³⁴ Despite the relatively low number of orders, NSA collected, in absolute terms, a large number of CDRs. In total, NSA estimates that

¹²⁸ (U) NSA briefing to the Board (May 23, 2019).

¹²⁹ (U) NSA briefing to the Board (May 23, 2019).

¹³⁰ (U) NSA briefing to the Board (May 23, 2019).

¹³¹ (U) NSA briefing to the Board (May 23, 2019).

¹³² (U) NSA briefing to the Board (May 23, 2019).

¹³³ (U) 2018 Statistical Transparency Report at 28. Those orders related to 93 unique targets.

¹³⁴ (U) 2018 Statistical Transparency Report at 28.

it received more than 151 million CDRs from providers in 2016, 534 million CDRs in 2017, and 434 million CDRs in 2018.¹³⁵

(U) NSA used these CDRs as part of its contact-chaining analysis. NSA's goal in contact chaining was to map an attacker's (or potential attacker's) network or find connections between the attacker and other individuals known to NSA.¹³⁶ To conduct contact chaining, an NSA analyst would use Tool 1 to query the internal metadata repository. NSA estimated that NSA analysts used 22,360 such query terms associated with US persons to conduct such queries in 2016, 31,196 in 2017, and 164,682 in 2018.¹³⁷ (Note, however, that some of these query terms were non-telephony identifiers that could not have returned CDRs.) NSA used the results of these queries, combined with information from other sources, in intelligence reports. These reports were disseminated to other US government agencies, including FBI, to assist their counterterrorism efforts.

(U) It is the Board's impression that, when combatting terrorism, NSA felt it had to use all available authorities, including the CDR program. This was done in case the data revealed an intelligence lead or a terrorist plot that otherwise would have been unknown. However, NSA told the Board that traditional telephony metadata, like that obtained through the CDR program, was unlikely to show a suspected terrorist's complete social network because it did not account for other modes of communication.¹³⁸ Further complicating matters, NSA was aware of data-integrity issues with the CDRs, which made them hesitant to rely solely on USA Freedom Act CDRs.¹³⁹

~~(S//NF)~~ In measuring value, NSA often looks to the number of reports that is generated by a collection platform or methodology.¹⁴⁰ NSA issued relatively few reports based on CDRs collected under the USA Freedom Act. Over a span of four years, NSA wrote and disseminated

¹³⁵ (U) 2018 Statistical Transparency Report at 30. These numbers include duplicates.

¹³⁶ (U) NSA briefing to the Board (May 23, 2019).

¹³⁷ (U) 2018 Statistical Transparency Report at 31. The intelligence community's annual statistical transparency report includes an estimate of the number of search terms associated with a US person used to query USA Freedom Act CDR data. It is likely, however, that these numbers overstate NSA analysts' "true" queries of information concerning a US person because NSA analysts group query terms together to run against multiple repositories that the analyst is authorized to query. The result is that a query containing a large amount of non-telephony metadata could be run against NSA's USA Freedom Act CDR holdings, along with data collected under other authorities more relevant to the analysis. Each of those query items would count in the numbers reported in the annual Statistical Transparency Reports, even though some queries would not conceivably return USA Freedom Act CDRs.

¹³⁸ (U) NSA briefing to the Board (May 23, 2019).

¹³⁹ (U) NSA briefing to the Board (May 23, 2019).

¹⁴⁰ (U) NSA briefing to the Board (May 23, 2019).

only 15 intelligence reports derived in whole or in part from these CDRs.¹⁴¹ While NSA would not expect a metadata collection program to produce as many reports as a content collection program, NSA characterized the 15 reports based on USA Freedom Act CDRs as extremely low for a program of this duration, especially in light of the performance of other collection authorities, including Section 702.¹⁴² NSA stated that an intelligence program of similar duration and cost would be expected to produce thousands or tens of thousands of reports.¹⁴³ Board staff reviewed 14 of the 15 reports; [REDACTED]

(U) NSA typically would use the CDR program in response to a terrorist attack or in response to a known terrorist threat. NSA used the CDR program in the intelligence analysis of the following attacks or threats from November 2015 until the program was suspended:

- ~~(TS//SI//NF)~~ **Ohio machete attack.**¹⁴⁴ On February 11, 2016, a man with a machete attacked customers at the Nazareth Restaurant in Columbus, Ohio.¹⁴⁵ The attack left four restaurant customers wounded; the attacker was killed by responding police officers.¹⁴⁶ NSA produced one report derived in whole or in part from USA Freedom Act CDRs as part of NSA's post-attack investigation and analysis. [REDACTED]
- ~~(TS//SI//NF)~~ **Pulse nightclub attack.**¹⁴⁷ On June 12, 2016, a mass shooter killed 49 people and wounded 53 inside Pulse, a nightclub in Orlando, Florida.¹⁴⁸ The attacker pledged allegiance to the Islamic State of Iraq and Syria ("ISIS") during the attack.¹⁴⁹ NSA produced two reports derived in whole or in part from USA Freedom Act CDRs related to the attack during NSA's post-attack investigation and analysis. [REDACTED]

¹⁴¹ (U) NSA briefing to the Board (May 23, 2019).

¹⁴² (U) As a comparison, during the same timeframe, a subset of NSA reports derived in whole or in part from data obtained by NSA under FISA Section 702 totaled 12,474. 2018 Statistical Transparency Report at 19. Note that this figure includes only reports concerning a US person, and not additional reports derived from data obtained under Section 702 of FISA that do not concern a US person. NSA briefing to the Board (May 23, 2019).

¹⁴³ (U) NSA briefing to the Board (May 23, 2019).

¹⁴⁴ [REDACTED]

¹⁴⁵ (U) *Cops kill man after machete attack at Ohio deli*, CBS NEWS (Feb. 12, 2016).

¹⁴⁶ (U) *Cops kill man after machete attack at Ohio deli*, CBS NEWS (Feb. 12, 2016).

¹⁴⁷ [REDACTED]

¹⁴⁸ (U) Lizette Alvarez & Richard Perez-Pena, *Orlando Gunman Attacks Gay Nightclub, Leaving 50 Dead*, N.Y. TIMES (June 12, 2016).

¹⁴⁹ (U) Lizette Alvarez & Richard Perez-Pena, *Orlando Gunman Attacks Gay Nightclub, Leaving 50 Dead*, N.Y. TIMES (June 12, 2016).

- [REDACTED]
- (U) **Potential terrorist threats.** The remaining reports produced by NSA which were derived in whole or in part from USA Freedom Act CDRs cover communications of persons suspected of having terrorism ties. These reports include information derived from USA Freedom Act CDRs concerning a suspected ISIS recruiter;¹⁵³ a US person located outside the United States who is believed to have been contacted by an international terrorist group;¹⁵⁴ an individual known to NSA as an ISIS supporter;¹⁵⁵ a US

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

person fighting overseas on behalf of an international terrorist group;¹⁵⁶ a suspected ISIS supporter;¹⁵⁷ and a person suspected of an association with ISIS.¹⁵⁸

~~(S//NF)~~ The 14 reports reviewed by Board staff were all similar in substance. They provided charts of contacts including, in some instances, information about individuals of interest associated with the target. In some cases, a person's contacts were conveyed in multiple reports. In others, the information regarding a particular person's contacts was provided in a single report. The number of contacts listed varied from report to report, [REDACTED]
[REDACTED]

~~(TS//SI//NF)~~ The reports combined information derived from USA Freedom Act CDRs with other information collected by NSA, including metadata from collection under Executive Order 12333 and FISA. For example, [REDACTED] Not all of the listed communications in this report were identified directly through USA Freedom Act CDR analysis: [REDACTED]

(U) An important caveat attaches to these reports—it is facially unclear which information in them would have been unavailable without the USA Freedom Act CDR program. This is because the 15 intelligence reports combined data from different authorities, such as Executive Order 12333 and FISA. In certain instances, NSA and FBI worked together to determine what parts of a report contained unique information gained from USA Freedom Act CDRs. The value that FBI obtained from these reports is discussed below.

C. (U) FBI Use of USA Freedom Act CDR Program Intelligence Reporting

(U) FBI received all reporting derived from the CDR program.¹⁶⁰ NSA intelligence reports, including those generated in part from the CDR program, allow readers or users of the

¹⁵⁶ [REDACTED]

¹⁵⁷ [REDACTED]

¹⁵⁸ [REDACTED]

¹⁵⁹ [REDACTED]

¹⁶⁰ (U) FBI briefing to the Board (June 11, 2019).

report to provide feedback.¹⁶¹ Neither NSA nor FBI is aware of any contemporaneous feedback from FBI or others suggesting that any of the 15 intelligence reports were, or were not, useful for these earlier stage investigatory and analytical activities. However, FBI subsequently conducted a review of the CDR program's contributions. During a briefing to Board staff, FBI explained that while most of the NSA intelligence reports provided redundant information, two reports provided unique information to FBI.¹⁶²

(U) During its review of the contributions of the CDR program, FBI determined that, of the 15 reports, 11 duplicated information that was already present in FBI files.¹⁶³ Of the remaining four reports, FBI determined that two contained information that was duplicated by FBI through information that FBI had received from the use of other lawful process.¹⁶⁴ This duplication reflects the fact that FBI can acquire one-hop metadata using a variety of other legal authorities, including grand-jury subpoenas. Agents can then progressively expand their map of a suspect's network by seeking a series of individualized court orders as new information comes in.

~~(TS//SI//NF)~~ FBI received unique information from the remaining two intelligence reports. The first report

¹⁶⁵

¹⁶⁶ FBI decided to open a foreign intelligence investigation based on the information contained in NSA's USA Freedom Act intelligence report, which included relevant "first hop" information from the USA Freedom Act and relevant information from another legal authority.¹⁶⁷

¹⁶⁸

¹⁶¹ (U) NSA briefing to the Board (May 23, 2019).

¹⁶² (U) FBI briefing to the Board (Oct 23, 2019).

¹⁶³ (U) FBI briefing to the Board (June 11, 2019).

¹⁶⁴ (U) FBI briefing to the Board (June 11, 2019).

¹⁶⁵ (U) FBI briefing to the Board (June 11, 2019).

¹⁶⁶ (U) FBI discussion with Board staff (Aug. 16, 2019).

¹⁶⁷ (U) FBI briefing to the Board (June 11, 2019).

¹⁶⁸ (U) FBI discussion with Board staff (Aug. 16, 2019).

[REDACTED]

169

~~(TS//SI//NF)~~ FBI used information in the second report to vet one other individual.¹⁷⁰
After doing so, FBI decided not to open an investigation or take further action.¹⁷¹ [REDACTED]

[REDACTED]

¹⁶⁹ (U) FBI briefing to the Board (June 11, 2019).

¹⁷⁰ (U) FBI briefing to the Board (June 11, 2019).

¹⁷¹ (U) FBI briefing to the Board (June 11, 2019).

IV. (U) Legal Analysis

(U) The Board’s statute authorizes us to review “actions by the executive branch relating to efforts to protect the nation from terrorism to determine whether such actions . . . are consistent with governing laws, regulations, and policies regarding privacy and civil liberties.”¹⁷² We understand our statutory mandate to reflect Congress’s desire that it receive a full, fair, and impartial assessment of a program’s legality when the Board issues reports.¹⁷³ Congress no doubt recognized that some programs, such as the now-suspended CDR program under the USA Freedom Act, might never give rise to litigation.¹⁷⁴ Moreover, many of the facts underlying a program’s operation might remain classified, thereby raising questions in Congress as well as the public whether the government has complied with its legal obligations in implementing the program. Finally, Congress itself might want additional legal advice as it fulfills its constitutional duty to enact the nation’s laws.¹⁷⁵

(U) For these reasons, we consider the USA Freedom Act CDR program in light of the Constitution’s Fourth Amendment and the text of the statutory framework.

¹⁷² (U) 42 U.S.C. § 2000ee(d)(2)(C)(ii).

¹⁷³ (U) The Board does not issue binding legal judgments like a court, nor does its legal advice bind actors within the executive branch. *See, e.g.*, 28 U.S.C. §§ 511, 512 (conferring such authority on the Attorney General); *Management of Federal Resources*, Executive Order 12,146. The Board’s legal advice is advisory and relevant to the extent it has “the power to persuade.” *Skidmore v. Swift & Co.*, 323 U.S. 134, 140 (1944).

¹⁷⁴ (U) With respect to the CDR program, limitations imposed by Article III of the Constitution would likely preclude a challenge to the program’s constitutionality, absent the government’s initiation of a criminal prosecution relying on evidence from the program. *See Clapper v. Amnesty International*, 568 U.S. 398, 410 (2013) (allegations relied on a “highly speculative fear” that plaintiffs’ communications would be collected, rather than demonstrating that alleged injuries were “certainly impending”); *cf. American Civil Liberties Union v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (plaintiffs challenging bulk CDR program “need not speculate that the government has collected, or may in the future collect, their call records”). The Second Circuit’s holding in *ACLU v. Clapper* rested on the fact that FISA court orders underpinning the bulk CDR program required “the production of all call detail records or telephony metadata,” *ACLU v. Clapper*, 785 F.3d. at 797 (internal quotation marks omitted), an approach to collection prohibited under the USA Freedom Act.

¹⁷⁵ (U) Our colleagues question the “utility of a constitutional analysis” given the Board’s “limited time and resources.” Statement of Ed Felten & Travis LeBlanc at 70. They suggest that is so because the USA Freedom Act CDR program “has been suspended,” “its existence and primary contours were publicly known and debated, and it was subject to oversight by the Foreign Intelligence Surveillance Court.” Statement of Ed Felten & Travis LeBlanc at 70. Respectfully, we disagree. Although the CDR program may currently be suspended, Congress is considering the reauthorization of a statutory provision under which the program could be restarted. In addition, the facts of the program are not “publicly known”; although many such facts have been released to the public for the first time as a result of the Board’s report, some remain classified. Finally, FISA court opinions often remain classified, precluding public knowledge of the conclusions—constitutional and otherwise—the court reaches. Whether the government has, in the past, acted consistent with the Constitution in implementing a classified program is of significant relevance to public debates over the appropriate statutory regimes to govern such programs.

A. (U) Fourth Amendment Analysis

1. (U) Summary

(U) The CDR collection program authorized by the USA Freedom Act was constitutional. Governing Supreme Court case law makes clear that collection of telephone dialing and routing information is not a “search” or “seizure” under the Fourth Amendment. The Supreme Court’s recent decision in *Carpenter v. United States* expressly reaffirmed that the key precedent establishing this principle, *Smith v. Maryland*, remains the law of the land.¹⁷⁶ Meanwhile, the USA Freedom Act barred the government from collecting the content of calls or cell-site location information, two types of data that typically require a warrant under Supreme Court precedent.

(U) Our conclusion accords with the Board’s unanimous conclusion in 2014 that the previous bulk CDR collection program was constitutional.¹⁷⁷ That program was more expansive and had fewer safeguards than this one: it involved bulk collection, rather than targeted collection based on individualized suspicion, and did not require judicial approval of individual selection terms. If that program was constitutional, it is difficult to see how this much narrower program would not be. The Board’s conclusion in its 2014 Report on the bulk CDR program remains valid: “Until the Supreme Court rules otherwise, *Smith v. Maryland* and the third-party doctrine remain in force today. Government lawyers are entitled to rely on them when appraising the constitutionality of a given action.”¹⁷⁸

(U) Finally, we note that our conclusion accords with Congress’s view when it enacted the USA Freedom Act. Sixty-seven Senators and 338 Members of the House voted for the Act. Senators who supported the Act believed that it would “protect[] the privacy of individuals”¹⁷⁹ while defending national security in a manner that is “respectful of the . . . letter and the spirit of the Fourth Amendment.”¹⁸⁰ Senate and House Members, including long-serving members of the Judiciary Committee, argued that “the USA FREEDOM Act represents a return to the basic principle of the Fourth Amendment”¹⁸¹ and effected “historic and sweeping reforms to the

¹⁷⁶ (U) 138 S. Ct. 2206, 2220 (2018).

¹⁷⁷ (U) *See* 2014 Board Report at 126; 2014 Board Report at 210 (statement of Rachel Brand) (“I agree with the Board’s ultimate conclusion that the program is constitutional under existing Supreme Court caselaw.”); 2014 Board Report at 215 (statement of Elisebeth Cook) (“Our conclusion that the program does not violate the Fourth Amendment is unanimous, as it should be.”).

¹⁷⁸ (U) 2014 Board Report at 126.

¹⁷⁹ (U) Statement of Sen. Leahy, Cong. Reg. S. 3422 (June 2, 2015); *see also* Cong. Reg. S. 3431 (June 2, 2015) (statement of Sen. Wyden) (“[W]e are going to protect their liberty and we are going to strengthen their security[.]”).

¹⁸⁰ (U) Statement of Sen. Lee, Cong. Reg. S. 3423 (June 2, 2015).

¹⁸¹ (U) Statement of Rep. Nadler, Cong. Rec. H. 2916 (May 13, 2015).

government's surveillance program and powers."¹⁸² These Members believed themselves to be protecting the Constitution, not violating it. We agree that the law they enacted was constitutional.

2. (U) The CDR Program Complied with the Fourth Amendment

(U) The Fourth Amendment provides that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."¹⁸³

(U) We first consider whether the collection of telephony metadata under the CDR program constituted a "search" or "seizure" under the Amendment's text as interpreted by relevant Supreme Court cases. We believe it did not, and that the program was constitutional for this reason alone. We then consider whether, even assuming it effected a "search" or "seizure," the program was nevertheless "reasonable" and, thus, constitutional. Consistent with the Board's analysis in its 2014 report, and its disinclination to offer constitutional opinions where unnecessary, we do not arrive at a conclusion on reasonableness; rather, we preview the analysis that a court would likely undertake. We conclude with our thoughts on the separate statement authored by our colleagues.

a.

