Comments to the Privacy and Civil Liberties Oversight Board re:
Section 702 of the Foreign Intelligence Surveillance Act

submitted by:

The Brennan Center for Justice at NYU School of Law

November 4, 2022

Elizabeth Goitein
Senior Director
Liberty & National Security Program
Brennan Center for Justice at NYU School of Law
1140 Connecticut Avenue, NW
Eleventh Floor
Washington, DC 20036

Introduction

Congress's goal when it enacted Section 702 of the Foreign Intelligence Surveillance Act ("FISA") in 2008 was to give our government more powerful tools to address terrorist threats. In writing the law, however, Congress did not expressly limit Section 702 surveillance to that purpose. Instead, Congress gave significant discretion to the executive branch and the Foreign Intelligence Surveillance Court ("FISA Court" or "FISC"), trusting them to ensure that the law was implemented in a manner consistent with its objective. For instance, Congress allowed the government to target almost *any* foreigner overseas, counting on intelligence agencies to focus their efforts on those who pose a threat to our country. Congress also did not specify what minimization should look like, leaving that to the agencies and the judges of the FISA Court.

Rather than tailoring its surveillance as Congress expected, the executive branch has taken full advantage of the leeway provided in the statute. Instead of simply acquiring the communications of suspected terrorists or foreign powers overseas, the government is scanning nearly all of the international communications that flow into and out of the United States via the Internet backbone, and is acquiring hundreds of millions of these communications each year. This surveillance inevitably pulls in vast amounts of Americans' calls, texts, and e-mails.

Section 702 also has fallen victim to mission creep. A statute designed to protect against foreign threats to national interests has become a major source of warrantless access to Americans' data and a tool for ordinary domestic law enforcement. The most recent statistical transparency report issued by the Office of the Director of National Intelligence ("ODNI") revealed that the FBI conducted more than *three million* searches of Section 702 data in 2021 for the purpose of finding Americans' communications. This outcome is contrary, not only to the original intent of FISA, but to Americans' expectations and their trust that Congress will protect their privacy and freedoms.

Perhaps most disturbingly, with every new release of a FISA Court opinion, it becomes increasingly clear that the rules designed to protect Americans' privacy are being honored in the breach. Agencies have repeatedly, and in some cases systemically, violated statutory or court-ordered limitations on collection, retention, querying, and dissemination. Some of these violations have rendered the operation of the program unconstitutional. When Congress last reauthorized Section 702, it sought to shore up privacy protections by requiring FBI agents to obtain a warrant before accessing Section 702 data about Americans in certain investigations. According to the government's own reports, the FBI has *never* complied with this requirement.

The concerns with Section 702 apply with even greater force to surveillance under Executive Order (EO) 12333, which is subject to far fewer constraints. Generally speaking, Section 702 applies when the collection takes place inside the United States or from a U.S. company, while Executive Order 12333 applies when the collection takes place overseas. In the digital era, however, this distinction has become artificial. Overseas surveillance can have just as great an impact on Americans' privacy as domestic surveillance, if not greater. Reforms to Section 702 will have limited effect if EO 12333 surveillance continues to be carved out of foreign intelligence surveillance legislation.

As Congress considers reauthorization of Section 702, the Privacy and Civil Liberties Oversight Board should use its authority in two ways. First, following up on its highly effective 2014 investigation into the workings of Section 702, the PCLOB should undertake three projects designed to elicit key information. The first project would entail working with the intelligence community to develop an estimate of how many communications involving U.S. persons are "incidentally" collected under Section 702. The second project would be an investigation of the government's targeting decisions under Section 702, with an eye toward making recommendations for narrowing the criteria for targeting. The third project would be an examination of how Section 702 is used for cybersecurity purposes, in light of indications that investigations into cybersecurity threats involve particularly broad surveillance.

Second, PCLOB should recommend reforms to Section 702. The core of Section 702 is the ability it gives the government to obtain the communications of foreign powers and suspected foreign terrorists without obtaining a warrant. There are several potential reforms that would leave this core intact, while adding badly needed protections for law-abiding citizens of this country and others. These reforms fall into the following categories: (1) narrowing the scope of Section 702 collection; (2) shoring up protections for "incidentally" acquired U.S. person information by requiring agencies to obtain a warrant, court order, or subpoena before running U.S. person queries of Section 702 data, and by placing stricter limits on retention; (3) modernizing FISA by establishing basic rules and requiring FISA Court oversight for EO 12333 surveillance; and (4) increasing transparency and accountability in the operations of Section 702 and EO 12333.

I. Section 702: A Massive Expansion in the Scope of Foreign Intelligence Surveillance

Technological advances have revolutionized communications. People are communicating at a scale unimaginable just a decade ago. International phone calls, once difficult and expensive, are now as simple as flipping a light switch, and the Internet provides countless additional means of international communication. Globalization makes such exchanges as necessary as they are easy. As a result of these changes, the amount of information about Americans that the NSA intercepts, even when targeting foreigners overseas, has exploded.[1]

But instead of increasing safeguards for Americans' privacy as technology advances, the law has evolved in the opposite direction since 9/11. In its zeal to bolster the government's powers to conduct surveillance of foreign threats, Congress has amended surveillance laws in ways that increasingly leave Americans' information outside their protective shield (the USA FREEDOM Act being the notable exception). Section 702 is a particularly striking example.

Before 2007, if the NSA, operating domestically, sought to wiretap a foreign target's communications with an American inside the U.S., it had to show probable cause to the FISA Court that the target was a foreign power — such as a foreign government or terrorist group —

[1] *See* ELIZABETH GOITEIN & FAIZA PATEL, WHAT WENT WRONG WITH THE FISA COURT 19–21 (Brennan Ctr. for Justice 2015), https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf.

or its agent. The Protect America Act of 2007 and the FISA Amendments Act of 2008 (which created Section 702 of FISA) eliminated the requirement of an individualized court order. Domestic surveillance of communications between foreign targets and Americans now takes place through massive collection programs that involve no case-by-case judicial review.[2]

Executive officials have often argued that Section 702 was necessary to address changes in communications technology and "modernize" FISA. They note that, before 2007, the law required the NSA to obtain a FISA Court order to collect certain foreign-to-foreign e-mails stored by internet service providers inside the United States — something Congress almost certainly did not intend when it originally passed FISA. Section 702, however, went much further than was necessary to correct that problem. It did not simply allow the warrantless collection of foreign-to-foreign e-mails inside the United States; it allowed the warrantless collection of communications, both stored and in transit, between foreign targets and Americans. This state of affairs differs fundamentally from the regime Congress designed in 1978.[3]

Another critical change is that the pool of permissible targets is no longer limited to foreign powers or their agents. Under Section 702, the government may target for foreign intelligence purposes any person or group reasonably believed to be foreign and located overseas.[4] The person or group need not pose any threat to the United States, have any information about such threats, or be suspected of any wrongdoing. This change not only renders innocent private citizens of other nations vulnerable to NSA surveillance; it also greatly

---

[2] *See* 50 U.S.C. § 1881a.

[3] Some executive branch officials have suggested that Congress in 1978 intended to regulate surveillance only for purely domestic communications. They note that FISA required the government to obtain an individual court order when collecting any communications involving Americans that traveled by wire, but required an individual court order to obtain satellite communications only when all of the communicants were inside the U.S. Asserting that wire technology was the norm for domestic calls, while most international communications were carried by satellite (and were thus "radio communications"), they infer that Congress intended to require the government to obtain an order when acquiring purely domestic communications, but not when obtaining communications between foreign targets and Americans. This intent, they argue, was undermined when fiber-optic cables later became the standard method of transmission for international calls.

The problem with this theory is two-fold. First, it would have been quite simple for Congress to state that FISA orders were required for purely domestic communications and not for international ones. Instead, Congress produced an elaborate, multi-part definition of "electronic surveillance" that relied on particular technologies rather than the domestic versus international nature of the communication. Second, contrary to the factual premise of this theory, the available evidence indicates that one third to one half of international communications *were* carried by wire back in 1978. David Kris, *Modernizing the Foreign Intelligence Surveillance Act* 3 (Brookings Inst., Working Paper, 2007), *available at* http://www.brookings.edu/~/media/research/files/papers/2007/11/15%20nationalsecurity%20kris/1115_nationalsecurity_kris.pdf.

A more plausible explanation for the original FISA's complex scheme was put forward by David Kris, a former head of the Justice Department's National Security Division. Mr. Kris concluded that Congress intended to require a court order for international wire communications obtained in the U.S., and that the purpose behind its definitional acrobatics was to leave legislation covering surveillance conducted outside the U.S. and NSA satellite surveillance for another day. *Id.* at 13–23. Although Congress never followed up, the legislative history of FISA made clear that the gaps in the statute's coverage of NSA's operations "should not be viewed as congressional authorization for such activities as they affect the privacy interests of Americans." S. REP. NO. 95-701, at 35 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4004.