(U) To begin, the collection of CDRs under the CDR program does not constitute a "search" or "seizure" under controlling Fourth Amendment precedent. The Supreme Court held in *Smith v. Maryland* that the government's acquisition of telephone dialing information using a pen register does not constitute a "search" under the Fourth Amendment, and therefore does not trigger the Amendment's protections.¹⁸⁴ In *Smith*, the Court rejected the argument that a caller has a "'legitimate expectation of privacy' regarding the numbers he dialed on his phone," finding it "too much to believe that telephone subscribers. . . harbor any general expectation that the numbers they dial will remain secret."¹⁸⁵ It further held that even if a caller had a subjective expectation of privacy in the numbers dialed, it would not be "one that society is prepared to recognize as 'reasonable.'"¹⁸⁶ "This Court," it explained, "consistently has held that a person

¹⁸² (U) Statement of Rep. Conyers, Cong. Rec. H. 2915 (May 13, 2015).

¹⁸³ (U) U.S. Const. amend. IV.

¹⁸⁴ (U) *See Smith*, 442 U.S. 745–46.

¹⁸⁵ (U) *Smith*, 442 U.S. at 742–43.

¹⁸⁶ (U) *Smith*, 442 U.S. at 743 (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967)).

has no legitimate expectation of privacy in information he voluntarily turns over to third parties,”¹⁸⁷ a principle which has since become known as the “third-party doctrine.”¹⁸⁸

(U) That holding remains good law, even as the Supreme Court has clarified the Fourth Amendment’s application to new technologies, including cellular networks. Most recently (in 2018), in *Carpenter v. United States*, the Court held that a demand issued to a third party for cell-site location information triggered the Fourth Amendment’s warrant requirement.¹⁸⁹ The USA Freedom Act explicitly excludes cell-site location information from collection under the CDR provision.¹⁹⁰ And while *Carpenter* “decline[d] to extend *Smith* and *Miller* to the collection of [cell-site location information],” the Court also reiterated that “the third-party doctrine applies to telephone numbers” and explicitly confirmed *Smith*’s continuing viability: “We do not disturb the application of *Smith*”¹⁹¹

(U) Likewise, four years earlier (in 2014), in *Riley v. California*, the Court held that the search-incident-to-arrest exception to the Fourth Amendment’s warrant requirement does not extend to accessing content stored on the arrestee’s smartphone.¹⁹² In doing so, the Court briefly addressed the relationship between its holding and *Smith*. The Court reaffirmed that *Smith* had held that “the use of a pen register was not a ‘search’ at all under the Fourth Amendment.”¹⁹³ It went on to find *Smith* inapplicable because there was “no dispute [in *Riley*] that the officers engaged in a search of [the] cell phone.”¹⁹⁴ In other words, *Smith* does not allow the government to collect phone numbers when the government first gains access to those numbers by

¹⁸⁷ (U) *Smith*, 442 U.S. at 743–44.

¹⁸⁸ (U) *See* 2014 Board Report at 110.

¹⁸⁹ (U) 138 S. Ct. at 2211–12.

¹⁹⁰ (U) 50 U.S.C. § 1861(k)(3)(B)(iii); *see also* NSA USA Freedom Act Transparency Report at 4 (“CDRs do not include . . . cell site location or global positioning system information[.]”).

¹⁹¹ (U) *Carpenter*, 138 S. Ct. at 2220 (emphasis added). The Supreme Court’s decision in *United States v. Miller*, 425 U.S. 435 (1976), upheld the collection of bank records by subpoena and without a warrant, *see Miller*, 425 U.S. at 440, and is often grouped with *Smith* as a case involving the “third-party doctrine.”

(U) Lower courts have since held *Carpenter* inapplicable “to grand jury subpoenas sent to an internet service provider (ISP) and an email provider for subscriber information associated with an ISP account and an email address,” “to fixed video monitoring, location-revealing bank records, and online-shopping histories.” Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After Carpenter*, Yale L.J. Forum 943, 950–51 (2019) (footnotes omitted). While we do not necessarily endorse the reasoning or holdings of these lower court cases (a result unnecessary to our opinion in this report), they demonstrate that *Smith* remains a live part of the jurisprudence after *Carpenter*.

¹⁹² (U) 573 U.S. 373, 386 (2014).

¹⁹³ (U) *Riley*, 573 U.S. at 400.

¹⁹⁴ (U) *Riley*, 573 U.S. at 400.

conducting a “search.”¹⁹⁵ Collecting CDRs under the USA Freedom Act does not involve any antecedent search by the government; under the Act, the government serves companies with court orders comparable to those they receive every day in criminal investigations.

(U) *Riley* is different from the CDR program for a second reason. In *Riley*, the government argued that even if other information on a phone was constitutionally protected, it “should always be able to search a phone’s call log.”¹⁹⁶ The Court rejected that argument, noting that smartphone call logs “typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label ‘my house.’”¹⁹⁷ The CDR provision, by contrast, explicitly prohibits the government from obtaining the contents of any communication, “the name, address, or financial information of a subscriber or customer,” or location information.¹⁹⁸ Telephony metadata, unlike smartphone call logs, does not include “any information that an individual might add”; rather, it comprises dialing and routing information recorded by the company.¹⁹⁹ The type of information that the government may collect under the USA Freedom Act CDR provision resembles the information collected by the pen register in *Smith* rather than the call logs in *Riley*.²⁰⁰ In short, there is no evidence that *Riley* intended to

¹⁹⁵ (U) A simple analogy might make this holding clearer. Assume that a suspect were to leave a paper with a list of phone numbers inside his house on his kitchen table. Assume that the government were to break into the house and obtain the list of phone numbers, without probable cause and a warrant, contrary to the Fourth Amendment. The government could not then argue that obtaining the list of phone numbers was not a “search” under the Fourth Amendment. The government’s immediately preceding actions—namely, breaking into the house without the requisite cause and warrant—would constitute a “search” under the Fourth Amendment, thereby triggering the Constitution’s protections. See *United States v. Turner*, 839 F.3d 429, 434 n.2 (5th Cir. 2016) (“There was no dispute in *Riley* that reviewing the contents of a cell phone involved a search. At issue was only whether such a search was permissible without a warrant when conducted during an arrest.”); *United States v. Guerrero*, 768 F.3d 351, 360 n.7 (5th Cir. 2014) (“The [*Riley*] Court’s concerns were thus cabined to the unique circumstances of the search-incident-to-arrest doctrine, and did not overrule the separate line of cases, including *Smith*, dealing with information already in the possession of an identifiable third party.”).

¹⁹⁶ (U) *Riley*, 573 U.S. at 400.

¹⁹⁷ (U) *Riley*, 573 U.S. at 400.

¹⁹⁸ (U) 50 U.S.C. § 1861(k)(3).

¹⁹⁹ (U) See FISC Order No. 0007-10, at 2 (May 2, 2007) (“Telephony meta data includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, communications device identifier, etc.), trunk identifier, telephone calling card numbers and time and duration of call”) [declassified, redacted opinion].

²⁰⁰ (U) Compare 18 U.S.C. § 3127(3) (pen register records “dialing, routing, addressing, or signaling information” but not “the contents of any communication”), with 50 U.S.C. § 1861(k)(3) (CDRs may include “session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call,” but not “the contents . . . of any communication,” “the name, address, or financial information of a subscriber or customer,” or “cell site location or global positioning system information”); see also *Riley*, 573 U.S. at 400 (distinguishing digital call log from “pen register” at issue in *Smith*); NSA USA Freedom Act Transparency Report at 10 (“CDRs, per the statute, contain only telephone metadata and not, for example, the contents of any personal communication or the caller’s name or location of any phone call.”).

alter *Smith*—a point reaffirmed when, as noted above, the Court subsequently made clear in *Carpenter* that it had not “disturb[ed] the application of *Smith*.”²⁰¹

(U) One-hop collection of CDRs under FISA’s business-records provision,²⁰² also known as Section 215 (after the section of the USA Patriot Act that brought this authority close to its current form), is comparable to the type of CDR production common in criminal investigations. Much as grand-jury subpoenas can be used to obtain business records relevant to criminal inquiries, Section 215 authorizes the FISA court to issue orders compelling the production of “tangible things,” including business records, in national-security investigations.²⁰³ Ordinary application of Section 215 to collect one “hop” of CDRs seeks to place the government in the same position when it compels production of information in national-security cases as when it compels production in criminal cases.

(U) While the use of Section 215 to obtain “one hop” of CDRs would operate much like the use of the pen register in *Smith v. Maryland*, this program raises the additional question of whether collecting a “second hop” of dialing information, as authorized by the USA Freedom Act, affects the constitutional analysis.

(U) The inclusion of “second hop” information results in the collection of a large number of records.²⁰⁴ The Court’s decision in *Smith* does not suggest, however, that the *number* of phone records determines whether collection constitutes a Fourth Amendment “search” for purposes of the warrant requirement.²⁰⁵ To the contrary: *Smith* and more recent cases focus on the *nature* of call metadata records, rather than the number of data points gathered by the

²⁰¹ (U) 138 S. Ct. at 2220.

²⁰² (U) 50 U.S.C. § 1861.

²⁰³ (U) Specifically, the statute permits the government to “make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.” 50 U.S.C. § 1861(a)(1).

²⁰⁴ (U) This is disclosed by the intelligence community’s Annual Statistical Transparency Reports. See, e.g., 2018 Statistical Transparency Report.

²⁰⁵ (U) The District Court opinion in *Klayman v. Obama*, a challenge to the bulk CDR program, would have taken the alternative view. See 957 F. Supp. 2d 1, 35–36 (D.D.C. 2013) (“Admittedly, what metadata *is* has not changed over time. As in *Smith*, the *types* of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like. But the ubiquity of phones has dramatically altered the *quantity* of information that is now available, and, more importantly, what that information can tell the government about people’s lives.”), *vacated and remanded by Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015). That opinion was vacated by the D.C. Circuit, however, and its reasoning as to telephone metadata has not been adopted by other courts. Moreover, its holding arose in the context of the government’s program collecting CDRs in *bulk*. The court did not have occasion to consider whether the same analysis would apply if the government collected solely the second “hop” of metadata. See, e.g., *Klayman v. Obama*, 957 F. Supp. 2d at 35–36 (relying on the “all-encompassing, indiscriminate” nature of the collection under the previous bulk telephony program).

government on a programmatic level. The Court in *Carpenter v. United States*, for example, distinguished cell-site location data from *Smith*'s pen register by noting that the former is more revealing: "After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier *not just dialed digits, but a detailed and comprehensive record of the person's movements*."²⁰⁶ Similarly, *Smith* explained that "pen registers do not acquire the contents of communications," "do not hear sound," and "disclose only the telephone numbers that have been dialed."²⁰⁷ To be sure, collection of telephone metadata at this scale raises legitimate policy concerns about its implications for privacy and civil liberties. But the Supreme Court has not elevated those concerns to a constitutional dimension by holding that collection of telephone call metadata can constitute a Fourth Amendment "search" or "seizure."²⁰⁸

b.

(U) *Even assuming* that the collection of CDRs under the CDR program could constitute a "search" or "seizure" under the Fourth Amendment, the program could find a constitutional basis under a separate strand of Fourth Amendment jurisprudence arising in the national security context. The Supreme Court has acknowledged that the Fourth Amendment may require different "safeguards" in the national security context than in ordinary criminal cases.²⁰⁹ Indeed, in *Carpenter*, the Court explained that its "opinion d[id] not consider other collection techniques involving foreign affairs or national security."²¹⁰

(U) Based on such language, lower courts, including the Foreign Intelligence Surveillance Court of Review, have embraced a "foreign intelligence" exception to the Fourth Amendment's warrant and probable cause requirement.²¹¹ These courts have held that foreign

²⁰⁶ (U) *Carpenter*, 138 S. Ct. at 2217 (emphasis added).

²⁰⁷ (U) *Smith*, 442 U.S. at 741–42.

²⁰⁸ (U) We do not address whether and how the quantity of data collected by the government impacts the Fourth Amendment analysis with respect to other types of information. *Cf. Carpenter*, 138 S. Ct. at 2217 n.3.

²⁰⁹ (U) *Katz v. United States*, 389 U.S. 347, 358 n.23 (1967); *United States v. U.S. Dist. Court for E. Dist. of Mich.*, 407 U.S. 297, 308–09 & n.8 (1972).

²¹⁰ (U) *Carpenter*, 138 S. Ct. at 2220.

²¹¹ (U) *See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1010 (FISA Ct. Rev. 2008); *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980); *accord United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973). Our colleagues would not here rely on the foreign intelligence exception to the warrant requirement or, more generally, the special needs exception. *See* Statement of Ed Felten and Travis LeBlanc at 71 n.336. Yet they do not make clear whether any other exception would apply. Their "reluctan[ce]" to rely on the special needs exception is grounded in a citation of a decades-old *dissenting* opinion of the Supreme Court. Statement of Ed Felten and Travis LeBlanc at 71 n.336 (citing *Skinner v. Railway Lab Execs. Ass'n*, 489 U.S. 602 (1989) (Marshall, J., dissenting)), but that exception has long been treated as settled law by the Supreme Court, *see, e.g., Los Angeles v. Patel*, 135 S. Ct. 2443, 2452 (2014) ("Search regimes where no warrant is ever required may be reasonable where special needs . . . make the warrant and probable-cause requirement impracticable, and where the primary purpose of the searches is

intelligence searches must satisfy the Fourth Amendment requirement of “reasonableness,” rather than the usual requirement that the government obtain probable cause and a warrant.

(U) The Foreign Intelligence Surveillance Court of Review has explained current doctrine in the following manner:

(U) When law enforcement officials undertake a search to uncover evidence of criminal wrongdoing, the familiar requirement of a probable-cause warrant generally achieves an acceptable balance between the investigative needs of the government and the privacy interests of the people. But it has long been recognized that some searches occur in the service of “special needs, beyond the normal need for law enforcement,” and that, when it comes to intrusions of this kind, the warrant requirement is sometimes a poor proxy for the textual command of reasonableness.

...

(U) [I]n this context, the warrant requirement is ill-suited to gauge what is reasonable. The textual command of reasonableness—“the ultimate touchstone of the Fourth Amendment,”—still governs. Indeed, it retains its whole force.²¹²

(U) Reasonableness analysis “examine[s] the totality of the circumstances and weigh[s] the promotion of legitimate governmental interests against the degree to which the search intrudes upon an individual’s privacy.”²¹³ Various factors would be relevant to assessing the Fourth Amendment reasonableness of the CDR program. The presence of “privacy protecting measures,” including “FISC-approved targeting and minimization” procedures, forms one

distinguishable from the general interest in crime control.” (citations, brackets, and internal quotation marks omitted)) (per Sotomayor, J.), and provides the constitutional basis for the passenger screening carried out by the Transportation Security Administration at airport checkpoints. See *Ruskai v. Pistole*, 775 F.3d 61, 68 (1st Cir. 2014) (“The courts of appeals treat transit security screenings as ‘administrative’ or ‘special needs’ searches, which may be conducted, at least initially, without individualized suspicion, a warrant, or probable cause.” (collecting cases)).

²¹² (U) *In re Certified Question of Law*, 858 F.3d 591, 605, 607 (FISA Ct. Rev. 2016) (citations omitted). The court’s holding is instructive on the question we address here. The court held: “when the government, acting pursuant to a program of surveillance involving a legitimate objective that goes beyond everyday crime control, seeks to use a pen register directed at a person located in the United States who is reasonably believed to be engaged in clandestine intelligence activities on behalf of a foreign government, it may do so without obtaining a probable-cause warrant even if its monitoring of post-cut-through digits constitutes a search under the Fourth Amendment.” *In re Certified Question of Law*, 858 F.3d at 605. In other words, the court held that, even if the particular collection at issue in the case would constitute a “search” and therefore require a warrant in the criminal context, a “probable-cause warrant” was not required in the context of a foreign-intelligence search. The court went on to hold that “[t]he search, assuming it is one, is reasonable.” *In re Certified Question of Law*, 858 F.3d at 607.

²¹³ (U) *United States v. Mohamud*, 843 F.3d 420, 441 (9th Cir. 2016) (quoting *Maryland v. King*, 569 U.S. 435, 448 (2013) (brackets and internal quotation marks omitted)).

“important component of the reasonableness inquiry.”²¹⁴ Others include the nature of the information collected, the privacy interest that attaches, and the government interest in the collection.

(U) In conducting this analysis, courts assess whether a proposed investigatory activity was reasonable *given what the government knew at the time*, rather than with the benefit of hindsight. In other words, rather than assess the success of a particular wiretap or a particular program based on what the government discovered, a court conducts a reasonableness analysis by placing itself in the shoes of a government investigator at the time of the government “search.” As then-Judge Scalia put the point, “just as ‘a search is not to be made legal by what it turns up,’ the fact that, *ex post*, a wiretap is seen to have been unsuccessful in developing national-security information does not establish that, *ex ante*, it was not reasonable to conduct it for that purpose.”²¹⁵ Similarly, then-Judge Ruth Bader Ginsburg explained “[t]hat probable cause may have been absent when viewing the arrest *ex post* does not in and of itself establish that the officer acted in an objectively unreasonable manner *ex ante*.”²¹⁶ Indeed, the contrary rule would mean that every government search that was lawfully predicated at the time would ultimately be “unreasonable” if it failed to discover evidence related to a crime or foreign intelligence. On that logic, every time the government properly elected, as a matter of sound policy, to shut down a program, the program would become unconstitutional because the government had effectively conceded that the program’s costs outweighed its benefits.²¹⁷

²¹⁴ (U) *Mohamud*, 843 F.3d at 443.

²¹⁵ (U) *Smith v. Nixon*, 807 F.2d 197, 203 (D.C. Cir. 1986) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948) (footnote omitted)).

²¹⁶ (U) *Martin v. Malhoyt*, 830 F.2d 237, 263 (D.C. Cir. 1987); *see also Anderson v. Creighton*, 483 U.S. 635, 639 (1987) (observing that the relevant Fourth Amendment inquiry is whether “in the light of preexisting law the unlawfulness” of government action was “apparent” and describing the question as an “objective (albeit fact-specified) [inquiry into] whether a reasonable officer could have believed” action was legal). For other cases using a similar approach in a variety of Fourth Amendment-related circumstances, *see Bruce v. Guernsey*, 777 F.3d 872 (7th Cir. 2015) (“Guernsey also argues that the fact that Bruce was ultimately admitted to the hospital and later involuntarily committed to a behavioral health center for three days demonstrates that he had probable cause to seize her. But the Fourth Amendment requires an *ex ante*, not an *ex post*, analysis.”); *United States v. Green*, 560 F.3d 853, 857 (8th Cir. 2009) (rejecting *ex post* analysis regarding whether a particular dresser could completely conceal a person).

²¹⁷ (U) That is why we focus on the perspective of those who established the CDR program. As for “whether an extension of that authority would be constitutional in light of the facts and circumstances known today,” Statement of Ed Felten and Travis LeBlanc at 71, we do not believe that a statute enacted by Congress to reauthorize the CDR program would be “facially” unreasonable, and hence unconstitutional, under the Fourth Amendment. The Court has made clear that “claims for facial relief under the Fourth Amendment”—direct attacks on the constitutionality of a statute, as opposed to the statute’s application to a particular set of facts—“are unlikely to succeed when there is substantial ambiguity as to what conduct a statute authorizes.” *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2450 (2015). That is because, to succeed on such a facial challenge, a “plaintiff must establish that a law is unconstitutional *in all of its applications*.” *Patel*, 135 S. Ct. at 2451 (emphasis added, quotation marks

(U) Viewing the CDR program from the “*ex ante*” perspective of those who initiated it, many factors weigh in favor of finding the program reasonable for constitutional purposes. To obtain FISA court approval for each “specific selection term” that was the basis for CDR collection, the government was required to demonstrate a “reasonable, articulable suspicion” that the specific selection term was associated with international terrorism.²¹⁸ The program was implemented under FISA court oversight, minimization procedures mandated by Congress and approved by the court, and internal oversight by NSA.²¹⁹ Moreover, the USA Freedom Act’s CDR provision expressly limits collection to information comparable to a pen register—dialing and routing information, a category of information about which, the Supreme Court held in *Smith*, callers have “no legitimate expectation of privacy.”²²⁰ And the program was inarguably run in furtherance of “the paramount interest in investigating possible threats to national security.”²²¹ That interest, the Supreme Court has held, “is an urgent objective of the highest order.”²²²

(U) On the other hand, the CDR program reached out to the second hop, capturing metadata about calls in which neither of the participants was the object of the “reasonable, articulable suspicion” reviewed by the court. And given the inherent math of multi-hop collection, the number of records collected at each succeeding hop would foreseeably be exponentially larger than those at the preceding hop.²²³ The result would be that the largest

omitted). Where a Fourth Amendment challenge to a statute necessarily rises or falls on the basis of facts yet unknown (such as a program’s costs and efficacy), such a challenge cannot be brought “facially.”

²¹⁸ (U) 50 U.S.C. § 1861(b)(2); *cf. In re Certified Question of Law*, 858 F.3d at 607–08 (referring, in Fourth Amendment reasonableness analysis, to “the investigative importance of having access to the dialing information provided by post-cut-through digits”). By contrast, in the Section 702 program held reasonable in *Mohamud*, targeting decisions were made pursuant to court-approved procedures but not individually reviewed by the FISA court. 843 F.3d at 443–44. (The court in *Mohamud* also held, in the alternative, that the 702 collection in that case did not require a warrant because it “was targeted at a non-U.S. person with no Fourth Amendment right.” *Mohamud*, 843 F.3d at 439 (citing *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990))).

²¹⁹ (U) *See* NSA USA Freedom Act Transparency Report at 13 (“Analysts will require appropriate and adequate training, and must have both an international terrorism mission purpose and a need to know in order to be provided access to the CDRs obtained through the USA Freedom Act. Analyst queries of records acquired under the USA Freedom Act will be intended to determine or identify persons of foreign intelligence interest who may be engaged in international terrorism. All queries will be subject to post-query auditing. The USA Freedom Act data will be used to produce intelligence reports, following reporting and minimization procedures.”). *Cf. In re Certified Question of Law*, 858 F.3d at 608 (relying, to assess Fourth Amendment reasonableness, on “the fact that FISA pen register interceptions are conducted only with the approval and under the supervision of a neutral magistrate, in this case a FISC judge” and that “minimization procedures are available, and are regularly employed”).

²²⁰ (U) *Smith*, 442 U.S. at 742; *see* 50 U.S.C. § 1861(k)(3).

²²¹ (U) *In re Certified Question of Law*, 858 F.3d at 607.

²²² (U) *Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010); *see also Haig v. Agee*, 453 U.S. 280, 307 (1981) (“no governmental interest is more compelling” than national security).

²²³ (U) *See* Remarks of Michael Bahar at Privacy and Civil Liberties Oversight Board Public Forum on the USA Freedom Act (May 31, 2019) (“But of course, the more hops, the greater the exponential sweep of records.”).

proportion of communicants in the records collected—the second-hop contacts—would be people who were neither the objects of “reasonable, articulable suspicion” themselves nor in direct contact with the object of that suspicion.²²⁴

(U) In weighing these factors, Fourth Amendment reasonableness analysis resists clear rules or rigid formulas.²²⁵ It is informative, however, that in the past few years, both the Foreign Intelligence Surveillance Court of Review and the United States Court of Appeals for the Ninth Circuit have upheld as reasonable under the Fourth Amendment the incidental (but foreseeable) collection of *content* in the context of FISA surveillance.²²⁶ (Notably, the Foreign Intelligence Surveillance Court of Review’s analysis also presumed that collecting a second tranche of “dialing information,” beyond the first number dialed, raised no constitutional problem.²²⁷) While the collection of a second hop here is intentional rather than incidental, the privacy interest attached to the category of information collected—telephone dialing and routing information—is, under settled Supreme Court precedent, qualitatively weaker, and the program was surrounded by comparable (in some respects, stronger) oversight safeguards.²²⁸

(U) Because the Board concludes that the program was constitutional under the *Smith* line of precedent described above, we need not resolve whether it separately would be constitutional under a reasonableness analysis. This accords with the Board’s 2014 report²²⁹ and reflects the Board’s disinclination to offer constitutional opinions where unnecessary; it is not a view of the merits.²³⁰

²²⁴ (U) Our report also describes various facts about the operation of the program in practice.

²²⁵ (U) *See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012–13 (FISA Ct. of Rev. 2008) (rigid test “would be at odds with the totality of the circumstances test that must guide an analysis in the precincts patrolled by the Fourth Amendment”).

²²⁶ (U) *In re Certified Question of Law*, 858 F.3d at 610; *Mohamud*, 843 F.3d at 441. In *In re Certified Question of Law*, the “content” at issue consisted of certain “additional digits” dialed after a telephone call is connected, which “do not constitute dialing information, but instead constitute a form of content information.” 858 F.3d at 594. These could include “a password, a personal identification number, . . . a bank account number,” “a credit card number,” “or a Social Security number.” *In re Certified Question of Law*, 858 F.3d at 594. By contrast, the USA Freedom Act’s CDR provision authorized the government to receive only limited categories of non-content information: “session-identifying information . . . , a telephone calling card number, or the time or duration of a call.” 50 U.S.C. § 1861(k)(3)(A).

²²⁷ (U) *See In re Certified Question of Law*, 858 F.3d at 594 & n.2.

²²⁸ (U) For example, under Section 702, targeting decisions are made by agencies themselves, subject to court-approved procedures. Under the USA Freedom Act CDR provision, the FISA court must approve each specific selection term used as the basis for collection. *See Mohamud*, 843 F.3d at 443–44.

²²⁹ (U) The Board’s 2014 report on the bulk CDR report limited its constitutional analysis to the *Smith*-based rationale. *See* 2014 Board Report at 126.

²³⁰ (U) To the extent our colleagues mean to suggest the program is vulnerable on First Amendment grounds, *see* Statement of Ed Felten and Travis LeBlanc at 76–77, we disagree. Assuming an intelligence program consistent with the Fourth Amendment could violate the First Amendment, *cf. Am. Civil Liberties Union v. Clapper*, 959 F. Supp. 2d 724, 753 (S.D.N.Y. 2013), *aff’d in part, vacated in part, remanded*, 785 F.3d 787 (2d Cir. 2015)

c.

(U) As explained elsewhere in this Report, we share our colleagues’ judgment that the CDR program’s value did not appear to outweigh its “risks and cost.”²³¹ As for the program’s constitutionality, we agree with our colleagues “that *Smith* remains good law” and that “the government had a reasonable legal argument” that the CDR program “was consistent with the Fourth Amendment at its inception.”²³² But we part ways with our colleagues’ judgments on the role that the Board can and should play in providing clear guidance to lawmakers and policymakers who seek to respect constitutional limits in designing intelligence programs—and who may be considering whether to reauthorize the two-hop provision of the USA Freedom Act. We worry that a conclusion that the entirety of Fourth Amendment doctrine is up for grabs may cast a cloud of legal uncertainty over the now-shuttered CDR program, without providing a clear theory of constitutional infirmity. Although it would intimate (while not concluding outright) that the program may have been unconstitutional, it would do so without offering the lawmakers who passed it and the government employees who implemented it a concrete explanation for why they may have violated the law, despite their sincere beliefs to the contrary. Our constitutional analysis has therefore sought to chart a reasonable middle ground of providing predictability where we see it in the doctrine, while not resolving questions unnecessary to a bottom-line constitutional analysis. We believe that this approach is the way that the Board may most effectively serve Congress, the Executive Branch, and the public. It is rare that a novel program does *not* diverge from prior cases, such as, here, *Smith* and its progeny; the question is how those distinctions affect the legal analysis. That is the question we have sought to address. And on that point, our colleagues’ statement is largely silent.²³³ Their statement posits, for example, that *Carpenter* and *Riley* “carry more significance in assessing the constitutionality of the CDR program . . . than the majority affords them,”²³⁴ yet does not explain what that significance might be.

(U) More concretely, our colleagues’ statement does not make clear how to apply *Smith* and subsequent cases to an analysis of the CDR program or other metadata-collection authorities.

(finding “well-supported” the government’s argument that “surveillance consistent with Fourth Amendment protections . . . does not violate First Amendment rights”), the collection of CDRs under the USA Freedom Act is not such a program. “[A]ny alleged chilling effect here arises from [a person’s] speculative fear that the Government will review telephony metadata related to [their] telephone calls.” *ACLU v. Clapper*, 959 F. Supp. 2d at 754. Such a fear was found insufficient to establish a First Amendment violation in the context of the bulk telephony program, *ACLU v. Clapper*, 959 F. Supp. 2d at 754; *cf.* 2014 Board Report at 136; 2014 Board Report at 210 (statement of Rachel Brand) (“I agree with the Board’s ultimate conclusion that the program is constitutional under existing Supreme Court caselaw.”), and by extension would be insufficient here as well.

²³¹ (U) Statement of Ed Felten and Travis LeBlanc at 68.

²³² (U) Statement of Ed Felten and Travis LeBlanc at 74.

²³³ (U) Statement of Ed Felten and Travis LeBlanc at 73-75.

²³⁴ (U) Statement of Ed Felten and Travis LeBlanc at 75.

It questions whether the CDR program is “similar enough” to *Smith* for that case to control, citing facts about the most recent incarnation of the CDR program.²³⁵ Specifically, it notes that, in *Smith*, “the police collected the numbers the defendant dialed . . . but did not collect information about the duration of the defendant’s calls or whether the calls were completed”; that, in *Smith*, the police did not “collect information about incoming calls to the defendant’s telephone line”; and that “*Smith* involved a short duration of use of a pen register (no more than 2 days) and the dialing information of just one person.”²³⁶

(U) The apparent implication of reciting these differences is that *Smith* should be strictly limited to those types of dialing information collected by the relatively primitive pen register available in the late 1960s. But if that is right, the USA Freedom Act CDR authority would be just one casualty among many: the Pen Register Statute²³⁷ and the Stored Communications Act,²³⁸ which are used every day in criminal cases, would be similarly vulnerable. So would the FISA business records provision, which allows the government to obtain non-content records based on reasonable, articulable suspicion rather than a probable-cause warrant.²³⁹ Accepting the statement’s narrow view of *Smith* would destabilize criminal and national-security investigations across the United States.

(U) Our colleagues note the potential that CDRs might allow for information about a user’s location in a way that would undermine *Smith*’s applicability and bring the program “into an intermediate area between *Smith* and *Carpenter*.”²⁴⁰ Yet—and as the prior Board pointed out in discussing the bulk telephony program it found constitutional—telephony metadata will often provide general insights into location. For example, area codes and telephone prefixes offer some indicia of location. The possibility our colleagues raise would not appear to be categorically distinct from these well-understood and expected indicia. For example, the mere fact that a subscriber of company A roams into company B’s network would not trigger the creation of a CDR; rather, the subscriber would have to place or receive a call. And even then, doing so would indicate only that they were in *a* company B coverage area, not *which* area.

²³⁵ (U) Statement of Ed Felten and Travis LeBlanc at 74.

²³⁶ (U) Statement of Ed Felten and Travis LeBlanc at 73.

²³⁷ (U) The Pen Register Statute authorizes the collection of both numbers dialed and incoming calls for a duration of 60 days, with the possibility of further 60-day extensions. 18 U.S.C. § 3123 (c); *see also* § 3127(3)–(4) (“pen register” obtains “dialing, routing, addressing, or signaling information”; “trap and trace device” “captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication”).

²³⁸ (U) 18 U.S.C. § 2073(c)–(d) (court order to obtain non-content information about subscribers and “electronic communication service or remote computing service” to issue upon a showing of “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation”).

²³⁹ (U) 50 U.S.C. § 1861.

²⁴⁰ (U) Statement of Ed Felten and Travis LeBlanc at 75.

Roaming, then, would not appear to provide more specific location information than was understood and accepted at the time of *Smith*—or, for that matter, more specific location information than is collected under any other authority that allows the government to receive telephony metadata. Perhaps for that reason, the Board is unaware of any information to support the suggestion that NSA actually used the CDRs in the manner suggested by our colleagues. Now, perhaps technology will change and available location information will become more exact. But the program was suspended. The information available to the government at the time of its operation simply is not the “near perfect surveillance” created by the type of location information discussed in *Carpenter*.²⁴¹

(U) Reasonable people can, of course, disagree in good faith about the legality of a national security program. Yet we worry when Members of the Board cast doubt about the constitutionality of a program (one that operated for years and collected data relating to millions of Americans) without explaining where lawmakers and policymakers may have erred in their efforts to follow the law—or what they can do differently in the future to place programs on surer legal footing.²⁴²

B. (U) Statutory Analysis

(U) In reviewing the operation of the USA Freedom Act CDR program, from its incarnation until its suspension in 2019, the Board considered whether the implementation of the program comported with the text of the statute. The Board concluded that the program was statutorily authorized. Moreover, the Board found no abuse of the program; nor did it find any instance in which government officials intentionally sought records they knew were statutorily prohibited. As noted in Part II(B) of this report, the program did not always function as intended: during its lifetime, a series of compliance incidents and data-integrity concerns arose. These compliance incidents raise technical questions about how to interpret the USA Freedom Act’s authorities in light of complicated and continually evolving telephony infrastructure. Importantly, in response to each compliance incident that raised questions about the scope of permitted collection under the statute, NSA chose not to retain or collect data, even where a reading of the statutory text might have justified it.

²⁴¹ (U) *Carpenter*, 138 S. Ct. at 2210.

²⁴² (U) Although our Board’s legal advice is not binding, *see supra* note 173, our views may have persuasive effect. *See, e.g.*, Statement of Sen. Leahy, Cong. Rec. S. 3426; Statement of Sen. Leahy, Cong. Rec. S. 3339; Statement of Sen. Paul, Cong. Rec. S. 3335 (all citing the Board’s Section 215 report); Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) (citing consultations with the Board in the President’s evaluation of potential intelligence reforms). We should move cautiously and provide clear explanations of constitutional infirmity when we intimate or conclude outright that intelligence programs may have run afoul of the law.

1. (U) The USA Freedom Act CDR Program was Statutorily Authorized

(U) Beginning in 2006, the FISA court accepted the government's argument that the then-existing version of FISA's business-records provision, known as Section 215, permitted bulk collection of CDRs.²⁴³ Once the bulk CDR program was revealed to the public, that interpretation became subject to wider scrutiny. In 2014, the Board's report on Section 215 concluded that NSA's bulk telephony program was not statutorily authorized.²⁴⁴ In May 2015, the United States Court of Appeals for the Second Circuit reached the same conclusion.²⁴⁵ The next month, Congress enacted the USA Freedom Act.²⁴⁶

(U) Unlike the previous bulk program, CDR collection under the USA Freedom Act rested unambiguously on statutory authority. By the time the Act was being debated, the details of the previous bulk program were known publicly. The program had been the subject of multiple press reports; the President had ordered a review of the program and instructed the Department of Justice and Director of National Intelligence to make changes to its implementation;²⁴⁷ and the Board had released its public report. During the debates themselves, Congress heard from an array of government officials and interest groups, many of whom testified to the potential benefits and drawbacks of the program.²⁴⁸

(U) The resulting statute took clear positions on the issues being debated: It authorized the government to compel with a court order the production of CDRs "on a daily basis"²⁴⁹ and to require the "prompt production of a second set of [CDRs]" based on information produced in

²⁴³ (U) See 2014 Board Report at 9 ("In May 2006, the FISC first granted an application by the government to conduct the telephone records program under Section 215. The government's application relied heavily on the reasoning of a 2004 FISA court opinion and order approving the bulk collection of Internet metadata under a different provision of FISA." (citing Order, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 06-05 (FISA Ct. May 24, 2006); Opinion and Order, No. PR/TT [redacted] (FISA Ct.)); Pub. L. 107-56, 115 Stat. 272, 287 (2001) (codified at 50 U.S.C. § 1861 (2001)).