[4] 50 U.S.C. § 1881a(b).

increases the number of communications involving Americans that are subject to acquisition — as well as the likelihood that those Americans are ordinary, law-abiding individuals.

Further expanding the universe of available communications, the government and the FISA Court have interpreted Section 702 to allow the collection of any communications to, from, *or about* the target.[5] The inclusion of "about" in this formulation is a dangerous leap that finds no basis in the statutory text and little support in the legislative history. In practice, it has been applied to collect communications between non-targets that include the "selectors" associated with the target (e.g., the target's e-mail address or phone number). In theory, it could be applied even more broadly to collect any communications that even mention Vladmir Putin, ISIS, or a wide array of other individuals and groups who are common topics of conversation. Although the NSA is prohibited from intentionally acquiring purely domestic communications, such acquisition is an inevitable result of so-called "abouts" collection.

The NSA's failure to comply with minimization rules for "abouts" collection (discussed later in these comments), which delayed the FISA Court's approval of the program in 2016, led the agency to stop the practice in April of 2017.[6] When Congress reauthorized Section 702 in early 2018, it required the government to provide 30 days' notice if it intended to restart "abouts" collection. There is no public indication that this has happened, and no FISA Court decision approving the reinstitution of "abouts" collection has been released. However, the door remains open to the NSA resuming this practice in the future.

Other than the foreignness and location criteria (and certain requirements designed to reinforce them), the only limitation on collection imposed by the statute is that the government must certify, on a program-wide basis, that acquiring foreign intelligence is a significant purpose of the collection.[7] FISA's definition of foreign intelligence is not limited to information about potential threats to the U.S. or its interests. Instead, it includes information "that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States."[8] This could encompass everyday discussions of current events. A conversation between friends or colleagues about trade between the U.S. and China "relates to the conduct of foreign affairs," as does a conversation about whether the U.S. should do more to support Ukraine. Moreover, while a significant purpose of the program must be the acquisition of foreign intelligence, the primary purpose may be something else altogether.[9] Finally, the statute requires the FISA Court to accept the government's certifications under Section 702 as long as they contain the required elements.[10] These factors greatly weaken the force of the "foreign intelligence purpose" limitation.

---

[5] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 37 (2014) [hereinafter PCLOB 702 REPORT], *available at* https://www.pclob.gov/library/702-report.pdf.

[6] Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets,* N.Y. TIMES (Apr. 28, 2017), https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html.

[7] 50 U.S.C. § 1881a(g)(2)(A)(v).

[8] 50 U.S.C. § 1801(e)(2).

[9] *In re* Sealed Case, 310 F.3d 717, 734 (FISA Ct. Rev. 2002).

[10] 50 U.S.C. § 1881a(i)(3)(A).

Going forward, the expansive scope of Section 702 surveillance might be somewhat constrained by President Biden's recent executive order establishing new rules for the collection of signals intelligence. The order sets forth twelve legitimate objectives for signals intelligence collection, [11] which are more specific than the general language contained in FISA's definition of "foreign intelligence information." However, these purpose-based limitations do not necessarily translate into constraints on the scope of surveillance. For instance, one of the permissible purposes is to protect against threats to cybersecurity — a goal that could in theory justify constant monitoring of any and all Internet networks. Furthermore, the order permits the president to add to the list of objectives, and to do so secretly if the president determines that disclosure of the new objective(s) would harm national security.

The government uses Section 702 to engage in two types of surveillance. The first is "upstream collection," whereby communications flowing into and out of the United States on the Internet backbone are scanned for selectors associated with designated foreigners. Although the data are first filtered in an attempt to weed out purely domestic communications, the process is imperfect and domestic communications are inevitably acquired.[12] The second type of Section 702 surveillance is "PRISM collection," under which the government provides selectors, such as e-mail addresses, to U.S.-based electronic communications service providers, who must turn over any communications to or from the selector.[13]

Using both approaches, the government collected more than 250 million Internet transactions a year as of 2011 — the last year for which such information is publicly available.[14] Because agencies generally may store Section 702 data for at least five years, a yearly intake of 250 million communications would result in at least 1.25 billion communications residing in government databases at any given time. The actual number is almost certainly higher, as the 250 million figure does not include telephonic communications, and the number of targets today is likely much larger than in 2011. Since 2013, when the government first began reporting the number of Section 702 targets, that number has risen from 89,138[15] to 232,432.[16]

In short, under Section 702, the rules for U.S.-based surveillance of foreigners overseas were rewritten to greatly loosen restrictions on targeting and to remove any individualized oversight of targeting decisions by the FISA Court. It is no wonder that this form of surveillance has ballooned, with hundreds of millions — if not billions — of communications collected each year.

---

[11] Exec. Order 14086, § 2(b)(i)(A), 87 Fed. Reg. 62283–4 (Oct. 7, 2022).
[12] PCLOB 702 REPORT, *supra* note 5, at 36–41.
[13] *Id.* at 33–34.
[14] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).
[15] OFF. DIR. NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013 (Jun. 2014), *available at* https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.
[16] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2021 (Apr. 2022), *available at* https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2022/item/2291-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2021.

This mass surveillance disregards the privacy rights of law-abiding foreign nationals — and that, in turn, is causing economic headaches for the United States. On two occasions, the Court of Justice for the European Union (CJEU) has struck down agreements between the United States and the European Union governing the transfer of data between EU and U.S. companies.[17] One major reason for the court's rulings is that Section 702 provides the U.S. government with ready access to EU citizens' data in the hands of U.S. companies, in contravention of European law. President Biden's recent executive order was issued to pave the way for a new data-transfer agreement, but observers doubt whether that order includes sufficient constraints on surveillance to satisfy the CJEU.[18] More than 5,000 U.S. companies rely on a U.S.-EU data-sharing agreement to do business.[19]

Beyond these economic woes, mass surveillance of foreigners overseas has inevitable and significant impacts on Americans' privacy, as discussed in the next Part.

II. The Impact of Section 702 on Americans' Privacy

Because the "target" of Section 702 surveillance must be someone reasonably believed to be a foreigner overseas, the collection of Americans' communications with those targets is described as "incidental," and the statute requires "minimization" of those Americans' information. These are terms of art that have particular legal meanings. Legal and policy defenses of Section 702 in its current form rely heavily on these terms and concepts.

The impact on Americans' privacy, however, does not. If the government is collecting tens of millions of Americans' communications and keeping them for years in databases where they are vulnerable to abuse, inadvertent mishandling, or theft, it matters little — from a practical perspective — that their initial acquisition was "incidental," or that the procedures allowing them to be kept and stored include "minimization" in their title. And if FBI agents are searching this data for Americans' communications, reading and listening to them, and using them against Americans in legal proceedings, those Americans will not be particularly comforted (indeed, they may well be baffled) to hear that they are not "targets."

The government has refused to provide any information that would give Congress and Americans a sense of the volume of Americans' communications being collected and stored. We do know, however, that the rules for "minimization" allow agencies to keep this "incidentally" acquired data for five years or longer. We also recently learned that the FBI searches through Section 702 data for Americans' communications literally millions of times each year — and that

---

[17] *See* Case C-311/18, Data Protection Commissioner v. Schrems, ECLI:EU:C:2020:559 (Jul. 16, 2020), *available at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4231279; Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct. 6, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

[18] American Civil Liberties Union, *To Make Real Progress, ACLU Calls on Congress to Enact Meaningful Surveillance Reform* (Oct. 7, 2022), https://www.aclu.org/press-releases/new-biden-executive-order-eu-us-data-transfers-fails-adequately-protect-privacy.

[19] *See* Adam Satariano, *E.U. Court Strikes Down Trans-Atlantic Data Transfer Pact*, N.Y. TIMES (Jul. 16, 2020), https://www.nytimes.com/2020/07/16/business/eu-data-transfer-pact-rejected.html.

it has never complied with the statutory warrant requirement that applies to some of these searches.

A. How Many Americans' Communications Does the NSA Collect?

Section 702 surveillance obtains the communications, not only of foreign targets, but of any Americans who are in contact with them. The number of Americans' communications thus collected is likely quite large: If only one out of every 250 communications involves an American, that would still add up to more than one million communications a year. But there is no official public information on how many Americans' communications are in fact swept up in Section 702 surveillance.

In 2011, Senators Ron Wyden and Mark Udall asked the Inspectors General of the Intelligence Community and the NSA to come up with a public estimate of this number.[20] They were later joined in this call by several other senators from both parties.[21] The Inspectors General responded that generating an estimate would itself violate Americans' privacy, ostensibly because it might involve reviewing communications that would otherwise not be reviewed.[22] In October of 2015, however, a coalition of more than thirty advocacy groups — including many of the nation's most prominent privacy organizations — sent a letter to the Director of National Intelligence (DNI) urging that the NSA go forward with producing an estimate.[23] The letter noted that, as long as proper safeguards were in place, the result would be a net gain for privacy.