²⁴⁴ (U) 2014 Board Report at 168–72. Two of the five Board Members did not concur with this analysis. 2014 Board Report at 209–18.

²⁴⁵ (U) *American Civil Liberties Union v. Clapper*, 785 F.3d 787, 812 (2d Cir. 2015).

²⁴⁶ (U) Pub. L. No. 114-23, 129 Stat. 268 (2015) (now codified at 50 U.S.C. § 1861 *et seq.*).

²⁴⁷ (U) See The White House, *Presidential Memorandum—Reviewing Our Global Signals Intelligence Collection and Communications Technologies* (Aug. 12, 2013), <https://obamawhitehouse.archives.gov/the-press-office/2013/08/12/presidential-memorandum-reviewing-our-global-signals-intelligence-collec>.

²⁴⁸ (U) See Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs, Hearing before the Committee on the Judiciary, S. Hrg. 113-334 (2013), <https://www.intelligence.gov/ic-on-the-record-database/results/38-hearing-of-the-senate-judiciary-committee-on-strengthening-privacy-rights-and-national-security-oversight-of-fisa-foreign-intelligence-surveillance-act-surveillance-programs>.

²⁴⁹ (U) 50 U.S.C. § 1861(c)(2)(F)(i).

response to the initial specific selection term.²⁵⁰ In short, it authorized the government to obtain two hops of CDRs on an ongoing basis.

(U) The statutory framework also imposed boundaries on CDR collection. A notable limitation arose from the definition of “call detail record,” which the statute defined to exclude the contents of a communication, the name of a subscriber or customer, and cell-site location or global positioning system information.²⁵¹ The Board is aware of no instance in which NSA sought to circumvent this or any other statutory limitation related to the program.²⁵² For example, the Board is not aware of any instance in which NSA sought or obtained global positioning system information, cell-site location information, or the names of subscribers.

(U) The technical architecture created by NSA to collect CDRs under the USA Freedom Act was designed to comport with the statute.²⁵³ As described in Part II of this report, the system contained a series of safeguards; many could be mapped directly to the statutory limitations, while others were implemented for policy and compliance purposes. For example, when 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. The system was technically unable to ingest information not contained in the roughly fifty specified data fields.²⁵⁴

2. (U) Compliance Incidents and Data-Integrity Concerns

(U) Beginning in 2016, NSA identified a series of compliance and data-integrity concerns. These can be divided into two categories: those that could arise in other areas of FISA or equivalent law enforcement authorities, and those unique to the USA Freedom Act’s statutory framework.

(U) The incidents involving information omitted from a 2016 application to the FISA court,²⁵⁵ certain NSA officers’ missing required training,²⁵⁶ and a provider’s production of data

²⁵⁰ (U) 50 U.S.C. § 1861(c)(2)(F)(iv).

²⁵¹ (U) 50 U.S.C. § 1861(k)(3)(B). The statute also required the government to conduct this collection under approved minimization procedures, and to destroy information as required by those procedures. 50 U.S.C. § 1861(c)(2)(A), (F)(vii).

²⁵² (U) Other statutory requirements include that collection be based on a specific selection term, that the government have approved minimization procedures, and that it destroys information as required by those procedures. 50 U.S.C. § 1861(c)(2)(A), (F)(vii).

²⁵³ (U) *See* Part II(A) for an explanation of this architecture. *See also* NSA USA Freedom Act Transparency Report.

²⁵⁴ (U//FOUO) *See* NSA Final Answers to PCLOB Questions (Nov. 22, 2019).

²⁵⁵ (U) Part II(B)(1)(a).

²⁵⁶ (U) Part II(B)(1)(c).

beyond the end date of an order do not uniquely implicate CDRs or the fact that the USA Freedom Act provides a two-hop collection authority. Based on our review of the facts, the Board determined that these incidents were inadvertent, not willful, and that NSA handled each case seriously. Whether purposeful or incidental, such compliance incidents are not trivial. In each instance, the government notified the FISA court and took steps to remediate the issue, including by deleting the affected data.²⁵⁷

~~(TS//SI//NF)~~ Other incidents raise questions that are unique to the contours of the USA Freedom Act. Specifically, the incidents involving ██████████²⁵⁸ ██████████²⁵⁹ raise other statutory questions. In these incidents, NSA systems automatically pushed requests to providers that were based on data received by NSA in response to a prior request. These incidents present intricate questions about the application of statutory terms to the telephony infrastructure.²⁶⁰

~~(TS//SI//NF)~~ In the first set of CDR-specific incidents, NSA's system automatically requested a second hop of data based off ██████████, rather than the ultimate recipient of a call.²⁶¹ Note, however, that the statute does not actually use the colloquial term "hop." Rather, the relevant text of the statute permits a FISA court order issued under the Act to "provide that the Government may require the prompt production of a second set of call detail records using session-identifying information . . . identified by the specific selection term used" as the basis for the first request for CDRs.²⁶² The question is thus whether ██████████ is the type of information the government can use to "require the prompt production of a second set of call detail records"; that is, in statutory terms, whether ██████████ constitutes

²⁵⁷ (U) See Part II(B)(1).

²⁵⁸ (U) Part II(B)(2)(a).

²⁵⁹ (U) Part II(B)(2)(b).

²⁶⁰ (U) Adding an additional layer of complexity, the relevant provision of the statute is addressed not to the agency, but to the FISA court, specifying what an order issued under the CDR provision may and must contain. 50 U.S.C. § 1861(c)(2)(F) ("An order under this subsection . . . shall authorize the production on a daily basis of call detail records . . . [shall] provide that the Government may require the prompt production of a first set of call detail records . . . [shall] provide that the Government may require the prompt production of a second set of call detail records using session-identifying information . . . identified by the specific selection term use to produce [the first set of] call detail records[.]"). Those statutory terms are then incorporated by the court in the primary orders issued to the agency and secondary orders issued to providers. The Board is not aware of any FISA court opinions that address the compliance incidents discussed here and their implications for compliance with the statute or relevant court orders.

²⁶¹ (U) Re: Preliminary Notice of Compliance Incident Regarding Applications of the Federal Bureau of Investigation for Orders Requiring the Production of Call Detail Records, Various Docket Numbers (Nov. 22, 2017).

²⁶² (U) 50 U.S.C. § 1861(c)(2)(F)(iv).

“session-identifying information . . . identified by the specific selection term used to produce” the first set of CDRs.²⁶³

(U) Although the statute does not define “session-identifying information,” it does provide a non-exclusive list of examples, specifying that “call detail record” means, among other things, “session-identifying information (including an originating or terminating telephone number, an [IMSI] number, or an [IMEI] number).”²⁶⁴ The word “including” indicates that these enumerated examples are illustrative, not exclusive. Accordingly, “session-identifying information” might include other things too.²⁶⁵

~~(TS//SI//NF)~~ But what other things? Could [REDACTED] used to connect a call constitute “session-identifying information” under the statute? [REDACTED]

[REDACTED] Furthermore, the statute excludes from its examples of session-identifying information other information that is part of a CDR, specifically “a telephone calling card number, or the time or duration of a call.” On the other hand, reading the phrase “session-identifying” to encompass only information about the endpoints—one possible attribute of a session, but not the only one—would effectively transform “session-identifying” into “user-identifying” or “endpoint-identifying.” Without more specific language in the statute, it remains uncertain whether the use of [REDACTED] as “session-identifying information” would have been appropriate under the statute as the basis for a request for a second set of CDRs. Moreover, this statutory question must be considered alongside other textual features of the Act, including Congress’s prohibition on the bulk collection of metadata.

~~(TS//SI//NF)~~ In the end, however, the agency adopted a narrow reading of the statute and acted accordingly, ending the inadvertent [REDACTED] collection, deleting the records it produced, and notifying the FISA court.²⁶⁶

²⁶³ (U) 50 U.S.C. § 1861(c)(2)(F)(iv).

²⁶⁴ (U) 50 U.S.C. § 1861(k)(3). A FISA court opinion predating the USA Freedom Act similarly defined session-identifying information as including, “e.g., originating and terminating telephone number, communications device identifier, etc.” FISC Order No. 2007-10, at 2 (May 3, 2007).

²⁶⁵ (U) *See, e.g., Federal Land Bank of St. Paul v. Bismarck Lumber Co.*, 314 U.S. 95, 100 (1941) (“[T]he term ‘including’ is not one of all-embracing definition, but connotes simply an illustrative application of the general principle[.]”).

²⁶⁶ (U) Another intricacy here is that NSA was unaware of the underlying infirmities in the first-hop results when its system automatically pushed them out to providers as the basis for second-hop collection. Whatever the legal significance of this fact for purposes of assessing NSA’s compliance with court orders, NSA took prompt corrective action once it became aware of the problem. *See* Re: Supplemental Notice of Compliance Incident Regarding

~~(TS//SI//NF)~~ A second set of CDR-specific incidents, which involved [REDACTED] raises equally complex statutory questions. There, [REDACTED]²⁶⁷ According to its subsequent public press release, NSA stated that “[t]hese irregularities . . . resulted in the production . . . of some CDRs that NSA was not authorized to receive.”²⁶⁸ NSA deleted the data that it had acquired as a result of these issues, a fact the agency then disclosed publicly.²⁶⁹

~~(TS//SI//NF)~~ The government subsequently considered whether it could, in fact, lawfully request an additional production of CDRs [REDACTED] It concluded that it *could* obtain CDR records based on [REDACTED] reasoning that [REDACTED] are . . . valid session identifying information because [REDACTED] in contact with [REDACTED] are included [REDACTED]²⁷⁰ Out of an abundance of caution, however, the government also determined that NSA would not forward any such information to its corporate repositories.²⁷¹

~~(TS//SI//NF)~~ In statutory terms, this incident raises subtle questions about the precise terms of the statute. Could [REDACTED] be considered [REDACTED] that could then be used to “require the prompt production of a second set of call detail records”?²⁷² Could [REDACTED] because of its role in routing the call?²⁷³ The answers to these questions are murky, and we are aware of no on-point precedent interpreting the relevant terms. [REDACTED], out of an abundance of caution, NSA did not forward

Applications of the Federal Bureau of Investigation for Orders Requiring the Production of Call Detail Records, Various Docket Numbers (Mar. 19, 2018).

²⁶⁷ (U) Supplemental Notice of Compliance Incident Regarding Multiple Dockets In Re Applications of the Federal Bureau of Investigation for Orders Requiring the Production of Call Detail Records (CDRs) Pursuant to Title V of FISA, as amended by the USA FREEDOM Act (Mar. 4, 2019).

²⁶⁸ (U) NSA Press Release, *NSA Reports Data Deletion*, PA-010-18 (June 28, 2018).

²⁶⁹ (U) NSA Press Release, *NSA Reports Data Deletion*, PA-010-18 (June 28, 2018).

²⁷⁰ (U) Supplemental Notice of Compliance Incident Regarding Multiple Dockets In Re Applications of the Federal Bureau of Investigation for Orders Requiring the Production of Call Detail Records (CDRs) Pursuant to Title V of FISA, as amended by the USA FREEDOM Act (Mar. 4, 2019).

²⁷¹ (U) Supplemental Notice of Compliance Incident Regarding Multiple Dockets In Re Applications of the Federal Bureau of Investigation for Orders Requiring the Production of Call Detail Records (CDRs) Pursuant to Title V of FISA, as amended by the USA FREEDOM Act (Mar. 4, 2019).

²⁷² (U) 50 U.S.C. § 1861(k)(3), (c)(2)(F)(iv).

²⁷³ (U) 50 U.S.C. § 1861(k)(3).

information derived from these providers into its long-term repositories—even though the Department of Justice believed that it could.²⁷⁴

(U) Other data-integrity errors involved inaccurate data transmitted to NSA by providers. In one such incident, a provider overwrote certain CDR fields with unrelated data. If the inaccurate fields were used as the basis for subsequent collection, it would raise the question whether an automated request for second-hop results based on irrelevant data returned by a first-hop request would constitute a request based on “session-identifying information . . . identified by the specific selection term used” in the first-hop request.²⁷⁵ NSA responded by (1) notifying the FISA court to describe each of these data-integrity errors and (2) deleting all of the affected records.

~~(TS//SI//NF)~~ Given the decision not to use the information obtained in incidents involving [REDACTED], as well as the subsequent decision to suspend the program, the government never litigated to a conclusion complications surrounding these issues. The agency’s decisions to err on the side of caution meant that abstract questions about the application of statutory text to these esoteric compliance incidents were never resolved. At bottom, this analysis reveals an inherent indeterminacy in the statutory text, which incorporates terms (most notably, “session-identifying information”) whose precise meaning is hinted at but not conclusively defined. NSA resolved statutory uncertainties related to compliance incidents by proceeding cautiously, opting to rely on narrow interpretations rather than more expansive alternatives. Nevertheless, this experience counsels close attention to the range of potential meanings of statutory terms relating to technology by drafters, overseers, and agencies themselves. This is particularly important when an agency will be tasked with applying these terms to large-scale data collection involving complex technical infrastructure whose precise contours may not yet be known. Ultimately, these incidents serve mostly to illustrate the unanticipated complications that can arise even within a seemingly straightforward statutory framework.

²⁷⁴ (U) Supplemental Notice of Compliance Incident Regarding Multiple Dockets In Re Applications of the Federal Bureau of Investigation for Orders Requiring the Production of Call Detail Records (CDRs) Pursuant to Title V of FISA, as amended by the USA FREEDOM Act (Mar. 4, 2019).

²⁷⁵ (U) 50 U.S.C. § 1861(c)(2)(F)(iv).

V. (U) Analysis of Privacy Risks

(U) The government has suspended the USA Freedom Act CDR program and deleted the CDRs it collected under the program.²⁷⁶ As the statutory sunset approaches, however, Congress will consider whether to reauthorize or modify the CDR provision or allow it to expire. For that reason, we consider the privacy and civil liberties risks arising from the type and scale of two-hop CDR collection permitted by the statute and the role that various safeguards play in mitigating those risks.

A. (U) Scale and Sensitivity of the Data Collected

(U) Although this program did not collect CDRs in bulk, the volume of records ingested was large. According to the Office of the Director of National Intelligence’s 2018 Statistical Transparency Report, NSA received more than 151 million CDRs in 2016, 534 million in 2017, and 434 million in 2018.²⁷⁷ (These include “duplicate records” and “numbers used by business entities for marketing purposes.”²⁷⁸) In 2018, NSA collected records pertaining to more than 19 million unique phone numbers.²⁷⁹

(U) It is critical to remember that CDRs collected under the USA Freedom Act contained limited information. Under the statute, CDRs cannot include a call’s content, the name, address, or financial information of a subscriber or customer, or cell-site or geolocation information.²⁸⁰ Rather, acquired CDRs contained a set of fields including phone numbers, device-identifying numbers (*e.g.*, IMEI), subscriber-identifying numbers (*e.g.*, IMSI), a telephone calling card number, various routing and status information, and call time and duration.

~~(S//NF)~~ In theory, the connections documented by CDRs may reveal intimate information about an individual’s personal life. They could indicate sensitive personal facts (such as a specific health condition), relationships, occupation, age, or sex. However, as noted in Part II(A)(2), [REDACTED] Moreover, Tool 1—the metadata viewer that NSA analysts used to retrieve USA Freedom Act CDRs—had limited

²⁷⁶ (U) *See* National Security Agency, *NSA Reports Data Deletion*, Statement No. PA-010-18 (June 28, 2018), <https://www.nsa.gov/news-features/press-room/Article/1618691/nsa-reports-data-deletion/>; Letter from Daniel Coats, Director of National Intelligence, to Senators Richard Burr, Lindsey Graham, Mark Warner, and Dianne Feinstein (Aug. 14, 2019) (“The National Security Agency has suspended the call detail records program that uses [FISA Title V as amended by the USA Freedom Act] and deleted the call detail records acquired under this authority.”).

²⁷⁷ (U) 2018 Statistical Transparency Report at 30.

²⁷⁸ (U) 2018 Statistical Transparency Report at 28–30.

²⁷⁹ (U) 2018 Statistical Transparency Report at 30.

²⁸⁰ (U) 50 U.S.C. § 1861(k)(3)(B).

mechanisms for analysts to annotate CDRs, and there was no mechanism [REDACTED]

281

(U) Researchers have concluded that phone numbers can be combined with public data to reidentify individuals with “trivial” effort, and that it “appears feasible—with further refinement—to draw Facebook-quality relationship inferences from telephone metadata.”²⁸² The feasibility of doing so augments the potential risks and harms associated with unauthorized users and malicious actors who, if they had access to records, could de-anonymize CDRs or infer sensitive data about individuals in that manner. However, as noted below, the Board is aware of no instance in which USA Freedom Act CDR data was accessed by unauthorized or malicious actors, and accordingly is aware of no instance in which this risk materialized during the life of the program.

B. (U) Privacy Risks Arising from Two-Hop CDR Collection

(U) Unlike legal processes that allow the collection of one-hop CDRs (*e.g.*, grand jury subpoenas), the USA Freedom Act authorizes the collection of a second hop. A two-hop program on this scale raises various privacy risks. Some could arise in any program that involves the large-scale collection of sensitive data. Distinctive features of two-hop collection, however, could have unique effects on the makeup of the dataset exposed to those risks.

(U) Specifically, privacy risks that arise from any large-scale collection of sensitive datasets about Americans include the risk that authorized users could misuse their access to view, steal, or leak sensitive data for personal, ideological, or other inappropriate ends; the risk of theft or breach by unauthorized users or malicious outsiders; or the possibility that future shifts in applicable law, policy, or available technology could alter the balance between privacy risks and programmatic benefits.²⁸³ Limits on retention, technological controls, and the agency’s compliance culture play an important role in mitigating these risks, but cannot eliminate them. While these risks are not specific to the USA Freedom Act CDR program, the exponential increase in the scale of collection that results from adding a second hop expands significantly the pool of data exposed to them.

²⁸¹ (U) Of course, if an NSA analyst was using a particular CDR—for example, to write an intelligence report—he or she may have used information from that CDR to find other data lawfully in NSA’s possession. Together with the CDR, this could have revealed additional information about the originator or recipient of a call. Learning more about the associates of people suspected of involvement in terrorism is, of course, one of the important purposes for which NSA collects and analyzes this information in the first place.

²⁸² (U) Jonathan Mayer, Patrick Mutchler, & John C. Mitchell, *Evaluating the privacy properties of telephone metadata*, 113 PNAS 5536, 5538 (May 17, 2016), <https://www.pnas.org/content/pnas/113/20/5536.full.pdf>.

²⁸³ (U) For example, future statutory changes could expand the purposes for which NSA is permitted to use or share the information. Technological changes could also create unanticipated risks; improved analytical tools might allow, for example, the government to draw more sophisticated inferences from the data than is possible today.

(U) Two distinctive features of two-hop collection affect the type of records exposed to those risks. The first arises from the possibility of errors in first-hop results. In a two-hop program, errors in first-hop records, if not caught and corrected, could lead to the collection of a large number of second-hop records that should not have been collected. For example, if a technical error caused a first-hop record to include an incorrect phone number as the call recipient, all second-hop records associated with that number could be erroneously collected. In a one-hop program, a human agent or analyst would identify relevant first-hop results to use as the basis for seeking additional collection; this potentially lessens (although does not eliminate entirely) the risk of erroneous additional collection based on first hops.

(U) The second distinctive feature of two-hop collection is that the government is likely to receive far more second-hop records, which include information about individuals who are *indirectly* connected to the target, than first-hop records, which relate to the target and the target's *direct* contacts. The result is that in a two-hop program, any privacy risks arising from the collection disproportionately affect individuals with no direct connection to the individualized suspicion on which the surveillance rests.

(U) These two distinctive features of two-hop collection manifested themselves during the life of the CDR program. At several points, incorrect first-hop results returned by providers were automatically used as the basis for second-hop requests.²⁸⁴ (Once these incidents were discovered, NSA notified the FISA court and deleted the resulting data.) With respect to volume, 14 orders produced more than 400 million records in 2018, and NSA has acknowledged the exponential growth in the number of records that results from adding a second hop.²⁸⁵

(U) The Board is not aware of any instances in which the abuses described above as potentially arising from large-scale data collection—breaches, leaks, theft, and so forth—materialized during the short life of the CDR program. The Board has no information suggesting that CDRs were leaked, breached, or misused by anyone within the agency. NSA implemented technological and process controls, discussed below, to reduce the risk of loss or misuse of CDRs.

C. (U) Program Limits and Controls

(U) The program operated subject to statutory limits, internal controls, and oversight, both within NSA and outside the agency. By statute, NSA may only seek CDRs based on seed numbers relevant to an authorized investigation to protect against international terrorism.²⁸⁶ The

²⁸⁴ (U) See Part II(B)(2).

²⁸⁵ (U) 2018 Statistical Transparency Report at 28–30.

²⁸⁶ (U) 50 U.S.C. § 1861(b)(2)(C). This collection limitation aligns with the data-minimization principle of the Fair Information Practice Principles (FIPPs), which states that “organizations should only collect [personal information]

agency's minimization procedures, which were adopted by the Attorney General and approved by the FISA court, limit when and for what purpose analysts may access USA Freedom Act CDR data.²⁸⁷ Specifically, NSA may only grant access to personnel who are trained on the procedures and restrictions that govern the handling and dissemination of that data and who have a need to know.²⁸⁸ The procedures also prohibit NSA from retaining CDRs for more than five years after they were delivered to NSA unless the relevant CDR contained information that formed the basis for a foreign intelligence report.²⁸⁹

(U) Internal policies and guidance impose further limits.²⁹⁰ Queries could only be initiated when "intended to determine or identify persons of foreign intelligence interest who may be engaged in international terrorism," and were subject to audit.²⁹¹ These limits and controls played a role in mitigating the privacy risks posed by the program during its operation.

(U) Like other NSA activities, the USA Freedom Act CDR program was overseen by various elements within NSA. The Board's oversight, including demonstrations of NSA's compliance technology, indicates that the agency has made significant investments in internal compliance and accountability processes. For instance, NSA had measures in place to ensure that only the right people could see CDR program information on NSA's systems and that those people could use the information only for authorized purposes. Every query by an NSA analyst is logged and later reviewed by a human auditor familiar with the analyst's mission, and NSA has deployed technology to augment the capabilities of these human auditors. Software developers seek to build minimization and compliance rules into the design of the user interfaces that analysts use, reducing the need to rely on human recall and judgment to ensure

that is directly relevant and necessary to accomplish the specified purpose(s)" of the collection. The White House, *National Strategy for Trusted Identities in Cyberspace*, Appendix A (Apr. 2011), https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

²⁸⁷ (U) The statute and minimization procedures limited the purposes for which data could be used. This speaks to the FIPPs purpose-specification principle, which provides that entities should articulate the authority under which personal information is collected and the purposes for which it is intended to be used. The White House, *National Strategy for Trusted Identities in Cyberspace*, Appendix A (Apr. 2011).

²⁸⁸ (U) NSA USA Freedom Act Transparency Report at 6. These restrictions relate to the FIPPs principle of "use limitation," which provides that organizations should use personal data for the stated purposes and share it in ways that are compatible with such purposes," and the principle of "data quality," which states that steps should be taken to ensure that personal data is "accurate, relevant, timely, and complete." The White House, *National Strategy for Trusted Identities in Cyberspace*, Appendix A (Apr. 2011).

²⁸⁹ (U) NSA USA Freedom Act Transparency Report at 7.

²⁹⁰ (U) See Part II(A)(2).

²⁹¹ (U) NSA USA Freedom Act Transparency Report at 13. Query limits reinforce the FIPPs principle of use limitation. NSA's training, compliance, and auditing practices address the FIPPs principle of auditing. See The White House, *National Strategy for Trusted Identities in Cyberspace*, Appendix A (Apr. 2011).

compliance.²⁹² Automated checks now ensure that analysts whose training has lapsed lose access to systems for which the training is required.

D. (U) Transparency and Public Understanding

(U) Since the unauthorized disclosures by an NSA contractor in 2013, the intelligence community has taken important steps to enhance transparency, oversight, and compliance. Some of these steps were initiated by NSA; others were mandated by Congress in the USA Freedom Act and other laws.²⁹³

(U) As noted in Part I of the report, the CDR program was based on a publicly debated statute that clearly authorized the government to obtain records out to two hops from the target number on an ongoing basis.²⁹⁴

(U) The plain text of the USA Freedom Act enabled Members of Congress, the media, outside experts and advocacy groups, and ordinary Americans to anticipate the broad attributes of the CDR collection that it authorized, even if specific operational details would remain classified.

(U) Further, the CDR program was subject to ongoing oversight from all three branches of government. Outside NSA, these included the FISA court, congressional committees, and the Privacy and Civil Liberties Oversight Board. NSA and the Department of Justice notified the FISA court, Congress, and the Board of compliance incidents and data-integrity issues as they were discovered.²⁹⁵ NSA also issued several public disclosures about these issues over the life of the program and published a detailed, unclassified description of the program's technical architecture shortly after it began.²⁹⁶

(U) The government also provided quantitative data about its use of the CDR authority and the number of records NSA received. Each year, beginning in 2014, ODNI has released an Annual Statistical Transparency Report that provides detailed information about the volume of collection and the number of targets surveilled under various authorities, including the USA

²⁹² (U) *Cf.* NSA/CSS Inspector General, Declassified Report on the Special Study of NSA Controls to Comply with the FISA Amendments Act §§ 704 and 705(b) Targeting and Minimization Procedures, ST-15-0005, at 7–8 (Jan. 7, 2015) (citing reliance on “manual checks that analysts perform before querying data” as factor contributing to non-compliant queries).

²⁹³ (U) *See, e.g.*, USA Freedom Act, Pub. L. No. 114-123, 129 Stat. 268, §§ 401–02, 502, 601–05 (June 2, 2015).

²⁹⁴ (U) 50 U.S.C. § 1861(b)(2)(C), (c)(2)(F); *see also* H.R. Rep. 114-109, at 17 (May 8, 2015).

²⁹⁵ (U) External oversight was relevant to several principles: it enhanced the program's transparency, helped to ensure data quality, and made provided accountability. *See* The White House, *National Strategy for Trusted Identities in Cyberspace*, Appendix A (Apr. 2011).

²⁹⁶ (U) NSA USA Freedom Act Transparency Report.

Freedom Act. The data in these reports conveyed the CDR program's scale, both in absolute terms and relative to the number of orders issued by the FISA court.²⁹⁷ As noted above, for example, NSA collected 434,238,543 records based on 14 court orders in 2018. That report also disclosed for the first time the number of unique phone numbers contained within those records: more than 19 million.²⁹⁸ The reports have provided progressively greater detail about how NSA and other agencies conduct these counts and why they opt for certain approaches over others. The significant effort that NSA, the Office of the Director of National Intelligence, and other agencies invest in compiling and declassifying this information is an important investment in public understanding of these activities.

²⁹⁷ (U) These reports also discuss the number of queries that NSA analysts ran against the agency's holdings of USA Freedom Act CDRs. These counts were likely over inclusive, however, for reasons discussed elsewhere in this report. *See* 2018 Statistical Transparency Report at 31; *see also* Part III(B).

²⁹⁸ (U) 2018 Statistical Transparency Report at 30.

VI. (U) Statement of Chairman Adam Klein

(U) When the Board began to review NSA's collection of call detail records under the USA Freedom Act, the program was active. By the end of our review, NSA had publicly announced that it had suspended the program and decommissioned the equipment used to gather CDRs from the providers.

(U) This project thus differs from the Board's past reports in an important respect: The program it describes is no longer operational. Nonetheless, the short life of CDR collection under the USA Freedom Act offers lessons for crafting and implementing future surveillance authorities.

(U) I join the Board's report in full and am grateful to our staff for their hard work in preparing it. Our work has profited immeasurably from their diligence, expertise, and judgment.

I. (U) Balancing Security and Liberty

(U) As Congress recognized in the law that created our Board, "[t]he choice between security and liberty is a false choice Our history has shown us that insecurity threatens liberty. Yet, if our liberties are curtailed, we lose the values that we are struggling to defend."²⁹⁹ The USA Freedom Act, like other post-9/11 legislation, reflects a delicate balancing aimed at preserving those two indispensable goods.

(U) Counterterrorism programs that entail large-scale collection and retention of sensitive information about Americans should be initiated and preserved only if the value they provide outweighs the costs, including risks to privacy and civil liberties, and there is no better way to obtain the same value. Even where an authority provides great value, policymakers should take all reasonable steps to mitigate privacy and civil liberties risks.³⁰⁰

(U) This program did not involve bulk collection, but it took in large numbers of records. During 2017 and 2018, NSA collected nearly 1 billion call detail records under the USA

²⁹⁹ (U) 42 U.S.C. § 2000ee(b)(3) (quoting National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 395 (2004)).

³⁰⁰ (U) *See The 9/11 Commission Report* at 394–95 (“The burden of proof for retaining a particular governmental power should be on the executive, to explain (a) that the power actually materially enhances security, and (b) that there is adequate supervision of the executive’s use of the powers to ensure protection of civil liberties. If the power is granted, there must be adequate guidelines and oversight to properly confine its use.”).

Freedom Act.³⁰¹ (This includes an unknown number of duplicates.³⁰²) The scale of the collection is also proportionally large relative to the number of seed numbers associated with international terrorism. Last year, the government obtained 14 FISA court orders based on a “reasonable articulable suspicion” that a specific selection term was associated with international terrorism.³⁰³ Those 14 orders enabled the government to collect 434 million records pertaining to more than 19 million unique phone numbers.³⁰⁴ Given the exponential math of two-hop collection, it is reasonable to assume that most of these were second-hop contacts—callers two degrees of separation removed from the initial suspicious actor. Our report describes the privacy considerations that arise from domestic collection and storage of call detail records on this scale.

(U) On the other side of the balance is the operational need for this collection. International terrorism remains a dangerous threat. Al Qaeda, ISIS affiliates, and other international terrorist groups continue to menace the United States. Terrorists have capitalized on modern communications technologies, including social media and encrypted messaging, to identify, radicalize, and even direct from afar potential attackers in the US homeland.³⁰⁵

(U) Given terrorist groups’ reliance on digital communications, electronic surveillance will continue to play an indispensable role in protecting the nation from terrorism. This includes collection and analysis of communications metadata. The insightful discussion by Board Members Nitze and Bamzai illustrates how metadata analysis, including multi-hop contact-chaining, can “add significant intelligence value to national security investigations.”³⁰⁶ Indeed, metadata analysis may become even more important for counterterrorism as content is increasingly protected by strong, end-to-end encryption.

(U) The question is what role USA Freedom Act CDRs can play in that defense. The upcoming sunset of the Act’s CDR authority arrives against the backdrop of terrorist groups’ widely documented shift away from telephony to newer, more secure modes of communication. Researchers have observed that “[a]fter the Snowden leaks revealed how valuable terrorists’ unencrypted communications were for US counterterrorism efforts, terrorist groups swiftly

³⁰¹ (U) Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities, Calendar Year 2017*, at 35 (Apr. 2018) (534.3 million records); 2018 Statistical Transparency Report at 30 (434.2 million records).

³⁰² (U) See Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities, Calendar Year 2017*, at 35 (Apr. 2018) (“[T]he number reported above . . . includes duplicate records[.]”).

³⁰³ (U) 2018 Statistical Transparency Report at 30.

³⁰⁴ (U) 2018 Statistical Transparency Report at 30.

³⁰⁵ (U) See, e.g., Bipartisan Policy Center, *Digital Counterterrorism: Fighting Jihadists Online*, 5, 15 (May 2018).

³⁰⁶ (U) Statement of Aditya Bamzai and Jane Nitze, Part I.

tightened up their operational security.”³⁰⁷ Their shift to IP-based communications, including social media and encrypted chat apps, has not made telephony irrelevant to counterterrorism—people still use phones—but, as academic researchers have noted, it has become less central.³⁰⁸ “We are dealing with a challenge right now: New technologies that enable encryption and allow them to be fairly confident that they are communicating in a way that can’t be detected,” one US official told the news organization ProPublica in 2016.³⁰⁹ “They know how to communicate securely.”³¹⁰

(U) This shift suggests that focusing on the full spectrum of digital communications technologies, rather than voice telephony in isolation, would likely yield greatest counterterrorism value going forward. Whether the complexities that led to compliance and data-integrity problems during the life of this program are likely to persist into the future depends on predictive judgments about the future of telephony networks and company billing practices, as well as the possibility that the government could develop technical approaches to mitigate these complexities. The technical experts at NSA and outside technologists familiar with the intricacies of telephony networks would be best positioned to render those predictive judgments. Given the persistence of terrorist threats to the homeland, Congress may wish to ask agencies whether they need alternative tools to meet the operational need that the USA Freedom Act and the prior bulk CDR program were designed to address.

(U) It is also important to note that USA Freedom Act CDRs were only one of several avenues by which NSA and FBI can obtain and analyze communications metadata for counterterrorism purposes. NSA collects phone metadata and electronic communications metadata as part of its global signals-intelligence mission carried out under Executive Order 12333. This metadata, stored in an internal repository, can be used to protect the homeland from international terrorism: NSA’s Supplemental Procedures Governing Communications Metadata Analysis allow “identifiers associated with both non-US persons and US persons to be used to query phone metadata and electronic communications metadata that NSA obtains through other lawful collection methods.”³¹¹ NSA can also collect communications metadata under Section

³⁰⁷ (U) Bipartisan Policy Center, *Digital Counterterrorism: Fighting Jihadists Online*, 15 (May 2018).

³⁰⁸ (U) Susan Landau and Asaf Lubin, *Explaining the Anomalies, Examining the Value: Should the USA Freedom Act’s Metadata Program be Extended?*, at 62 (2019).

³⁰⁹ (U) Sebastian Rotella, *ISIS via WhatsApp: “Blow Yourself Up, O Lion,”* ProPublica (July 11, 2016).

³¹⁰ (U) Sebastian Rotella, *ISIS via WhatsApp: “Blow Yourself Up, O Lion,”* ProPublica (July 11, 2016).

³¹¹ (U) Part II(A)(1).

702 of FISA, and FISC-approved procedures permit NSA to run US-person queries of 702 data if those queries are “reasonably likely to retrieve foreign intelligence information.”³¹²

(U) FBI receives a small subset of NSA’s 702 collection and can query that data in search of foreign-intelligence information or evidence of a crime.³¹³ Ordinary FISA business records requests can be used to obtain one hop of CDRs and metadata from other modes of digital communication. Given that terrorism-related conduct is often a crime, FBI can also use grand-jury subpoenas, which are less burdensome to obtain than FISA orders, to obtain first-hop CDRs in terrorism cases.