In April 2016, a bipartisan group of fourteen House Judiciary Committee members sent the DNI a letter making the same request.[24] Eight months later, the members wrote again to memorialize their understanding, in light of interim conversations and briefings, that the DNI would provide the requested estimate "early enough to inform the debate," and with a target date of January 2017.[25] By all private and public accounts, the intelligence community was close to launching its count at the beginning of 2017.

---

[20] *See* Letter from Senators Ron Wyden and Mark Udall to The Honorable I. Charles McCullough III, Inspector General of the Intelligence Comm., and Dr. George Ellard, Inspector General, Nat'l Sec. Agency (May 4, 2011), *available at* https://www.wyden.senate.gov/download/?id=CE360936-DFF9-4273-8777-09BF29565086&download=1.

[21] *See* Ron Wyden, *Senators Seek Answers from DNI on How Many of Americans' Communications Have Been Monitored* (Jul. 12, 2012), https://www.wyden.senate.gov/news/press-releases/senators-seek-answers-from-dni-on-how-many-of-americans-communications-have-been-monitored.

[22] Letter from The Honorable I. Charles McCullough, III, Inspector General of the Intelligence Comm., to Senators Ron Wyden and Mark Udall (June 15, 2012), *available at* https://www.wyden.senate.gov/download/?id=E5DEF293-A8D6-4014-A23A-909C82A3C510&download=1.

[23] Letter from Brennan Ctr. for Justice, et al., to James Clapper, Dir. Nat'l Intelligence (Oct. 29, 2015), *available at* https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf.

[24] Letter from Rep. John Conyers, Jr., et al., to James Clapper, Dir. Nat'l Intelligence (Apr. 22, 2016), *available at* https://www.brennancenter.org/sites/default/files/legal-work/Letter_to_Director_Clapper_4_22.pdf.

[25] *See* Press Release, U.S. House Comm. on the Judiciary Democrats, Bipartisan House Coalition Presses Clapper for Information on Phone & Email Surveillance (Dec. 16, 2016), *available at* https://democrats-judiciary.house.gov/news/press-releases/bipartisan-house-coalition-presses-clapper-information-phone-email-surveillance.

Following the change in administration, however, the government backed down from this commitment. In June 2017, then-Director of National Intelligence Dan Coats testified before Congress that it was technologically infeasible to generate an estimate without invading Americans' privacy — the very same claim that was addressed and seemingly resolved under the previous administration.[26] The government retreated to its 2012 assertion that there is no automated way to assess whether a particular communication is to or from an American.

The problem with this claim is that the NSA can, and routinely does, make such an assessment when it conducts upstream surveillance. The FISA Court has held that the Constitution requires the government to take certain steps to minimize the acquisition, retention, and searching of wholly domestic communications. One of these steps, as the PCLOB reported in 2014, is the NSA's use of IP addresses and "comparable technical means" to filter out domestic communications when conducting upstream surveillance of Internet transactions.[27] Both the NSA and the FISA Court consider this method of identifying the domestic-versus-foreign status of communicants sufficient for purposes of complying with the Constitution. If it is sufficient for that purpose, it is certainly adequate to give Congress and the public a rough sense of how Section 702 collection impacts Americans.

In addition, there should be no difficulty in generating an estimate of how many Americans' telephone calls are collected: The government can simply use the country code as a proxy. The method is not perfect — a cell phone's country code does not always correspond with the location or nationality of the user — but again, lawmakers are seeking a rough estimate, not an exact count.

Stored e-mails, obtained through the PRISM program, are admittedly a harder case. However, computer scientists Jonathan Mayer and Anunay Kulshrestha of Princeton University have proposed a method that would leverage information in communications providers' possession, using encryption at various stages in the process to restrict the information actually visible to the providers and to the government.[28] If that fails, the privacy community is unanimous in its conclusion that the NSA should perform a one-time limited sampling of collected communications, under conditions (such as the immediate deletion of the communications after review) that would minimize the privacy intrusion.[29]

It is worth noting that the government maintained for many years that it could not track the number U.S. person queries the FBI performed on Section 702 data, in part because doing so would require an added intrusion into the query subjects' privacy. Based on this representation, Congress excluded the FBI from a reporting requirement imposed on other agencies. In 2018, however, Congress required the FBI to keep records of its U.S. person queries, and when the FBI

---

[26] Dustin Volz, *NSA Backtracks On Sharing Number of Americans Caught in Warrant-less Spying*, REUTERS (Jun. 12, 2017), http://www.reuters.com/article/us-usa-intelligence-idUSKBN19031B.
[27] *See* PCLOB 702 REPORT, *supra* note 5, at 38.
[28] Anunay Kulshrestha & Jonathan Mayer, *Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum* (USENIX Sec. Symposium, 2022), *available at* https://www.usenix.org/system/files/sec22-kulshrestha.pdf.
[29] *See* Letter from Brennan Ctr. for Justice, et al., to James Clapper, *supra* note 23.

failed to do so, the FISA Court ordered it to comply.[30] In 2022, the ODNI's annual statistical transparency report included the number that the FBI had claimed it could not produce.[31]

If the government is truly incapable of ascertaining, even roughly, how many Americans' communications it is collecting, that fact is in itself alarming. Regardless of whether it is lawful, the "incidental" collection of Americans' communications has real and significant effects on privacy — particularly when (as discussed below) that information can be stored for years, searched, and used in legal proceedings. The government cannot simultaneously assure the public that the impact of Section 702 surveillance on Americans' privacy is minimal, while also maintaining that it has no idea — and no way to discover — how many Americans' communications it is acquiring and storing.

B. Minimization and Its Loopholes

Minimization procedures are intended to mitigate the effects of "incidental" collection. The concept behind minimization is fairly simple: The interception of Americans' communications when targeting foreigners is inevitable, but because such interception would otherwise require a warrant or individual FISA order, incidentally collected U.S. person information generally should not be kept, shared, or used, subject to narrow exceptions.

The statutory language, however, is much more complex. It requires the government to adopt minimization procedures, which it defines as procedures "that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[32] The statute also prohibits disseminating non-foreign intelligence information in a way that identifies U.S. persons unless their identity is necessary to understand foreign intelligence information or assess its importance. The one caveat is that the procedures must "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes."[33]

The lack of specificity in this definition, and the tension between its general rule and its caveat, has allowed the government to craft rules that are permissive and contain multiple exceptions. To begin with, the NSA may share raw data from its PRISM collection with the FBI, the CIA, and (as of April 2017) the National Counterterrorism Center (NCTC).[34] All four agencies generally may keep unreviewed raw data — including data about U.S. persons — for

---

[30] [Redacted], 402 F. Supp. 3d 45, 66–73 (FISA Ct. 2018).
[31] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 16, at 21.
[32] 50 U.S.C. § 1801(h)(1).
[33] 50 U.S.C. § 1801(h)(3).
[34] WILLIAM BARR, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 7(c) (Sept. 16, 2020) [hereinafter NSA 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Minimization%20Procedures_10.19.2020.pdf.

five years after the certification expires;[35] they also can seek extensions from a high-level official,[36] and the 5-year limit does not apply to encrypted communications (which are becoming increasingly common among ordinary users of mobile devices) or communications that "reasonably appear[]…to contain secret meaning."[37] The agencies may keep indefinitely any U.S. person information that has foreign intelligence value or is evidence of a crime.[38]

If the NSA discovers U.S. person information that has no foreign intelligence value and contains no evidence of a crime, the agency is supposed to purge the data.[39] The NSA, however, interprets this requirement to apply only if the NSA analyst determines "not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need."[40] This is an impossibly high bar, and so, "in practice, this requirement rarely results in actual purging of data."[41]

The FBI, CIA, and NCTC have no affirmative requirement to purge irrelevant U.S. person data on detection, relying instead on age-off requirements. Moreover, if the FBI reviews U.S. person information and *does not identify it* as foreign intelligence information or evidence of a crime, the 5-year limit evaporates, and the FBI may keep the data for 15 years.[42] A similar rule applies to the NCTC.[43]

---

[35] *Id.* at § 4(c)(1)-(2) (2020); WILLIAM BARR, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § III.D.4.b (Oct. 19, 2020) [hereinafter FBI 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_FBI%20Minimization%20Procedures_10.19.2020.pdf; WILLIAM BARR, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 2.a (Sept. 16, 2019) [hereinafter CIA 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_CIA%20Minimization%20Procedures_10.19.2020.pdf; WILLIAM BARR, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § B.2.a (Oct. 19, 2020) [hereinafter NCTC 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NCTC%20Minimization%20Procedures_10.19.2020.pdf.

[36] PCLOB 702 REPORT, *supra* note 5, at 60; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 35, at § B.2.a.

[37] NSA 702 MINIMIZATION PROCEDURES, *supra* note 34, at § 7(a)(1).a; FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § I.4; CIA 702 MINIMIZATION PROCEDURES, *supra* note 35, at § 3.c.