(U) NSA is well-positioned to assess which of its various capabilities provide the greatest operational value. It chose to suspend this program “after balancing the program’s relative intelligence value, associated costs, and compliance and data integrity concerns.”³¹⁴ Facts detailed earlier in this Report support that conclusion, even independent of the privacy concerns raised by domestic collection on this scale. The low volume of intelligence reporting produced by the program—15 reports over several years—is particularly informative, especially when coupled with NSA’s assessment that it would expect a program of this scale and expense to generate hundreds or thousands.³¹⁵

(U) That candor is creditable. It is not easy for any government agency to acknowledge that a program was not successful, despite the resources and effort it consumed. Agencies should be encouraged to periodically reassess their collection activities and terminate them when they outlive their usefulness or when their costs outweigh their value, with privacy and civil liberties considerations forming an integral part of that analysis. Scrutiny of intelligence programs is an essential corrective in our democratic system. However, outside observers should be careful to distinguish between abuse or overreach—neither of which we found here—and programs that, despite good faith efforts, yield less than anticipated. Intelligence is a complex enterprise in which uncertainty is pervasive. It is not always clear in advance whether or not a program will yield benefits commensurate with its costs and risks. If agencies feel compelled to defend rather than abandon unproductive programs, the principal casualty will be the privacy of those Americans whose data continues to be collected.

³¹² (U) Declassified 2018 NSA Querying Procedures for Section 702, § IV.A.

³¹³ (U) Christopher Wray, Director, Federal Bureau of Investigation, Speech on Section 702 at the Heritage Foundation (Oct. 13, 2017) (FBI receives only on targets for which it has “full national security investigations,” amounting to “about 4.3 percent of the targets that are under NSA collection[.]”); Declassified 2018 FBI Querying Procedures for Section 702, § IV.A.1.

³¹⁴ (U) Unclassified Letter from Director of National Intelligence Dan Coats to Senators Richard Burr, Lindsey Graham, Mark Warner, and Dianne Feinstein, at 1 (Aug. 14, 2019).

³¹⁵ (U) *See* Part III(B).

II. (U) Root Causes of the Compliance Incidents and Data-Integrity Challenges

(U) The Board reviewed in detail each compliance incident or data-integrity problem reported during the program's life. We found no malfeasance or intentional abuse by NSA personnel in implementing this program. Nor did we find any instance in which the agency intentionally sought to obtain information that it may not have been authorized to receive. NSA personnel worked diligently to diagnose, report, and repair the problems encountered during the program's operation and to delete erroneously provided information once it was discovered.

(U) The compliance incidents arose, with limited exception,³¹⁶ from issues that were latent in the records NSA received from the providers. Phone companies' billing systems are understandably designed to meet their own business needs. By contrast, NSA's mission of extracting reliable intelligence from these CDRs while complying with statutory restrictions, court orders, and other legal obligations required a high level of precision and certainty about the attributes of the data.

(U) While we found no intentional attempts to collect more data than authorized, *unintentional* over-collection, triggered by anomalies in the first-hop data returned by providers, proved a recurrent problem. The program involved a complex, machine-to-machine technical architecture, with limited human intervention once initial, court-approved selection terms entered the system. One side effect was that errors in the data could "cascade[] across large numbers of records, with lagging human awareness."³¹⁷ In other words, the system, by design, automatically pulled in second-hop records before a human could evaluate the first-hop results. With ordinary requests for one hop of CDRs, by contrast, a human FBI agent or analyst would review the initial results. Before using any first-hop results to seek additional, second-hop records, that agent or analyst would work to distinguish meaningful connections from irrelevant or erroneous data, including by using information acquired under other legal authorities.

(U) By all accounts, NSA technical and analytical personnel demonstrated diligence and considerable ingenuity in uncovering, diagnosing, and working to repair each problem as it arose. NSA also built checks into the system in an attempt to prevent collection errors before they occurred, and updated those checks as new problems were discovered.³¹⁸ The fact that irregularities continued despite these exertions reflects the unique technical and compliance challenges that attended this program.

³¹⁶ (U) See Part II(B).

³¹⁷ (U) Julian Sanchez, Senior Fellow, Cato Institute, Remarks at Privacy and Civil Liberties Oversight Board Public Forum on the USA Freedom Act (May 31, 2019).

³¹⁸ (U) See Part II(A).

(U) The lesson here is not that Congress should prescribe the precise technical mechanisms by which surveillance authorities may be implemented, or that automated, iterative mechanisms will never be appropriate. To the contrary: In some cases, they may be the only choice, particularly as the expanding volume of data makes constant human oversight of every technical process less feasible. What's more, automated mechanisms may be more privacy-protective in some respects, by keeping human eyes off of the data and removing human bias and temptation as a point of failure.

(U) The point, rather, is that a program may present qualitatively different implications for privacy, civil liberties, and compliance if implemented using an automated, machine-to-machine architecture with limited human intervention, than if it relies on human-to-human fulfillment of one-off requests. The remedy is not prescriptive technical specifications, but to remain aware of the potential implications of program architecture as outside bodies conduct oversight and the agency itself structures its compliance and audit mechanisms.

III. (U) The Role of Statutes in Regulating Domestic Surveillance

(U) I agree with much of the insightful statement penned by Board Members Nitze and Bamzai. I take a somewhat more sanguine view, however, of two topics they address: the ability of Congress to constructively regulate in the area of domestic surveillance, and the utility of specifying particular technologies in statutory text.

(U) Since 1978, Congress has created a comprehensive statutory architecture to govern domestic surveillance for national-security purposes. That system, which began with FISA and which Congress has continued to expand and diversify since then,³¹⁹ has helped protect privacy and civil liberties. But it has also been good for the agencies themselves. Codification places domestic surveillance practices on a publicly enacted legal foundation, empowering agencies to act with the confidence that comes from explicit authority conferred by the people's representatives. The contrast between the reaction to the 2013 leaks that revealed the bulk call-records program, which rested on a secretly approved legal interpretation, and the reaction to this program, which rested on clear, publicly debated, publicly enacted statutory authority, is illustrative.

(U) Of course, the risk that statutes will produce unintended consequences is ever present, in intelligence statutes as in any other, and calls for careful drafting. I share my colleagues' view that the accidental, unavoidable compliance errors that can occur in any large

³¹⁹ (U) *See, e.g.*, Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458; Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53; FISA Amendments Act of 2008, Pub. L. No. 110-261; USA Freedom Act of 2015, Pub. L. No. 114-23; FISA Amendments Reauthorization of 2017, Pub. L. No. 115-118 (2018).

enterprise, private or public, should not by overly granular codification be transformed into statutory violations, triggering disproportionate consequences and undesirable risk-aversion.

(U) In my view, however, FISA generally achieves the right balance in this regard by requiring agencies to create minimization, targeting, and querying rules, requiring the FISA court to review them, and requiring the intelligence community to declassify them as far as possible.³²⁰ Congress has not sought to supply this intricate web of permissions and prohibitions by statute, but instead opted to mandate that they exist and provide mechanisms to verify their adequacy.

(U) Finally, we should remember that the possibility of unintended consequences runs both ways: it arises equally when Congress declines to act, allowing agencies to develop domestic surveillance programs without explicit statutory authority or boundaries. To legislate, or merely to oversee: there is no universally right choice.

(U) My colleagues also consider the disadvantages created by the USA Freedom Act's limitation of two-hop collection to *telephone* metadata, rather than other, newer technologies. Technology-neutrality, is, of course, often well-advised in crafting statutes in this era of rapid technological change. I agree with my colleagues on that. Yet I see the implications somewhat differently, both with respect to this statute and the principle of technology neutrality more generally.

(U) First, it is true, as my colleagues note, that by tying the USA Freedom Act's two-hop authority to telephone metadata, Congress "limited the statute's usefulness."³²¹ But we should also remember why it did that. It is not because Congress was unaware of the benefits of technology-neutral authorities: witness Section 702, a technology-neutral collection authority that has proved "highly valuable."³²² FISA's business-records provision, which is also up for reauthorization this March, provides technology-neutral authority to collect one hop of metadata. The government reports that that provision is very useful, precisely because it embraces the latest communication technologies.³²³ Rather, Congress limited two-hop collection in the USA

³²⁰ (U) *See, e.g.*, 50 U.S.C. § 1881a(e) (requirement to adopt, submit for judicial review, declassify, and publish minimization procedures for Section 702).

³²¹ (U) Statement of Aditya Bamzai and Jane Nitze, Part II.

³²² (U) *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 104–10 (2014) ("Since 2008, the number of signals intelligence reports based in whole or in part on Section 702 has increased exponentially," and 702 is "highly valuable" for other foreign-intelligence purposes.').

³²³ ~~(S//NF)~~ FBI briefing to the Board (Mar. 12, 2019). Specifically, the Bureau told the Board [REDACTED] of the 56 business records requests in 2018 sought electronic communications transaction records, or ECTRs, which FBI described to the Board as arguably the most valuable use of this authority.

Freedom Act to telephone metadata because the law was designed to achieve a very specific end: providing a narrower replacement for the previous bulk CDR program.³²⁴

(U) Second, while I agree that, when crafting surveillance laws, technology-neutrality should be the default, there are times when it will make sense for a law to pick out particular technologies. The churn of technological innovation will inevitably spit out new modes of communication and other technologies whose privacy implications we cannot presently foresee. For that reason, it may be rational for Congress to specify that an authority permits use of a known, present-day technology, while excluding emerging or yet-unknown technologies that may prove more invasive.

(U) Consider a hypothetical technology-neutral statute authorizing an agency to employ “biometric analysis.” Congress might reasonably prefer to allow an agency to use fingerprinting, and perhaps some forms of facial recognition, while excluding “rapid DNA identification devices, which are making positive identifications possible in as little as 90 minutes,” or other intrusive biometric checks yet unimagined.³²⁵ Or legislators might choose to permit facial recognition where photos are taken at a clearly identified checkpoint in a secure area, but to prohibit it where images are taken in public, or by stealth.

(U) The point is that enacting a technology-specific statute is not always a blunder. Rather, where consciously chosen, technology-specificity may reflect a considered judgment to rule out applications that would transform the authority at issue into something more intrusive than Congress intended. The USA Freedom Act supplies a real-world example: Congress approved two-hop CDR collection, but specifically barred the government from collecting “the contents . . . of any communication,” “the name, address, or financial information of a subscriber or customer,” and “cell site location or global positioning system information,” presumably based on its view that these types of data would be qualitatively more revealing than other data that CDRs ordinarily contain.³²⁶

(U) Indeed, technology-specific legislation, with its effect of anchoring levels of intrusion in the present, may become more common as technology races forward. Avulsive technological change seems to arrive every few years: the internet, IP-based messaging, social media, smartphones, biometrics, big data, the internet of things, and AI, each galloping past with

³²⁴ (U) See H.R. Rep. No. 114-109 (2015), at 17 (USA Freedom Act’s CDR provision “relies on” previous reforms to bulk metadata collection “to establish a new, narrowly-tailored mechanism for the targeted collection of telephone metadata . . . as part of an authorized investigation to protect against international terrorism. This new mechanism is the only circumstance in which Congress contemplates the prospective, ongoing use of Section 501 of FISA in this manner.”).

³²⁵ (U) International Biometrics & Identity Association, *Biometrics & Identify: DNA Biometrics* (visited Oct. 18, 2019), <https://ibia.org/biometrics-and-identity/biometric-technologies/dna>.

³²⁶ (U) 50 U.S.C. § 1861(k)(3).

irresistible momentum, with quantum computing and more on the horizon. Congress may choose to legislate more frequently to ensure that, as new technologies emerge, the statutory dispensation continues to balance security and liberty in the manner it intends.

VII. (U) Statement of Board Members Ed Felten and Travis LeBlanc³²⁷

(U) We appreciate the tireless work of the PCLOB staff, the thoughtfulness of our colleagues, and the unyielding dedication of the men and women of the national security establishment who every day commit themselves to protecting our great country. The threat of terrorism—both domestic and foreign—is very real and has taken a long toll on our nation’s history. It is in this context that the Board conducts oversight of the USA FREEDOM Act CDR program, mindful of our mission to balance privacy and civil liberties with national security. Together, we join the Board in issuing this Report to enhance transparency and public understanding of this discontinued program.

(U) We write separately to stress our view that the USA FREEDOM Act CDR program should remain shuttered and the program should not be reauthorized. We reach this conclusion for three reasons. First, the program produced minimal national security value. Second, the program’s expense is disproportionate to its value. And third, the program intruded on the privacy and civil liberties of millions of Americans who were not subjects of individualized suspicion. On balance, the privacy and civil liberties impacts, combined with the program’s costs, outweighed the program’s national security value. Also, we do not join the Board’s constitutional analysis for the reasons stated below. Finally, we disagree with suggestions that the same program with data from different media would solve the problems experienced with the USA FREEDOM Act CDR program.

I. (U) The value of the CDR program was not worth the risks and cost.

(U) In August 2019, following three years of operation of the USA FREEDOM Act CDR program, the Director of National Intelligence acknowledged in a letter to select Members of Congress that

[NSA] has suspended the [USA FREEDOM Act] call detail records program . . . and deleted the call detail records acquired under this authority. This decision was made after balancing the program’s relative intelligence value, associated costs, and compliance and data integrity concerns caused by the unique

³²⁷ (U) Statement from Travis LeBlanc: While I do join the Board in issuing this document to provide transparency about the facts and history of the program so that Congress and the public may scrutinize its value, I respectfully decline to adopt the document’s conclusions beyond transparency about the USA FREEDOM Act CDR program. Statement from Ed Felten: I join the Board’s report in full, except that I disagree with the constitutional analysis, for the reasons discussed in this statement.

complexities of using these company-generated business records for intelligence purposes.³²⁸

(U) The program remains dormant today. Over the three years this program was operational, it cost over \$100 million.

(U) As discussed in detail in the Report, since implementing the revised CDR program, NSA encountered multiple data integrity and compliance problems. While NSA expended considerable effort to diagnose and remediate the problems as they arose and mitigate the likelihood of recurrence, the errors nevertheless recurred. To NSA's credit, in response to "technical irregularities in some data received from telecommunications service providers[.]" NSA ultimately concluded that "it was not feasible to identify and isolate properly produced data"³²⁹ from improperly produced data so it deleted data collected under the program.³³⁰

(U) There is no indication that the conditions that led to the compliance errors are likely to change. If the program were reauthorized and restarted, it is hard to see what NSA could do to avoid further data integrity problems and accesses to data beyond the boundaries envisioned by the statute.

(U) Further, advancements in communications technology have already reduced the potential value of the CDR program. Independent experts³³¹ and academics³³² have argued that telephony data is of decreased value given the shift to different communications protocols, such as encrypted messaging. Both NSA³³³ and FBI³³⁴ agree that communications patterns and platforms have changed and that the current environment is unlike what it was years ago. These communication platforms and technologies will continue to change and develop. And, as

³²⁸ (U) Letter from Director of National Intelligence, Dan Coats, to Senators Richard Burr, Lindsey Graham, Mark Warner, and Dianne Feinstein (Aug. 14, 2019) (expressing support for reauthorization of sunset provisions of the USA FREEDOM Act).

³²⁹ (U) NSA Press Release, *NSA Reports Data Deletion*, PA-010-18 (June 28, 2018).

³³⁰ (U) A very small number of records were retained because they were referenced in disseminated reports.

³³¹ (U) *See, e.g.*, Privacy and Civil Liberties Oversight Board, Transcript of Public Forum to Examine the USA Freedom Act, Telephone Records Program (May 31, 2019) (statement of Mr. Michael Bahar), <http://pclob.gov> ("[I]t's fair to say the terrorists know as much as you can to stay off your phones. Or if you stay on your phone . . . start transitioning to encrypted communication . . . And if you've got everything, you've got nothing.").

³³² (U) *See, e.g.*, Privacy and Civil Liberties Oversight Board, Transcript of Public Forum to Examine the USA Freedom Act, Telephone Records Program (May 31, 2019) (statement of Professor Susan Landau), <http://pclob.gov> ("There are a number of changes that have happened since the summer of 2001. Technically and socially in the way we communicate, in the way terrorists communicate.").

³³³ (U) NSA briefing to the Board (May 23, 2019).

³³⁴ (U) FBI briefing to the Board (June 19, 2019).

counterterrorism targets increasingly rely upon non-phone communications modalities,³³⁵ the utility of phone metadata analysis in counterterrorism will continue to decrease.

II. (U) We cannot join the Board's constitutional analysis.

(U) The majority devotes over a dozen pages of the report to a constitutional analysis of the USA FREEDOM Act CDR program. We respectfully part ways with our colleagues in two ways.

(U) First, we question whether a constitutional analysis of the CDR program was prudent. While we can contemplate a circumstance where assessment of the constitutionality of a program would be helpful and informative, given our Board's limited time and resources, we question the utility of a constitutional analysis of this particular program. The USA FREEDOM Act CDR program has been suspended. Its existence and primary contours were publicly known and debated, and it was subject to oversight by the Foreign Intelligence Surveillance Court. However, in light of the constitutional analysis provided by our colleagues we address our thoughts below.

(U) Second, the majority does not go as far as we would have gone in discussing a full picture of complex and evolving constitutional law. As the courts are continuing to grapple with how to apply the Fourth Amendment to new technologies, and especially to records held by communications providers, we would have preferred a discussion of this challenging area of law, rather than a conclusion of constitutionality resting on a formalistic application of case law that the Board declined to endorse in its 2014 report. Further, the majority's constitutional assessment is silent on the First Amendment implications of the USA FREEDOM Act program. Assuming *arguendo* that "reasonableness" is the appropriate Fourth Amendment standard for evaluating any resumption of the USA FREEDOM Act CDR program, we would have instead assessed not the reasonableness of the program at its inception, but whether a resumption of the program as we know it now would be constitutional. Because the point of a Fourth Amendment reasonableness analysis is to weigh privacy intrusions on individuals against government national security and law enforcement interests, we would have preferred a forward-

³³⁵ (U) Privacy and Civil Liberties Oversight Board, Transcript of Public Forum to Examine the USA Freedom Act, Telephone Records Program (May 31, 2019) (statement of Professor Susan Landau) ("[C]ommunication is not happening over the telephone network. . . . When I look at the question of records, what I see is a change in communication modality."), <https://www.pclob.gov/reports/report-public-forum>; Privacy and Civil Liberties Oversight Board, Transcript of Public Forum to Examine the USA Freedom Act, Telephone Records Program (May 31, 2019) (statement of Mr. Michael Bahar) ("[I]t's fair to say the terrorists know as much as you can to stay off your phones. Or if you stay on your phone . . . start transitioning to encrypted communication[.]") <https://www.pclob.gov/reports/report-public-forum>.

looking analysis that factored in the now-known minimal national security value of the program balanced against its privacy impacts.³³⁶

A. (U) Whether the Board should conduct a constitutional analysis of the CDR program.

(U) The Board has a statutory responsibility to provide independent oversight of government activities that involve more personnel than the Board employs and greater resources than the Board possesses. It is essential that the Board exercise careful discretion in both its selection of matters to review and in how it conducts its reviews. In much the same way that courts practice judicial economy, we recommend that the Board responsibly adhere to a similar principle of oversight economy. We should prioritize providing constitutional and legal analysis where the Board has an institutional comparative advantage that will inform the Executive Branch, Congress, courts, and the American people. In contrast to the circumstances surrounding the Board's constitutional analysis of the 215 bulk records program, for the reasons noted above, we would have focused the Board's time and resources elsewhere.