[38] NSA 702 MINIMIZATION PROCEDURES, *supra* note 34, at §§ 6(a)(1), 7(a); FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § III.A.3; CIA 702 MINIMIZATION PROCEDURES, *supra* note 35, at §§ 3.a, 7.d; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 35, at § B.3.

[39] NSA 702 MINIMIZATION PROCEDURES, *supra* note 34, at §§ 4(b)(1), 4(c).

[40] PCLOB 702 REPORT, *supra* note 5, at 62.

[41] *Id.*

[42] FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § III.D.4.c.

[43] [Redacted], at 40 (FISA Ct. Apr. 26, 2017), *available at* https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

If any of the four agencies — all of which have access to raw data — disseminate information to other agencies, they must first obscure the identity of the U.S. person; but once again, there are several exceptions to this rule. For instance, the agencies need not obscure the U.S. person's identity if it is necessary to understand or assess foreign intelligence or if the communication contains evidence of a crime.[44]

In short, the NSA routinely shares raw Section 702 data with the FBI, CIA, and NCTC; and the agencies' minimization procedures suggest that U.S. person information is almost always kept for at least five years and, in many circumstances, much longer. The sharing and retention of U.S. person information are not unrestricted, but it is a stretch to say that they are "minimized" under any common sense understanding of the term.

C. Back Door Searches

Perhaps the most glaring failure of "minimization" is the fact that all four agencies are permitted to query Section 702 data using U.S. person identifiers, with the express goal of retrieving and analyzing Americans' communications.[45] This practice, commonly known as "back door searches," is both constitutionally suspect and at odds with the stated purpose and design of the statute.

If the government wishes to obtain an American's communications for foreign intelligence purposes, it must secure an individual court order from the FISA Court after showing probable cause that the target is an agent of a foreign power. If the government wishes to obtain an American's communications for law enforcement purposes, it must get a warrant from a neutral magistrate. To ensure that Section 702 is not used to avoid these requirements, the statute contains a prohibition on "reverse targeting" — i.e., targeting a foreigner overseas when the government's intent is to target "a particular, known person reasonably believed to be in the United States." Before conducting Section 702 surveillance, the government must certify that it does *not* intend to target particular, known Americans.

And yet, immediately upon obtaining the data, all four agencies may sort through it looking for the communications of particular, known Americans — the very people in whom the government just disclaimed any interest. Worse, even though the FBI would be required to obtain a warrant in order to access Americans' communications absent a significant foreign intelligence purpose, the FBI may — and, "with some frequency,"[46] does — search the Section 702 data for Americans' communications to use in criminal proceedings having no foreign

---

[44] NSA 702 MINIMIZATION PROCEDURES, *supra* note 34, at § 7(b); FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § IV.A.1–2; CIA 702 MINIMIZATION PROCEDURES, *supra* note 35, at §§ 5, 7.d; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 35, at § D.1–2. In addition, the FBI may disseminate unminimized Section 702 data to the NSA, CIA, and in some cases the NCTC. FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § IV.E.

[45] NSA 702 MINIMIZATION PROCEDURES, *supra* note 34, at § 4(b)(4); FBI 702 MINIMIZATION PROCEDURES, *supra* note 35, at § III.D.3; CIA 702 MINIMIZATION PROCEDURES, *supra* note 35, at § 4; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 35, at § C.1.

[46] PCLOB 702 REPORT, *supra* note 5, at 59.

intelligence dimensions whatsoever.[47] This is a bait and switch that is utterly inconsistent with the spirit, if not the letter, of the prohibition on reverse targeting. It also creates a massive end run around the Fourth Amendment's warrant requirement.

For years, the FBI resisted calls to disclose how many backdoor searches it performs each year. But after Congress and the FISA Court forced the FBI to track those queries, the government lost its excuse to withhold the number. In 2022, the ODNI's annual statistical transparency report revealed that the FBI had conducted up to *3.4 million* U.S. person queries in 2021 alone.[48] The report notes that the figure likely overstates the number of Americans affected, in part because there could be multiple searches relating to a single individual. But even if the figure is off by an order of magnitude, that still means that every day, nearly a thousand Americans are subject to a warrantless search for their personal communications.

Indeed, on some days, that number is much higher. The FBI has adopted a practice of "batch queries," in which it runs hundreds or thousands of queries under a single justification. In March 2017, against the advice of its Office of General Counsel, the FBI performed a batch query for 70,000 people — most of whom were presumably U.S. persons, given that the targets of the query were people with access to FBI facilities.[49]

In the past, some have defended back door searches, claiming that as long as information is lawfully acquired, agencies may use the information for any legitimate government purpose. This legal defense entirely misses the point. The staggering figure of 3.4 million U.S. person queries per year,[50] even with all the government's caveats, makes clear that there is nothing "incidental" about Section 702's impact on Americans. Warrantless access to Americans' communications has become a core feature of a surveillance program that purports to be solely foreign-focused.

In any event, the argument that Section 702 data may lawfully be used for any purpose ignores Congress's command to agencies to "minimize" information about U.S. persons. The very meaning of "minimization" is that agencies may *not* use the information for any purpose they wish. Minimization is a constitutional requirement as well as a statutory one: As Judge Bates of the FISA Court has observed, "[T]he procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."[51]

---

[47] ROBERT S. LITT, OFF. DIR. NAT'L INTELLIGENCE, PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: AN OVERVIEW OF INTELLIGENCE COLLECTION (July 18, 2013), https://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection.

[48] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 16, at 21.

[49] [Redacted], 402 F. Supp. 3d 45, 76 (FISA Ct. 2018).

[50] Although the FBI is by far the most prolific user of back door searches, other agencies also make use of them. In 2021, the NSA, CIA, and NCTC performed U.S. person queries of communications *content* on 8,790 occasions. The NSA and CIA further conducted U.S. person queries of communications *metadata* 3,958 times. OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 16, at 18–19.

[51] [Redacted], 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011). In cases involving the so-called "foreign intelligence exception" to the warrant requirement, the reasonableness of a surveillance scheme turns on weighing the government's national security interest against the privacy intrusion. While the surveillance scheme (*cont'd*)

Indeed, restrictions on searches of lawfully obtained data are the constitutional norm, not the exception. In executing warrants to search computers, the government routinely seizes and/or copies entire hard drives. However, agents may only conduct searches reasonably designed to retrieve those documents or files containing the evidence specified in the warrant.[52] Moreover, if a different agency wishes to search the seized data for a different purpose, it must obtain a separate warrant for that search.[53] The fact that the government lawfully obtained and is in possession of the computer's contents does not give it license to conduct any search it wishes.

Compounding the constitutional harm of back door searches, the government has not fully and consistently complied with its statutory and constitutional obligation to notify criminal defendants when it uses evidence "obtained or derived from" Section 702 surveillance. Before 2013, the government interpreted "obtained or derived from" so narrowly that it notified no one. In the nine years since the government's approach reportedly changed,[54] the government has provided notification in fewer than ten known cases, even though the PCLOB reports that the FBI searches Section 702 every time it conducts a national security investigation and there have been nearly two thousand terrorism and national security convictions during this time.[55]

There is reason for concern that the government is avoiding its notification requirements by engaging in "parallel construction" — i.e., recreating the Section 702 evidence using less controversial means.[56] This is a well-documented practice that the government has used in a

---

should be evaluated as a whole, it is difficult to see how any scheme could pass the reasonableness test if a significant component of the scheme were not justified by any national security interest. This is one of several errors in the FISA Court's 2015 decision upholding the constitutionality of back door searches. *See* Elizabeth Goitein, *The FBI's Warrantless Surveillance Back Door Just Opened a Little Wider,* JUST SEC. (Apr. 21, 2016), https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider/.

[52] *See, e.g.*, United States v. Ganias, 755 F.3d 125 (2d Cir. 2014), *rev'd en banc on other grounds,* 824 F.3d 199 (2d Cir. 2016).

[53] *See* United States v. Hulscher, 2017 WL 657436 (D.S.D. February 17, 2017).

[54] For more background, see Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?*, JUST SEC. (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again.

[55] *See* Brief for the Brennan Ctr. for Justice et al. as Amicus Curiae at 23 n.23, *Wikimedia v. Nat'l Sec. Agency*, No. 22-190 (2022); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2021 at 14 (133 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2020 at 14 (172 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2019 at 14 (181 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2018 at 14 (185 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2017 at 14 (196 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2016 at 14 (210 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2015 at 14 (273 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2014 at 14 (265 guilty dispositions); DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2013 at 60 (290 guilty dispositions).

[56] *See* Toomey, *supra* note 54; John Shiffman and Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans,* REUTERS (Aug. 5, 2013), http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805#X7BeCQSb0GrEDTJX.97.

variety of settings, including foreign intelligence surveillance cases.[57] Attorneys have asked the Department of Justice to share its policies for determining when information is considered to be "derived from" Section 702, but the Department refuses to provide them.

Importantly, opposition to warrantless searches for U.S. person information is not a call to re-build the barriers to cooperation among agencies often attributed to "the wall." Threat information, including threat information that focuses on U.S. persons, can and should be shared among agencies when identified, and the agencies should work together as necessary in addressing the threat. What the Fourth Amendment cannot tolerate is the government collecting information without a warrant with the intent of mining it for use in ordinary criminal cases against Americans. That is why President Obama's Review Group on Intelligence and Communications Technologies — a five-person panel including a former acting director of the CIA (Michael J. Morell) and chief counterterrorism advisor to President George W. Bush (Richard A. Clarke) — unanimously recommended closing the "back door search" loophole by prohibiting searches for Americans' communications without a warrant.[58]

III. Violations of Statutory and Court-Ordered Privacy Protections

The substantive legal restrictions on collecting information about Americans are looser than they have been since before 1978. At the same time, the amount of data available to the government and the capacity to store and analyze that data are orders of magnitude greater than they were during the period of J. Edgar Hoover's worst excesses. History teaches us that this combination is an extraordinarily dangerous one.

To date, there is limited evidence of intentional abuse of foreign intelligence surveillance authorities.[59] But the government's record of non-compliance with statutory, constitutional, and court-ordered requirements is extensive and alarming. Notably, this includes cases in which the government did not detect the non-compliance for years, and external overseers (including the FISA Court) had no way to uncover the incidents in the meantime. Given that these incidents went unreported for years even when the agency was *not* trying to conceal them, it is not clear how overseers would learn about intentional abuses that agency officials were making every effort to hide.

---

[57] *See* Human Rights Watch, *Dark Side: Secrets Origins of Evidence in US Criminal Trials* (Jan. 9, 2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.

[58] *See* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 29 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[59] *See, e.g.*, [Redacted], 402 F. Supp. 3d 45, 78 (FISA Ct. 2018) (noting "[a] small number of cases in which FBI personnel apparently conducted queries for improper personal reasons — for example, a contract linguist who ran queries on himself, other FBI employees, and relatives"); Letter from Dr. George Ellard, Inspector Gen., Nat'l Sec. Agency, to Sen. Charles E. Grassley (Sept. 11, 2013), *available at* http://www.privacylives.com/wp-content/uploads/2013/09/09262013-NSA-Surveillance-09-11-13-response-from-IG-to-intentional-misuse-of-NSA-authority.pdf (detailing 12 instances of intentional abuse of NSA bulk surveillance data, most involving employees searching for information on their romantic partners).

In any event, inadvertent failures to adhere to privacy protections are a concern in their own right, especially when they are as persistent and pervasive as they are here. They can result in Americans being investigated without proper legal basis; sensitive information falling into the hands of people who could misuse it; information being improperly retained and thus subject to hacking or theft; and a range of other harms. The knowledge that information is being improperly collected, stored, and accessed also creates a chilling effect on free and open communication[60] — particularly among marginalized communities who are more likely to be the victims of abusive surveillance practices.

A. FBI Violations of Limitations on U.S. Person Queries

Since Section 702 was last reauthorized, it has emerged that the FBI has widely disregarded the modest limits on U.S. person queries imposed by Congress and the FISA Court. There is every reason to believe that these violations have occurred since the program's inception, and no indication that the FBI is putting a stop to them.

In the vast majority of cases, the only substantive restriction on the FBI's use of U.S. person identifiers to query Section 702 data is the standard set forth in its querying procedures. Congress required agencies to develop these procedures when it reauthorized Section 702 in 2018. Although agencies' minimization procedures already had some limits on queries,[61] the

---

[60] After Edward Snowden revealed the NSA's bulk collection program in June 2013, an analysis of Google Trends data showed a significant five percent drop in U.S.-based searches for government-sensitive terms (e.g., "dirty bomb" or "CIA"). A control list of popular search terms or other types of sensitive terms (such as "abortion") did not show the same change. *See* Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (Apr. 29, 2015), *available at* http://dx.doi.org/10.2139/ssrn.2412564. Similarly, after the Associated Press reported on the New York City Police Department's surveillance activities, Muslims reported a decline in mosque attendance and Muslim Student Association participation, as well as a marked reticence to speak about political matters in public places or to welcome newcomers into the community. *See* MUSLIM AMERICAN CIVIL LIBERTIES COALITION (MACLC) ET AL., MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS (2013), *available at* http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[61] For instance, the FBI's 2016 minimization procedures provided that, "[t]o the extent reasonably feasible, authorized users with access to raw FISA-acquired information must design such queries to find and extract foreign intelligence information or evidence of a crime." LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § III.D (Sept. 21, 2016), *available at* https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf. The 2016 minimization procedures for both the CIA and NCTC required queries to be "reasonably likely to return foreign intelligence information, as defined in FISA." WILLIAM BARR, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 4 (Sept. 21, 2016), *available at* https://www.dni.gov/files/documents/icotr/51117/2016_CIA_Section_702_Minimization_Procedures_Se_26_2016.pdf; LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § C.1 (Sept. 21, 2016) , *available at* https://www.dni.gov/files/documents/icotr/51117/2016_NCTC_Section_702_Minimizatio_Procedures_Sep_26_2016.pdf.

new requirement clarified that this was a mandatory aspect of minimization and that the constraints must be set forth in detail. The querying procedures must be approved by the FISA Court, and the Court's annual approval of Section 702 surveillance is predicated on compliance with these and other court-approved procedures.

The FBI's querying procedures provide that "[e]ach query of FBI systems [containing raw Section 702 data] . . . must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, or evidence of a crime, unless otherwise specifically excepted in these procedures."[62] This is a fairly low bar, to be sure. Even so, FISA Court opinions issued in recent years show that the FBI has repeatedly failed to meet it.

In an October 2018 opinion, the FISA Court noted that, "[s]ince April 2017, the government has reported a large number of FBI queries that were not reasonably likely to return foreign-intelligence information or evidence of a crime."[63] These included multiple one-off incidents of FBI personnel running U.S. person queries accidentally or for improper personal purposes. (In a frank statement that reveals why limits on access are a poor substitute for adequate limits on collection, the FISA Court commented that it was less concerned about personal misuses of the data, because "[i]t would be difficult to completely prevent personnel from querying data for personal reasons."[64]) They also included several incidents indicative of more systemic problems, including:

- In March 2017, the FBI, against the advice of the FBI's Office of General Counsel, conducted queries using 70,000 identifiers "associated with" people who had access to FBI facilities and systems.
- On a single day in December 2017, the FBI conducted over 6,800 U.S. person queries using Social Security Numbers.
- Between December 7-11, 2017, an FBI official improperly reviewed raw FISA information resulting from 1,600 U.S. person queries.
- On more than one occasion, the FBI conducted dozens of U.S. person queries to gather information about potential informants.[65]

The government told the FISA Court that these errors stemmed from "fundamental misunderstandings by some FBI personnel [about] what the standard 'reasonably likely to return foreign intelligence information' means."[66] This is a remarkable admission, given that the standard essentially carried forward a limitation that had been in place for a decade in the FBI's minimization procedures,[67] and given the government's repeated assurances to the FISA Court

---

[62] [Redacted], 402 F. Supp. 3d 45, 75 (FISA Ct. 2018).
[63] *Id.* at 76.
[64] *Id.* at 78.
[65] *Id*. at 76–7.
[66] *Id*. at 77.
[67] Specifically, the FBI's 2008 minimization procedures provided that, "[t]o the extent reasonably feasible, authorized users must design such queries to find and extract foreign intelligence information or evidence of a crime…" MICHAEL MUKASEY, U.S. DEP'T OF JUSTICE, STANDARD MINIMIZATION PROCEDURES FOR FBI SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

during this time that access to Americans' data was restricted to personnel who were carefully trained in the applicable limits.

The Court expressed "serious concern" about "the large number of queries evidencing a misunderstanding of the querying standard — or indifference to it."[68] The Court posited that the reported violations were likely the tip of the iceberg. It noted that some FBI offices field offices go for periods of two years or more between oversight visits, and ultimately, Justice Department overseers "review only a small portion of the queries conducted."[69] It also observed that "the documentation available to [overseers] lacks basic information that would assist in identifying problematic queries."[70] Given these limitations on existing oversight mechanisms, the Court wrote, "it appears entirely possible that further querying violations involving large numbers of U.S.-person query terms have escaped the attention of overseers and have not been reported to the Court."[71]

The Court was equally disturbed by the FBI's use of "batch queries." The FBI's querying procedures require that "[e]ach query" must be reasonably likely to retrieve foreign intelligence information or evidence of a crime. The government, however, took the position that "an aggregation of individual queries" — also referred to as a "batch query" — "can satisfy the querying standard, even if each individual query in isolation would not be reasonably likely to return foreign-intelligence information or evidence of a crime."[72] So, for instance, if the FBI has information that an employee at a particular company is planning illegal actions, but the FBI has no knowledge of who the employee is, the Bureau would be justified (according to the government's argument) in running queries for *every employee at that company*. The Court rightly expressed skepticism that such an approach could be reconciled with the text of the FBI's querying procedures.