B. (U) The majority's constitutional analysis of the CDR program does not go far enough.

(U) A conclusion that a now defunct program was constitutional at its inception is not as helpful as a discussion about whether the current landscape of facts and jurisprudence would find it so. Accordingly, we would ask not whether Congress acted appropriately when it passed the USA FREEDOM Act CDR provision, but rather whether an extension of that authority would be constitutional in light of the facts and circumstances known today.³³⁷ This, we believe, would be

³³⁶ (U) We also do not support the majority's reliance on a "foreign intelligence" exception to the Fourth Amendment warrant requirement in its analysis. It is our understanding that the Supreme Court has left open the question of whether there is a "foreign intelligence exception" to the Fourth Amendment. We are mindful to exercise caution in expanding any special needs exception to the Fourth Amendment. Such a malleable exception is at risk of not only expanding the Fourth Amendment beyond the expectations of the Founding Fathers, but also of expanding it beyond the literal text of the Amendment. Such an expansion risks sweeping into its ambit numerous activities solely because they are un-favored today. Thus, we tread cautiously and inspired by the wisdom of Justice Marshall, who wrote in *Skinner v. Railway Labor Executives' Association*, "There is no drug exception to the Constitution, any more than there is a communism exception or an exception for other real or imagined sources of domestic unrest. [A]bandoning the explicit protections of the Fourth Amendment seriously imperils 'the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.'" *Skinner v. Railway Labor Executives' Ass'n.*, 489 U.S. 604, 641 (1989) (Marshall, J., dissenting) (citation omitted) (quoting *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)). Accordingly, we are also reluctant here to assert that the "special needs" exception to the Fourth Amendment may apply.

³³⁷ (U) We are taking the *ex ante* position that Congress must now contend with a different landscape of known facts and circumstances than those which advised its decision in 2015. That altered landscape includes new facts about the value of the program and difficulties operating it, new Supreme Court jurisprudence, and a new understanding of both the privacy intrusions fostered by this program as well as the government interest furthered by the program.

most helpful to Congress and the public as they consider what to do with the program in the future. To be clear, we do not reach a conclusion here. We do, however, raise points that we believe should be considered by Congress. We conclude that there are considerable distinctions between precedent on which our colleagues rely and the reasonable expectations of privacy in a modern world.

(U) The crux of the majority's position is this: In *Smith v. Maryland*, the Supreme Court held that law enforcement collection of certain types of call records is not a "search" under the Fourth Amendment. The USA FREEDOM Act CDR program involved the collection of call records. *Ipso facto*, the CDR program is not a search or seizure under the Fourth Amendment.

(U) In 2014, however, the Board expressed doubts about whether that legal argument was right as applied to bulk collection of call detail records. In its prior report, the Board explained that basic argument, and then discussed factual, policy, and legal reasons why *Smith* and the "third-party doctrine" may not have been a sufficient constitutional basis for the bulk CDR program. Importantly, the 2014 report did not reach a conclusion on the constitutionality of the bulk program. Instead, the Board provided an accurate and evenhanded perspective: it indicated that the government's reliance on *Smith* was a reasonable legal position, that courts had reached differing conclusions about that position, and that the law in this area is challenging, rapidly changing, and difficult to predict.³³⁸ We believe the Board's assessment from 2014 remains spot-on, and subsequent legal developments like *Riley v. California* and *Carpenter v. United States* lend further support to that perspective.

(U) We take issue with the majority's characterization that the 2014 Board was "unanimous" in finding the pre-2015 bulk telephony program constitutional—notwithstanding the factual differences between that program and *Smith*. As the Board wrote in 2014: "it is possible that the contemporary Supreme Court—if called upon to evaluate [the bulk collection telephony CDR program] under the Fourth Amendment—would not consider *Smith v. Maryland* to have resolved the question." And in congressional testimony just weeks after the 2014 report was released, our then-Chairman David Medine explained: "The Board also believes that the NSA's bulk telephone records program raises concerns under both the First and Fourth Amendments to the United States Constitution. Our report explores those concerns, explaining that while government officials are entitled to rely on existing Supreme Court doctrine in formulating policy, the existing doctrine does not fully answer whether the Section 215 program is

Knowing what we know now, we have serious doubts going forward about whether the USA FREEDOM Act CDR program is reasonable under the Fourth Amendment.

³³⁸ (U) 2014 Board Report at 11, 103–27.

constitutionally sound.”³³⁹ As the majority points out, the Board also noted in its 2014 report the following: “Until the Supreme Court rules otherwise, *Smith v. Maryland* and the third-party doctrine remain in force today. Government lawyers are entitled to rely on them when appraising the constitutionality of a given action.”³⁴⁰ Were we serving on the Board in 2014, we would have entirely agreed, as we do now. To us, however, both can be true: the Board’s analysis of the constitutionality of the 215 bulk program raised questions about the constitutionality of the program under both the First and Fourth Amendments, but notwithstanding those concerns, the government was entitled to rely on the law as it stood at the time to govern the contours of its intelligence program. We would reach the same conclusion about the USA FREEDOM Act CDR program now.

(U) Because *Smith* and the third-party doctrine are so central to Fourth Amendment analysis of the USA FREEDOM Act CDR program, we briefly outline some of the Board’s 2014 concerns and discuss how subsequent legal and technical developments reinforce those concerns in the context of the CDR program as we know it now. We do not endeavor to rehash the Board’s 2014 report, and we encourage the public to read this report in tandem with the 2014 report.

(U) In the 2014 report, the Board outlined key factual differences between the bulk telephony CDR program under Section 215 of the USA PATRIOT Act and the *Smith* case.³⁴¹ For example, the Board noted that the bulk telephony CDR program gathered significantly more information about each telephone call and about far more people than did the pen register in *Smith*. In *Smith*, the police collected the numbers the defendant dialed after the pen register was installed, but did not collect information about the duration of the defendant’s calls or whether the calls were completed, nor about calls made previously by the defendant. Nor did the police in *Smith* collect information about incoming calls to the defendant’s telephone line. Further, *Smith* involved a short duration of use of a pen register (no more than 2 days) and the dialing information of just one person. Finally, in 1979, there was no ability to aggregate dialing records with those of other individuals and gain additional insight from that analysis.³⁴²

(U) We will have to agree to disagree with our colleagues on the significance of the ways in which the USA FREEDOM Act CDR program differs from the underlying facts in *Smith*. It

³³⁹ (U) Recommendations to Reform Foreign Intelligence Programs: Hearing Before the H. Comm. On the Judiciary, 113th Cong. 9 (2014) (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board), https://www.pclob.gov/library/Medine-Testimony-20140204-House_Judiciary_Comm.pdf.

³⁴⁰ (U) 2014 Board Report at 126.

³⁴¹ (U) We do not repeat the Board’s full analysis here. For a full analysis, see the 2014 Board Report at 111–12. For a more detailed discussion of the underlying facts in *Smith v. Maryland*, see the 2014 Board Report at 111–14.

³⁴² (U) See 2014 Board Report at 126.

is our view that those differences are more significant than the majority believes them to be and that nothing in the intervening five years has undercut them.³⁴³ If anything, recent research has put the Board's concerns from 2014 on an even more solid factual foundation: there is a significant privacy impact associated with large-scale telephone record collection.³⁴⁴

(U) We do not dispute that *Smith* remains good law. Nor do we dispute that the government has a reasonable legal argument, grounded in *Smith*, for why the shuttered USA FREEDOM Act CDR program was consistent with the Fourth Amendment at its inception. But, just like the Board in 2014, we are not prepared to endorse that argument given what we believe to be the serious factual differences from *Smith*. In short, we question whether a court considering the specific facts of the USA FREEDOM Act CDR program would find them similar enough to the underlying facts of the primitive "pen register" in *Smith* to extend that forty-year-old precedent to cover the USA FREEDOM Act CDR program. We believe that the majority places much greater weight on *Smith* than is warranted.³⁴⁵

(U) There are additional facts about the USA FREEDOM Act CDR program that remain classified, and that bolster our view that *Smith* may not be as dispositive as suggested by the majority.

(U) In *Smith*, the police collected a list of called numbers. In the CDR program, a record can be returned if a selection term matches the record's originating number, dialed number, terminating number, billing number, IMSI (unique identifier for a phone subscriber), IMEI (unique identifier for a phone handset), equipment serial number, or calling card number. In addition, the CDR program collected about 50 data fields for each call, including information about the caller, callee, their phone carriers, and various routing and status information.³⁴⁶ The information collected appears consistent with the statute, but it goes well beyond what the court

³⁴³ (U) Moreover, a recognition that the Supreme Court's opinion in *Carpenter* and *Riley* should be fairly considered alongside *Smith* is a reasonable assessment of the state of constitutional precedent. The majority appears to have embraced the dissenting view in *Carpenter* of the third-party doctrine that such a recognition would "destabilize criminal and national-security [sic] investigations across the United States." See Part IV(A)(2); see also *Carpenter v. United States*, 138 S. Ct. 2206, 2223, 2233–35 (2018) (Kennedy, J., dissenting). However, in *Carpenter*, the majority of the Supreme Court embraced the same caution we urge today: As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future." *Carpenter*, 138 S. Ct. at 2220 (quoting *Northwest Airlines, Inc. v. Minnesota*, 322 U.S. 292, 300 (1944)).

³⁴⁴ (U) Jonathan Mayer, Patrick Mutchler, & John C. Mitchell, *Evaluating the privacy properties of telephone metadata*, 113 PNAS 5536, 5538 (May 17, 2016) (finding "that telephone metadata is densely interconnected, can trivially be reidentified, enable automated location and relationship inferences, and can be used to determine highly sensitive traits"), <https://www.pnas.org/content/pnas/113/20/5536.full.pdf>.

³⁴⁵ (U) *Riley v. California*, 573 U.S. 373, 400 (2014) (citing *Smith v. Maryland*, 442 U.S. 735 (1979)).

³⁴⁶ (U) See Appendix B.

considered in *Smith*. As an example, CDRs could include information about whether a mobile phone involved in a call was roaming and on which network it was roaming. This might serve as a proxy for a phone's location within broad coverage areas. For example, if a CDR records that a phone whose home provider is Company A was roaming on Company B's network, this implies the phone was very likely in a location covered by B's network but not by A's. In addition, a CDR can contain information about which switching equipment handled a call, which can convey further location information.³⁴⁷

(U) It is facts like these that take the USA Freedom Act CDR program further from *Smith* and into an intermediate area between *Smith* and *Carpenter*.³⁴⁸ In *Carpenter*, the Court determined that warrantless collection of cell site location information violated the Fourth Amendment, and Chief Justice Roberts noted that “[a] majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements.”³⁴⁹ The more precise location data becomes, the more such data has the potential to reveal personal details of one's life.³⁵⁰ Although NSA did not collect cell site information in CDRs, and the statute expressly prohibited such collection, the fact that CDRs contained information indicative of more coarse-grained location does make *Carpenter* relevant. We cannot say how the Court would ultimately rule on the facts of the USA Freedom Act CDR program, but in viewing the Court's most recent Fourth Amendment decisions, the picture becomes less clear than the majority would suggest.

(U) Legal developments since the 2014 report strengthen our argument that *Smith* may not be as definitive as the majority suggests. We note, as our colleagues do, that as technology evolves, so too has the Supreme Court's Fourth Amendment jurisprudence. While the Court has not considered facts similar to the USA FREEDOM Act CDR program, and has not overturned *Smith*, we believe that *Riley* and *Carpenter* carry more significance in assessing the constitutionality of the CDR program based on the facts as we know them now than the majority affords them. In *Riley v. California*, the Supreme Court addressed a longstanding rule in Fourth Amendment law: that law enforcement need not obtain a search warrant before conducting a search incident to a suspect's lawful arrest. The Court held that the search-incident-to-arrest exception to the Fourth Amendment's warrant requirement does not apply to cell phones: “Our

³⁴⁷ (U) The implied location that might be inferred from a CDR is generally coarse-grained and does not violate the statute's prohibition on CDRs containing “cell site location or global positioning system information.”

³⁴⁸ (U) *Carpenter*, 138 S. Ct. at 2206.

³⁴⁹ (U) *Carpenter*, 138 S. Ct. at 2217 (citing *United States v. Jones*, 565 U.S. 400, 415, 430 (2012) (concurrences of Alito, J., and Sotomayor, J.)).

³⁵⁰ (U) *Carpenter*, 138 S. Ct. at 2218.

answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple— get a warrant.”³⁵¹

(U) More recently, and even more relevant to the USA FREEDOM Act CDR program, the Court held in *Carpenter v. United States* that law enforcement access to a week or more of cell-site location records constitutes a Fourth Amendment “search” and ordinarily requires a search warrant based on probable cause. In *Carpenter*, the government argued that *Smith* and the third-party doctrine should lead to the conclusion that because cell-site location records are held by telephone companies, or third-parties, government access to them is not subject to the Fourth Amendment. But the Court didn’t go that way. The Court expressly distinguished *Smith* and explained that the volume of data, the sensitivity of the data, and the unavoidability of the data collection by the third-party all weighed in favor of Fourth Amendment protection.

(U) The majority makes much of the Supreme Court’s insistence in *Carpenter* that *Smith* remains good law. This we likewise do not contest. But the *Carpenter* discussion does not address how *Smith* applies to the USA FREEDOM Act CDR program. *Carpenter*—like *Riley* and *United States v. Jones*³⁵²—instructs that that is not an easy question.

(U) While *Riley* and *Carpenter* do not overturn *Smith*, each contains commentary that presents a window into the Court’s view of the intersection of new technology and the Fourth Amendment. It is against this backdrop that we would have preferred the Board’s constitutional analysis to have been set.

(U) In addition to presenting an incomplete picture of how the Fourth Amendment may intersect with the USA FREEDOM Act CDR program as we now know it to be, the majority does not assess the program’s First Amendment implications. This large-scale CDR program surely sweeps in the CDRs of protestors, journalists, political activists, whistleblowers, and ordinary people. The First Amendment protects fundamental rights including the freedoms of speech and association. The Board’s 2014 analysis of the First Amendment challenges to the previous bulk CDR program largely extends to the USA FREEDOM Act CDR program, especially with respect to the potential chilling effect created by a program that collects the phone records of millions of people, without individualized suspicion.³⁵³ One would expect a court’s review of the reasonableness of the constitutionality of the USA FREEDOM Act’s CDR

³⁵¹ (U) *Riley*, 573 U.S. at 403.

³⁵² (U) “In *United States v. Jones*, the Supreme Court ruled that placing a GPS device on a Jeep driven by a criminal suspect, and then using the device to track the Jeep’s movements continuously for four weeks, was a “search” under the Constitution.” 2014 Board Report at 122 (discussing *United States v. Jones*, 565 U.S. 400 (2012)). For a more complete discussion of *Jones*, see the 2014 Board Report at 122–24.

³⁵³ (U) We do not repeat the Board’s full analysis here. For a full analysis, see the 2014 Board Report at 128–36.

program to also consider the program's implications on the First Amendment rights of Americans.

(U) We do not know whether a court, presented with the facts available to us, would find the USA FREEDOM Act CDR program to be constitutional. That is the same basic conclusion that the Board reached in 2014 about the bulk telephony CDR program. We do not believe, however, that the majority's analysis presents a complete picture of the current First and Fourth Amendment landscapes to establish that reauthorization and reoperation of the program, knowing what we know today, would be constitutional.

III. (U) The same program with data from different media is not the answer.

(U) Finally, in assessing the USA FREEDOM Act CDR program's national security value, it has been suggested, including by some of our fellow Board Members, that a multi-hop metadata collection program governing other types of communication media may prove more valuable than the CDR program. While this has not been a part of the Board's oversight review of the CDR program and is not something the Board investigated, we think it is important to note our disagreement with these suggestions.

(U) On this point, we are in general agreement with Chairman Klein. Congress knew what it was doing when it chose to limit this authority to telephony. The prior bulk 215 program had been focused on telephony, and the USA FREEDOM Act framework was designed to authorize a version of that program. The limitation of the bulk program to two hops had already been adopted as a matter of policy—so Congress was authorizing the program more or less as it was operating at the time.

(U) Even with the limitation to telephony—a technology with a 100-year history—there was substantial debate about legislating clear boundaries for its use in the CDR program. Had Congress instead tried to legislate over a broader and more rapidly evolving set of technologies, the definitional and boundary-drawing problems would have been vastly more difficult.

(U) And there is no reason to think the compliance or data quality issues encountered in the CDR program would have been less severe for other types of communications media. Working with a sector where developing new capabilities without fully examining downstream impacts is a common business practice would not have been conducive to stability and data accuracy—let alone compliance. Congress chose to scope the program to cover a more established technology operated by stable, long-lived, and historically regulated American companies.