The Court held that the extent of improper querying rendered the FBI's procedures, as implemented, inconsistent with Section 702's "minimization" requirement. It also held that the FBI's practices ran afoul of the Fourth Amendment. Weighing the privacy interests at stake against the government's interests, the Court found the privacy interests to be substantial: "The goal of the Fourth Amendment is to protect individuals from arbitrary governmental intrusions on their privacy…The FBI's use of unjustified queries squarely implicates that purpose: the FBI searched for, and presumably examined when found, private communications of particular U.S. persons on arbitrary grounds."[73] Although the Court found the government's interest in acquiring foreign intelligence information to be "particularly intense," it quoted a decision by the Foreign Intelligence Surveillance Court of Review stating that if "the protections that are in place for individual privacy interests are . . . insufficient to alleviate the risks of government error and

---

§ III.D (Oct. 22, 2008), *available at* https://www.aclu.org/sites/default/files/field_document/2017.5.8_savage-nyt-foia-fbi-2008-09-fisa-standard.pdf.

[68] [Redacted], 402 F. Supp. 3d 45, 78 (FISA Ct. 2018).

[69] *Id*. at 79.

[70] *Id.*

[71] *Id*. at 79–80.

[72] *Id*. at 81.

[73] *Id.* at 89.

abuse, the scales will tip toward a finding of unconstitutionality."[74] The Court concluded: "Here, there are demonstrated risks of serious error and abuse, and the Court has found the government's procedures do not sufficiently guard against that risk."[75]

To cure these defects, the Court recommended — and the FBI ultimately adopted, after the government's unsuccessful appeal to the Foreign Intelligence Surveillance Court of Review — a remedy proposed by *amici*. Specifically, any time the FBI runs a U.S. person query that returns Section 702 data, FBI personnel are not permitted to view the content (although they may still view non-content "metadata") unless they first document the reasons why they believed the query was likely to return foreign intelligence or evidence of a crime.

When the Court next signed off on Section 702 surveillance, however, there had been no improvement. In a December 2019 opinion, the Court observed that "there still appear to be widespread violations of the querying standard by the FBI."[76] The list of violations compiled in the Court's opinion includes (among others) queries of college students participating in a "Collegiate Academy"; queries of police officer candidates; and one case in which the FBI ran 16,000 U.S. person queries — for a purpose that remains classified — of which only seven were justified.[77] The Court nonetheless approved Section 702 for another year, reasoning that the FBI had not been given sufficient time to fully implement the remedy previously imposed by the Court.

A year later, in a November 2020 opinion, the FISA Court reported that "the FBI's failure to properly apply its querying standard" was "more pervasive than … previously believed."[78] The targets of the improper queries included people who came to the FBI to perform repairs; victims who approached the FBI to report crimes; and business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy."[79] Moreover, when conducting batch queries, the FBI had failed in many cases to document the justifications for the queries, due to a "system failure [that] went undetected or unreported for nearly a year."[80] As the Court noted, "[t]he failure to require a written justification for a bulk query involving a U.S.-person query term is particularly concerning given the indiscriminate nature of such queries."[81]

Once again, however, the Court approved Section 702 surveillance. This time, it reasoned that government office closures resulting from the Covid-19 pandemic had prevented the

---

[74] *Id*. at 86–7 (quoting *In re* Directives Conducted Pursuant of Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008)).
[75] *Id*. at 88.
[76] [Redacted], at 65 (FISA Ct. Dec. 6, 2019), *available at* https://repository.library.georgetown.edu/bitstream/handle/10822/1060343/gid_c_00282.pdf?sequence=1&isAllowed=y.
[77] *Id.* at 66–7.
[78] [Redacted], at 39 (FISA Ct. Nov. 18, 2020), *available at* https://repository.library.georgetown.edu/bitstream/handle/10822/1061209/gid_c_00289.pdf?sequence=1&isAllowed=y.
[79] *Id*. at 39–40.
[80] *Id*. at 51.
[81] *Id.* at 50.

oversight necessary to determine whether the new training and record-keeping requirements implemented by the FBI in late 2019 and early 2020 had made any difference. As the Court stated, "While the Court is concerned about the apparent widespread violations of the querying standard… it lacks sufficient information at the time to assess the adequacy of the FBI system changes and training, post-implementation."[82]

The Court's repeated excuses for the FBI's behavior amount to an admission that the FBI's systems, procedures, and training have been inadequate since Section 702's inception — which means the improper queries have likely occurred from the outset. Throughout this period, the government has touted these same systems, procedures, and training, portraying them as robust protections for Americans' privacy. The notion that the FBI simply needs a little more time to get its house in order is far too dismissive of the constitutional rights that have been violated for at least five years (and probably closer to fourteen). Moreover, there is little reason to expect that additional record-keeping requirements or training sessions will solve the problem.

Indeed, even the most robust procedural protection of all — a warrant requirement — has proven insufficient to constrain the FBI. In 2018, Congress required the FBI to obtain a probable-cause order from the FISA Court before reviewing the results of U.S. person queries in a small subset of cases, i.e., predicated criminal investigations unrelated to national security.[83] According to the ODNI's statistical transparency reports, this requirement has been triggered on more than 100 occasions over the past four years.[84] This figure is almost certainly a substantial undercount, given that it measures the number of days on which queries that require warrants were performed rather than the number of queries. Incredibly, the FBI did not obtain a FISA Court order in a *single one* of those cases.

Addressing this issue in its December 2019 opinion, the FISA Court noted that "*[s]ome* violations resulted *in part* from the manner in which FBI systems displayed information in response to queries" (emphasis added).[85] Specifically, systems would display query results in a summary field that showed 100 characters of text around the query term within the records identified as responsive to the query. Of course, FBI agents still could have obtained FISA Court orders before opening the results to see more than the 100 characters. According to the Court, however, "FBI personnel are known to have taken further steps in response to such displays (e.g., opening "products" containing contents returned by a query), thereby accessing Section 702-acquired contents beyond what was initially displayed to them."[86] In any event, this feature of the FBI systems did not account for all of the violations.

---

[82] *Id.* at 44.
[83] 50 U.S.C. § 1881a(f)(2)(A). The PCLOB has reported that the FBI routinely performs U.S. person queries at the "assessment" stage, which happens before the FBI has sufficient information to open a predicated investigation. PCLOB 702 REPORT, *supra* note 5, at 59.
[84] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2020 at 21 (Apr. 2021); OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 16, at 22.
[85] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 76, at 69.
[86] *Id*. at 70.

It is stunning that the FBI has ignored a statutory warrant requirement for four years, and equally astonishing that the FISA Court has permitted Section 702 surveillance to continue despite this fact. Promises that the FBI will fix these violations in the future ring empty given its long record of systemic non-compliance. At a minimum, because the Court itself has determined that the FBI's non-compliance with querying limitations renders the surveillance unreasonable under the Fourth Amendment, it seems clear that the surveillance — or, at least, the FBI's access to Section 702-acquired data — should be suspended until the FBI can prove that its queries of already-collected data are fully compliant with the law and the Constitution.

B. Other Violations

On multiple other occasions in the past fourteen years, the FISA Court has had occasion to rebuke the government for repeated, significant, and sometimes systemic failures to comply with court orders. These failures took place under multiple foreign intelligence collection authorities (including Section 702) and at all points of the programs: collection, access, dissemination, and retention. It is instructive to review some of the Court's comments in these cases. The following statements are excerpted from nine opinions spanning the years 2009 through 2020:

- "In summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast [Section 215 telephony metadata] collection program have been premised on a flawed depiction of how the NSA uses [the] metadata. This misperception by the FISC existed from the inception its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall [bulk collection] regime has never functioned effectively."[87]
- "The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions . . . to the FISC."[88]
- "[T]he NSA continues to uncover examples of systematic noncompliance."[89]
- "Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures."[90]
- "[U]ntil this end-to-end review is completed, the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation . . . will be the last."[91]
- "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the

[87] *In re* Production of Tangible Things from [Redacted], No. BR 08-13, at 10–11 (FISA Ct. Mar. 2, 2009).
[88] *Id.* at 6.
[89] *Id.* at 10.
[90] *Id.* at 15.
[91] *Id.* at 16.

government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[92]

- "The current application [for pen register/trap and trace data] . . . raises issues that are closely related to serious compliance problems that have characterized the government's implementation of prior FISA orders."[93]
- "As far as can be ascertained, the requirement was simply ignored."[94]
- "Notwithstanding this and many similar prior representations, there in fact had been systematic overcollection since [redacted]. . . . This overcollection . . . had occurred continuously since the initial authorization . . . ."[95]
- "The government has provided no comprehensive explanation of how so substantial an overcollection occurred."[96]
- "[G]iven the duration of this problem, the oversight measures ostensibly taken since [redacted] to detect overcollection, and the extraordinary fact that the NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively."[97]
- "The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection. The government's poor track record with bulk PR/TT acquisition…presents threshold concerns about whether implementation will conform with, or exceed, what the government represents and the Court may approve."[98]
- "As noted above, NSA's record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained… The government has provided no meaningful explanation why these violations occurred, but it seems likely that widespread ignorance of the rules was a contributing factor."[99]
- "Given NSA's longstanding and pervasive violations of the prior orders in this matter, the Court believes that it would be acting well within its discretion in precluding the government from accessing or using such information."[100]
- "[The] cases in which the FBI had not established the required review teams seemed to represent a potentially significant rate of non-compliance."[101]

---

[92] [Redacted], 2011 WL 10945618, at *5 n. 14 (FISA Ct. Oct. 3, 2011).
[93] [Redacted], Docket No. PR/TT [Redacted], at 4 (FISA Ct. [Redacted]), *available at* https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[94] *Id.* at 19.
[95] *Id.* at 20.
[96] *Id.* at 21.
[97] *Id.* at 22.
[98] *Id.* at 77.
[99] *Id.* at 95.
[100] *Id.* at 115.
[101] [Redacted], at 48–49 (FISA Ct. Nov. 6, 2015), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/official-statement/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

- "The Court was extremely concerned about these additional instances of non-compliance."[102]
- "Perhaps more disturbing and disappointing than the NSA's failure to purge this information for more than four years, was the government's failure to convey to the Court explicitly during that time that the NSA was continuing to retain this information . . . ."[103]
- "The Court did not find entirely satisfactory the government's explanations of the scope of [its] segregation errors and the adequacy of its response to them . . . ."[104]
- "[A] non-compliance rate of 85% raises substantial questions about the appropriateness of using [a redacted tool] to query FISA data."[105]
- "At the October 26, 2016 hearing, the Court ascribed the government's failure to disclose those [Inspector General] and [NSA Office of Compliance for Operations] reviews at the October 4, 2016 hearing to an institutional lack of candor on NSA's part and emphasized that this is a very serious Fourth Amendment issue."[106]
- "Beginning in October 2016, while the 2016 Certifications were pending before the FISC, the government reported that NSA had violated that querying prohibition much more frequently than had been previously disclosed."[107]
- "The quarterly reports also revealed that in several of these incidents the CIA or the FBI was responsible for conducting post-targeting content review but did not conduct timely reviews."[108]
- "It must be noted . . . that the government has unjustifiably disregarded the current reporting requirement . . . . It should be unnecessary to state that government officials are not free to decide for themselves whether or to what extent they should comply with Court orders."[109]
- "The government has not reported such instances [of non-compliance] in timely fashion. Rather, they have been reported to the Court belatedly, usually after they were uncovered during oversight reviews."[110]
- "The FBI's handling of the Carter Page applications, as portrayed in the OIG report, was antithetical to the heightened duty of candor . . . . The frequency with which representations made by FBI personnel turned out to be unsupported or contradicted by information in their possession, and with which they withheld information detrimental to their case, calls into question whether information contained in other FBI applications is reliable."[111]
- "[T]he OIG expressed a 'lack of confidence that the Woods Procedures are working as intended' — i.e., 'as a means toward achiev[ing]' the FBI's professed policy 'that FISA

---

[102] *Id.* at 50.
[103] *Id.* at 58.
[104] [Redacted] (FISA Ct. Apr. 26, 2017), *supra* note 43, at 80.
[105] *Id.* at 82.
[106] *Id*. at 19 (internal quotation marks omitted).
[107] [Redacted], 402 F. Supp. 3d 45, 56 (FISA Ct. 2018).
[108] *Id.* at 104.
[109] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 76, at 44–5.
[110] *Id.* at 72.
[111] *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, at 3 (Dec. 17, 2019), *available at* https://www.fisc.uscourts.gov/sites/default/files/MIsc%2019%2002%20191217.pdf.

> applications be "scrupulously accurate."' . . . It would be an understatement to note that such lack of confidence appears well founded. None of the 29 cases reviewed had a Woods File that did what it is supposed to do: support each fact proffered to the Court. For four of the 29 applications, the FBI cannot even find the Woods File . . . . For three of those four, the FBI could not say whether a Woods File ever existed."[112]

A particularly notable Section 702 compliance failure, discussed in the FISA Court's April 26, 2017 opinion, was the NSA's widespread use of U.S. person identifiers to query certain data obtained through upstream collection. The FISA Court had prohibited such queries in 2011, in response to its discovery that the NSA had for years been pulling in substantial numbers of wholly domestic communications by virtue of "abouts" collection. The Court had found the NSA's handling of this data unconstitutional, and the ban on U.S. person queries of upstream data was one of the key remedies adopted to cure the constitutional defect.

In January 2016, however, the NSA Inspector General reported internally that agency analysts were not fully complying with this limitation, based on an examination of three months of audit data from early 2015. The Inspector General and the NSA's Office of Compliance for Operations began studies of other time periods, and "preliminary results [suggested] the problem was widespread during all periods under review."[113] In other words, at no point during the operation of upstream collection — either in the years before the NSA informed the Court that it was collecting wholly domestic communications, or in the subsequent years when this data was supposedly off limits to U.S. person queries — had this surveillance operated within the bounds of the Constitution.

Nonetheless, the NSA waited for several months before informing the FISA Court of the problem, which it blamed on "human error" and "system design issues."[114] The Court chided the government for this "institutional lack of candor."[115] It granted short-term extensions of Section 702 surveillance authority while the government attempted to resolve the issue, but as of late January 2017, "[t]he government still had not ascertained the full range of systems that might have been used to conduct improper U.S.-person queries,"[116] and as of March, "continued to . . . investigate potential root causes of non-compliant querying practices."[117] With no resolution in sight, and with the Court unwilling to certify the program for another year while the problem remained, the NSA made the only possible choice: to halt "abouts" collection for the time being.

The Court's April 2017 opinion also includes a long list of other compliance failures. For instance, between November 2015 and May 2016, no less than *85 percent* of queries using identifiers of U.S. persons targeted under Sections 704 and 705(b) resulted in improper querying

---

[112] *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, at 2 (Apr. 3, 2020), *available at* https://www.fisc.uscourts.gov/sites/default/files/Misc%2019%2002%20Order%20PJ%20JEB%20200403.pdf.
[113] [Redacted] (FISA Ct. Apr. 26, 2017), *supra* note 43, at 19.
[114] *Id.* at 20.
[115] *Id.* at 19.
[116] *Id.* at 21.
[117] *Id.* at 23.

of Section 702 data.[118] The Court also found that the FBI had shared raw Section 702 information with a redacted entity "largely staffed by private contractors," and that "the [redacted] contractors had access to raw FISA information that went well beyond what was necessary" to perform their jobs.[119] And the Court noted that "[r]ecent disclosures regarding [redacted] systems maintained by the FBI suggest that raw FISA information, including Section 702 information, may be retained on those systems in violation of applicable minimization requirements," resulting in "indefinite retention" of some data.[120]

More compliance incidents followed. As recounted in the FISA Court's December 2019 opinion, the NSA determined that it was losing foreign intelligence information as a result of a court-ordered rule that required the agency to use certain technical methods to limit collection of purely domestic communications. Its solution was to disregard the rule. Only when Section 702 was next up for reauthorization did the NSA disclose the violation and ask the Court to rescind the requirement. The Court, in a model of understatement, noted that "the proper course would have been to seek amendment of the procedures earlier, rather than unilaterally deciding to deviate from them."[121] The Court's November 2020 decision also makes reference to a heavily redacted "potential compliance incident" involving NSA that was under investigation by the government.[122]

The most recent revelation of NSA non-compliance came just this week, when the agency responded to a Freedom of Information Act request filed six years ago by releasing a heavily redacted 2016 report of the NSA's Inspector General.[123] The report details how one NSA analyst launched a surveillance project in early 2013 that targeted Americans' communications without a FISA Court order and without a foreign intelligence purpose, in violation of FISA, Executive Order 12333, and multiple agency policies. Despite whistleblowers' complaints, NSA officials allowed the project to continue because — as they explained to the Inspector General — the project was complex and they didn't understand it. This illegal project continued for three years until the Inspector General's office completed its investigation.