(U) All of that said, there is and will continue to be significant intelligence value in first-hop communications metadata, and in additional hops where there is specific analytical

justification for acquiring them. What experience with the CDR program has taught is that domestic multi-hop metadata, without specific justification for its collection, is likely to have little impact on national security but would undermine the privacy of large numbers of Americans.

* * *

(U) The USA FREEDOM Act CDR program was implemented with knowledge of the Board's findings in 2014 regarding the bulk collection program, finding that the government could not demonstrate a strong enough showing of efficacy to justify the privacy and civil liberties implications of the program. The Board noted that "[i]f the government and Congress seek to develop a new program to replace the Section 215 program, any such new program should be crafted far more narrowly, and the government should demonstrate that its effectiveness will clearly outweigh any intrusions on privacy and civil liberties interests."³⁵⁴ This balance has not been realized in the USA FREEDOM Act CDR program. In the end, whether for concerns over constitutional implications or for policy reasons, we concur with NSA's decision to end the program and believe the program should remain shuttered.

³⁵⁴ (U) 2014 Board Report at 169.

VIII. (U) Statement of Board Members Aditya Bamzai and Jane Nitze

(U) Congress's consideration of legislation to reauthorize the call detail records program of the USA Freedom Act provides occasion to assess not only the program's costs and benefits, but also the manner in which Congress can legislate best in rapidly evolving technological areas. When the Board reviewed NSA's bulk telephony metadata program in 2014, it was divided. Key findings on the program's value split the Board three to two. In Congress and the public sphere, too, there were disputes, we believe largely in good faith, about the merits of the program. Five years after the USA Freedom Act was enacted and a new CDR program established, there is less room for debate. The program was statutorily authorized and constitutional under controlling precedents. It also was expensive, plagued with data-integrity concerns, and produced minimal intelligence relative to other national security programs. It is, of course, incumbent on us not to fall into a cycle of "timidity and aggression,"³⁵⁵ or to assume we are safe irrespective of, rather than because of, our security programs. But we have a hard time looking at this *particular* program as it *actually* operated and concluding much other than that the game is not worth the candle. That's not to say, though, that a well-designed metadata program, one not restricted by some of the USA Freedom Act's statutory limitations, couldn't succeed.

I.

~~(S//NF)~~ To get some figures down: Over its short lifetime the CDR program cost, at a minimum, 100 million dollars. NSA estimates over [REDACTED] were given to the providers alone, on top of the administrative costs of running the program and the resources expended unpacking and then resolving each of the compliance concerns. Against these costs, the specific benefit that the CDR program provided was the ability to get a "second hop" of CDRs in a relatively expeditious manner, without the need for a FISA business-records order for each "first-hop" number.³⁵⁶ Yet as noted in Part III(B) of the Board's report, the program

³⁵⁵(U) Many have noted that the national security apparatus engages in "controversial action[s] at the edges of the law," faces recriminations for those actions, and acts with timidity until a crisis spurs it, once again, to act at the edges of the law. JACK GOLDSMITH, *THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION* 163 (2007). *See also* 2014 Board Report at 209 (statement of Rachel Brand).

³⁵⁶ (U) The USA Freedom Act does not speak of "hops." Instead, it uses the following language:

An order under this subsection . . . shall . . . (iii) provide that the Government may require the prompt production of a first set of call detail records using the specific selection term . . . [and] (iv) provide that the Government may require the prompt production of a second set of call detail records using session-identifying information or a telephone calling card number identified by the specific selection term used to produce call detail records under clause (iii)[.]

resulted in the issuance of only 15 intelligence reports. While we may not expect metadata collection activities to produce as many reports as content collection activities, the government itself noted the program's limited relative value.³⁵⁷ The Board was informed, moreover, that FBI found the reports largely (though not wholly) redundant: in only two instances did FBI receive unique information from USA Freedom Act CDRs.

~~(TS//SI//NF)~~ Some of the reasons the CDR program did not produce a large volume of useful intelligence can be traced back to evolutions in technology since the first iteration of a post-9/11 telephony metadata program. Experts in and out of government have noted a shift away from traditional telephony, with terrorists increasingly using chat applications and encrypted messaging. Yet CDRs collected under the USA Freedom Act did [REDACTED]. As a result, the program could not have detected the 2019 analog of the reason it was created: to see [REDACTED]. The blame does not rest with NSA. Traditional telephone records simply do not carry the same importance they once did; no version of a domestic metadata program fixed solely on traditional telephony was likely to have produced intelligence reflective of its costs.

(U) That should not, however, distract us from the reality that multi-hop analysis can have important intelligence value. Simple commonsense examples illustrate how. First, consider the case of a terrorist organization using a trusted intermediary, or "cutout," for communications. The government may be investigating a particular target ("A") who communicates with a person ("B"), who in turn communicates with a senior terrorist leader ("C"). Investigators know of both A's and C's connection to the terrorist network, but do not know with whom C is communicating. If investigators are unaware of B, single-hop collection would show only that A is communicating with an unknown party, B. Because B is unknown, the government may be unable to establish the "reasonable articulable suspicion" necessary to secure process for further hops.³⁵⁸ Two-hop collection, by contrast, allows the government to see that A and C may be communicating through an intermediary, thereby bringing B's potential significance as a cutout to investigators' attention.

(U) This is but one of many examples that illustrate how contact-chain analysis may add significant intelligence value to national-security investigations. Here are two more. Consider that the target of an investigation ("A") could be communicating directly with a senior terrorist leader ("C") and also, at the same time, with an unknown party ("B"). The government may

(U) 50 U.S.C. § 1861(c)(2)(F)(iii)–(iv). For ease of exposition, we use the more colloquial term "hop," but we mean to capture the precise text of the statute.

³⁵⁷ (U) See NSA briefing to the Board (May 23, 2019); see also Letter from Daniel Coats, Director of National Intelligence, to Senators Richard Burr, Lindsey Graham, Mark Warner, and Dianne Feinstein (Aug. 14, 2019).

³⁵⁸ (U) 50 U.S.C. § 1861(b)(2)(B).

have no reason to investigate B until second-hop data shows that B, too, is communicating with C. Or consider that second-hop data may reveal a hub-and-spoke organization to a terrorist network, with an intermediary in communication with other parties of interest whose call records the government does not have. Contact chain analysis could give investigators the ability to identify the relevant persons within a network—leaders and critical individuals worthy of further investigative time and resources.

(U) Consider, as well, that in areas where the government is required to obtain orders from the FISA court for collection, multi-hop collection may allow the government to acquire information faster and more efficiently than single-hop authorities. With regard to the FISA court: there are, no doubt, salutary benefits to requiring the government to express in writing its justifications for surveillance and to seek approval from an independent entity before obtaining sensitive data. Yet, as the Board’s report explains, the drafting and approval process for applications to the FISC can take “days or weeks.”³⁵⁹ And we wonder if the time lost and the resources required might not sometimes deter investigators from seeking perfectly lawful and appropriate orders. By allowing more data to be acquired with fewer FISA court applications, multi-hop collection lessens these potential drawbacks and carries efficiency advances as compared to single-hop authorities—even in spaces in which equivalent data may be theoretically available under other authorities.

(U) All this is not to say that multi-hop analysis is without its costs. Like for any national security program, policymakers have to weigh the resources required to run multi-hop analysis against its intelligence value. They also should consider that by its nature, multi-hop analysis inevitably results in the collection of an exponentially larger amount of data than single-hop analysis. Just imagine for a moment all the numbers you dial—and that dial you—ranging from restaurants from which you order takeout, to banks with whom you check your account balance, to telemarketers who call you unannounced. Then imagine all of the numbers that those numbers call and all the other people who call those numbers. Even when the CDR program operated as designed, multi-hop collection acquired all those numbers—along, of course, with the numbers of terrorists A, B, and C in the examples above.

(U) The difficulty of quantifying costs and benefits in this area is not a unique feature of multi-hop programs. Indeed, more often than not people disagree in good faith about the relative costs and benefits of particular intelligence programs. On rare occasions, though, the balance will be fairly apparent—as it was to NSA (and to us) in the case of the USA Freedom Act CDR program. The value of multi-hop analysis in the abstract may be substantial; the value of this *particular* multi-hop program, in our view, was not.

³⁵⁹ (U) See Part II(A).

II.

(U) Many will point—as we do—to changing times and technologies in assessing the relative value of the CDR program. But that obvious truth should not pull us away from the harder question of how law and policy affect intelligence programs in both intended and unintended ways, potentially altering both their operational utility and invasiveness. In reviewing the transition from the bulk collection program to the operation, and then suspension, of the CDR program, we see the following worth noting.

(U) *First*, by tying the USA Freedom Act to telephony metadata alone, Congress limited the statute's usefulness as terrorists moved away from traditional telephony as their primary mode of communication. Experts have noted that the codification of surveillance authority in one technological medium will naturally push those seeking to evade government detection to substitute alternative methods of communications.³⁶⁰ And yet the Act did not provide multi-hop authority for the myriad other ways in which terrorists may communicate, from emails to encrypted messaging. That proved to be a problem. Thus, in the future, for surveillance authorities to be useful in a world of rapidly advancing technology, they should be neutral as to communications methods.³⁶¹

~~(TS//SI//NF)~~ *Second*, several of the compliance incidents arose when Congress codified in statute a two-hop architecture, a framework that seems to assume that telephone communications occur between two parties (*i.e.*, A calls B). But in a world where communications can occur through intermediaries, the two-hop statutory framework results in ambiguities as to how to determine the scope of a particular communication. The compliance incidents related to [REDACTED] were created by this statutory ambiguity and premised on the fundamental question left open by the statute: What's a hop? In this fashion, the USA Freedom Act itself created the potential for compliance difficulties, prompted by statutory confusion when the application of law to technology arose in unforeseen circumstances.³⁶²

³⁶⁰ (U) *See generally* Remarks of Robert Litt, General Counsel for the Office of the Director of National Intelligence, Statement before the Senate Judiciary Committee (Dec. 13, 2013).

³⁶¹ (U) The same issue arose when Congress amended the pen register statute in the USA PATRIOT Act of 2001. *See In re Certified Question*, 858 F.3d 591, 602 (FISA Ct. Rev. 2016) (“The principal change to the pen register/trap-and-trace provision was to make those provisions applicable not just to telephony, but to all forms of wire and electronic communications.”).

³⁶² (U) Courts have addressed comparable questions in the context of the pen register statute. *See, e.g., In re Certified Question of Law*, 858 F.3d at 591; *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125 (3d Cir. 2015).

(U) *Third*, some compliance incidents were caused simply because telephone providers turned over incorrect data to NSA.³⁶³ The government would appropriately request first- and second-hop data from a provider, only to receive data that did not meet the statute's expectations. There are, of course, many authorities, such as the Pen Register Statute³⁶⁴ and the Stored Communications Act,³⁶⁵ under which the government seeks telephony metadata. We do not know the number of compliance incidents under those separate authorities and whether the rates of incorrect data from providers under the CDR program were higher than rates under other programs. We would like to know the numbers, and if any differences were due to unique features of the USA Freedom Act.³⁶⁶ At a minimum, we believe the issue warrants further inspection.

(U) All the foregoing suggests that we should be wary of overly strict statutory regimes that limit technological flexibility; under some circumstances, rigorous use of oversight functions may even be superior in ensuring that government activities properly balance security and privacy interests. The President ordered significant changes to the bulk telephony metadata program after internal executive review, and the Board reported that after one year (and prior to the passage of the USA Freedom Act) the government had "accept[ed] many of the recommendations" in its report.³⁶⁷ Although these assessments did not occur until unlawful disclosures of the program led to public debate, that doesn't mean we should reflexively seek answers in unduly prescriptive statutory regimes that offer little by way of technological flexibility to implementing agencies.

(U) To be sure, law is essential to ensuring that the government does not overreach and that our national security apparatus remains democratically accountable to the people. Yet explicit and detailed codification of intelligence practices carries risk to both operations and privacy. It carries operational risk when it is unduly rigid, given the ever-changing threats our country faces. And it carries risk to our civil liberties when it serves as a continued source of positive authority even as technology evolves. Some of the laws governing access to electronic

³⁶³ (U) *See* Letter from Daniel Coats, Director of National Intelligence, to Senators Richard Burr, Lindsey Graham, Mark Warner, and Dianne Feinstein (Aug. 14, 2019) (noting "the unique complexities of using these company-generated business records for intelligence purposes").

³⁶⁴ (U) 18 U.S.C. § 3121 *et seq.*

³⁶⁵ (U) 18 U.S.C. § 2701 *et seq.*

³⁶⁶ (U) It is possible the error rate under the USA Freedom Act CDR program was either higher or lower than is found in records collected under other authorities. Given time limitations, we were unable to determine if it was even feasible to answer this question, never mind account for any differences in the error rate.

³⁶⁷ (U) Privacy and Civil Liberties Oversight Board, *Recommendations Assessment Report 1* (Jan. 29, 2015), https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf.

communications that precede the commercial internet (not to mention the smartphone) exemplify these risks.³⁶⁸

(U) The impact on intelligence and privacy of the changes wrought by the USA Freedom Act is particularly difficult to assess. For example, under the bulk collection program NSA approved only about 300 query terms in 2012. Yet under the USA Freedom Act, which prohibited bulk collection of call detail records, 164,682 US person query terms were run against NSA's data last year alone, perhaps in part because queries no longer required pre-approval either from designated agency officials or from the FISA court.³⁶⁹ At the same time, the number of intelligence reports dropped precipitously from one program to the next. In the three-year period between 2006 and 2009, NSA issued 277 intelligence reports—more than ten times the number produced during the life of the USA Freedom Act CDR program. It's not immediately obvious to us how to compare bulk collection with limited querying against more limited collection with more extensive querying; we also do not know if the drop in reports was due largely to changes in technology. At a minimum, though, it strikes us that a case can be made that the USA Freedom Act rendered the collection of CDRs less operationally valuable while augmenting the very privacy concerns it sought to lessen.

*

(U) The threats we face have not abated and technology continues to evolve. We encourage legislators to work with the executive branch as well as technology experts to understand any gaps in current authorities and how technology may be leveraged to better protect privacy while respecting national security imperatives.³⁷⁰ To retain operational value over time,

³⁶⁸ (U) For example, the Electronic Communications Privacy Act addresses the interception of electronic data and access to stored communications. But it was passed in 1986 and contains provisions that lead to counterintuitive results with modern technology. It allows the government to use a subpoena to obtain emails and similar electronic messages if they are stored on a third-party server for more than 180 days, but requires a warrant to access the same emails if they were in storage for a shorter period of time. 18 U.S.C. § 2703(a)–(d).

³⁶⁹ (U) To be sure, as noted in Part III(B), this number is inflated because of the manner in which NSA tracks and counts queries; many of the 164,682 query terms would never return USA Freedom Act CDRs. However, that number is still over 500 times higher than the number of annual query terms during the operation of the bulk program. Even substantial overcounting would not appear to make up for the difference.

³⁷⁰ (U) Our colleagues suggest that a multi-hop metadata program not limited to telephony metadata could never prove more valuable than the CDR program. *See* Statement of Ed Felten and Travis LeBlanc at 77. On the basis of this record, none of us can know. In light of the theoretical advantages of multi-hop analysis we have described above, it should be unsurprising that the intelligence community has identified contact-chain analysis as a significant tool that is worth the cost of collection and compliance under appropriate circumstances. Perhaps, though, we agree on more than we disagree. Our colleagues say there “is and will continue to be significant intelligence value in first-hop communications metadata, *and in additional hops where there is specific analytical justification for acquiring them.*” Statement of Ed Felten and Travis LeBlanc at 77–78 (emphasis added). It seems we agree that there is value in exploring that potential.

new communications surveillance authorities should be technologically neutral, allowing the government's implementation—both in gathering intelligence and in protecting civil liberties—to evolve alongside technology and the manner in which our adversaries plot and threaten our Nation. We look forward to working with Congress on these issues.

(U) Appendix A

(U) Part II includes an unclassified description of the compliance and data-integrity issues NSA experienced with the USA Freedom Act CDR program. The Board worked with the intelligence community to declassify and include as many facts related to these issues as possible in Part II. However, many facts necessarily remain classified because their release could be expected to cause exceptionally grave damage or serious damage to the national security. To protect this information, but also to ensure additional transparency for appropriately cleared individuals, including members of Congress, this annex describes those issues and NSA's response in a more comprehensive, classified manner.

A. (U) General Compliance Matters

1. (U) Omitted Information from FISA Application

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

2. (U) Overproduction

[REDACTED]

-
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

3. (U) Training Compliance Incidents

[REDACTED]

[REDACTED]

-
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

B. (U) Data-Integrity Issues

(U) This section provides additional, classified detail to NSA's repeated discovery of anomalies in the data produced by providers in response to FISA court orders and NSA's response to these incidents.

1. (U) Production of Inaccurate First-Hop Numbers

[REDACTED]

[REDACTED]

-
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2. ~~(S//NF)~~ Production of Inaccurate Data Associated with [REDACTED]

[REDACTED]

[REDACTED]

-
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

-
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

[REDACTED]

[REDACTED]

3. (U) Expanding Accuracy Concerns Lead NSA to Delete All CDRs

[REDACTED]

-
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

1. **Identify the main components of the system.**
 2. **Define the scope and objectives of the study.**
 3. **Formulate a hypothesis or research question.**
 4. **Design the experiment or study.**
 5. **Collect and analyze data.**
 6. **Draw conclusions and discuss implications.**

-

[REDACTED]

4. (U) Additional Compliance Issues and Concerns

[REDACTED]

[REDACTED]

-
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

-
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

[REDACTED]

[REDACTED]

-
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

(U) Appendix B

[REDACTED]

- I [REDACTED]
- I [REDACTED]
- I [REDACTED]
- I [REDACTED]

[REDACTED]

[REDACTED]