Former NSA Director Keith Alexander, commenting on the report's release, asserted that "[w]hen somebody does the wrong thing, we find them, and we hold them accountable."[124] In fact, the Inspector General's report specifically found that oversight by NSA officials was inadequate, and the NSA has refused to answer questions about whether any action was taken against the analyst who developed and ran the illegal program.[125]

---

[118] *Id.* at 82.
[119] *Id.* at 84.
[120] *Id.* at 87–9.
[121] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 76, at 13.
[122] [Redacted] (FISA Ct. Nov. 18, 2020), *supra* note 78, at 37–8.
[123] OFF. INSPECTOR GEN., NAT'L SEC. AGENCY, REPORT OF INVESTIGATION: MISUSE OF SIGINT SYSTEMS (Feb. 12, 2016), *available at* https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rgMApjakmUtM/v0.
[124] Jason Leopold, Katrina Manson & William Turton, *NSA Watchdog Concluded One Analyst's Surveillance Project Went Too Far*, BLOOMBERG (Nov. 1, 2022), https://www.bloomberg.com/news/articles/2022-11-01/nsa-watchdog-concluded-one-analyst-s-surveillance-project-went-too-far.
[125] *Id.*

The long, unbroken string of violations recounted here paints a vivid and unmistakable picture of foreign intelligence surveillance operating outside the constraints of the law. It is unclear whether the violations are occurring because agencies are not putting sufficient effort into compliance, because they lack the technical capability to ensure compliance, or for some other reason. It may be the case that collection programs have become so massive in scope, and the systems for retaining and processing the data so technically complex, that it is simply impossible to achieve consistent compliance with the rules governing their use. Whatever the explanation, the fact that the government's widespread failures to honor privacy protections have been mostly inadvertent is of limited comfort when the government is asking Congress and the public to entrust it with immense quantities of Americans' private data.

IV. The Artificial Distinction Between Section 702 and EO 12333

As a general matter, FISA applies when the government collects foreign intelligence inside the United States or from U.S.-based companies. When the government collects foreign intelligence overseas, it proceeds under Executive Order 12333, unless it is targeting a specific, known U.S. person or intentionally collecting purely domestic communications. There is one caveat to this rule: While FISA is the exclusive means by which the government may conduct "electronic surveillance,"[126] the definition of that term[127] does not cover the collection of many types of records containing communications metadata and other sensitive non-contents information, such as geolocation data. Accordingly, collection of such information inside the United States may also take place under EO 12333.

A geographic limitation on FISA's reach might have made some sense in 1978 (the year of FISA's enactment), when surveillance inside the United States generally meant surveillance of Americans and surveillance overseas generally meant surveillance of foreigners. Today, however, communications are routed and stored all over the world. Indeed, the fact that purely foreign communications may be stored by internet service providers inside the United States — which, under FISA as originally enacted, would have triggered the requirement to obtain a probable-cause order[128] — is one of the main reasons the government sought to "modernize" FISA in 2008 through the enactment of Section 702.

The government notably failed to seek a solution to the other half of this problem: the fact that Americans' communications and other personal data are routinely routed and stored overseas, removing them from FISA's protections and exposing them to EO 12333 surveillance. Particularly when the government engages in bulk collection — i.e., the collection of information without the use of selectors that would identify particular targets — it is almost certain to sweep

[126] 50 U.S.C. § 1812.
[127] 50 U.S.C. § 1801(f).
[128] *See* Ex Parte Brief for Respondents at 8–9, *In re* Directives to Yahoo Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (FISA Ct. Rev. 2008), *available at* https://cdt.org/wp-content/uploads/2014/09/2-yahoo702-governments-ex-parte-merits-brief.pdf (noting that when the government obtains stored emails from an internet service provider, this acquisition is covered by the fourth prong of the definition of "electronic surveillance," which applies to collection inside the United States regardless of the U.S. person status of the communicants).

in Americans' information, including wholly domestic communications, potentially in large amounts. Bulk collection is prohibited under FISA, but it is permitted under EO 12333.

In February of this year, Americans learned that the CIA had been conducting bulk collection programs that pull in an unknown quantity of Americans' data. At the request of Senators Ron Wyden and Martin Heinrich, the CIA released documents pertaining to two reports authored by the PCLOB, titled "Deep Dive I"[129] and "Deep Dive II."[130] The surveillance described in Deep Dive I includes the bulk acquisition of information about financial transactions involving Americans and others. For Deep Dive II, the CIA has disclosed neither what type of information it is collecting in bulk nor for what purpose. However, the CIA's sparse public statements on the program suggest that the collection impacts "Americans who are in contact with foreign nationals,"[131] which implies that this program involves communications records. The two pages of PCLOB staff recommendations released by the CIA show that CIA analysts query the data acquired under this program for information about US persons, and that they do so without recording the justification for the queries — making it virtually impossible to conduct even internal oversight.

Even when EO 12333 surveillance is targeted, it will acquire the communications of Americans in contact with the targets, just as Section 702 surveillance does. The FISA Court has recognized that the collection of communications between foreigners overseas and Americans implicates the Fourth Amendment.[132] Congress clearly shares this understanding and has therefore included minimization and close oversight by the FISA Court as critical elements of Section 702. Although these protections have proven insufficient in practice (as detailed above), they far exceed the protections established by EO 12333, even as supplemented by President Biden's recent executive order.

Two critical distinctions suffice to prove the point. First, under Section 702, the government must submit its targeting, minimization, and querying procedures to the FISA Court on an annual basis, and the Court must find that these procedures — both on paper, and in practice — comport with the statute and the Constitution. The government must report significant instances of non-compliance to the Court and implement any remedies that the Court orders. No such judicial oversight — indeed, no judicial oversight whatsoever — exists for EO 12333 surveillance.

---

[129] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON CIA FINANCIAL DATA ACTIVITIES IN SUPPORT ON ISIL-RELATED COUNTERTERRORISM EFFORTS (accessed Oct. 31, 2022), *available at* https://www.cia.gov/static/63f697addbbd30a4d64432ff28bbc6d6/OPCL-PCLOB-Report-on-CIA-Activities.pdf.

[130] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., RECOMMENDATIONS FROM PCLOB STAFF (accessed Oct. 31, 2022), *available at* https://www.cia.gov/static/f61ca00cbcda9b5d46a04e0b53b5f2b9/OPCL-Recommendations-from-PCLOB-Staff.pdf.

[131] Katie Bo Lillis, *Senators allege CIA collected data on Americans in warrantless searches*, CNN (Feb. 11, 2022), https://www.cnn.com/2022/02/10/politics/cia-data-collection-americans/index.html.

[132] *See, e.g.,* [Redacted] (FISA Ct. Apr. 26, 2017), *supra* note 43, at 61–2 (acknowledging that Section 702 surveillance "implicates interests protected by the Fourth Amendment" insofar as it captures communications to or from Americans).

Second, while the NSA[133] and NCTC[134] have procedures in place that include substantive restrictions on U.S. person queries of EO 12333 data (albeit without any judicial oversight to ensure compliance), there are no meaningful constraints on U.S. person queries by the CIA or FBI. The CIA's EO 12333 procedures allow it to run U.S. person queries for any information "related to a duly authorized activity of the CIA"[135] — a much broader standard than that contained in the agency's Section 702 querying procedures, under which queries "must be reasonably likely to retrieve foreign intelligence information, as defined by FISA."[136] The distinction is even more stark when it comes to U.S. person queries by the FBI. For Section 702 data, such queries "must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, or evidence of a crime."[137] For data obtained under EO 12333, there are no specific restrictions on querying. Rather, under the Attorney General's Guidelines for Domestic FBI Operations, there is simply a general admonition that "[a]ll activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines."[138]

There is no justification for giving lesser protections to Americans' constitutional rights based simply on where the data was obtained. If anything, the privacy implications of EO 12333 for Americans are likely even greater than those of Section 702. The government has acknowledged that the majority of its foreign intelligence surveillance activities take place under

---

[133] DEP'T OF DEFENSE, DOD MANUAL S-5240.01-A, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES GOVERNING SIGNALS INTELLIGENCE INFORMATION AND DATA COLLECTED PURSUANT TO SECTION 1.7(C) OF E.O. 12333 (Jan. 7, 2021), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/Redacted%20Annex%20DODM%205240.01-A(1).pdf.

[134] NAT'L COUNTERTERRORISM CTR., NATIONAL COUNTERTERRORISM CENTER IMPLEMENTATION PROCEDURES FOR THE ODNI INTELLIGENCE ACTIVITIES PROCEDURES APPROVED BY THE ATTORNEY GENERAL PURSUANT TO EXECUTIVE ORDER 12333 (accessed Oct. 31, 2022), *available at* https://www.dni.gov/files/NCTC/documents/news_documents/NCTC_Implementation_Procedures_executed_3_22_21_U_final.pdf.

[135] CENTRAL INTELLIGENCE AGENCY, THE CIA'S UPDATED EXECUTIVE ORDER 12333 ATTORNEY GENERAL GUIDELINES 6 (accessed Oct. 31, 2022), *available at* https://www.cia.gov/static/100ea2eab2f739cab617eb40f98fac85/Detailed-Overview-CIA-AG-Guidelines.pdf.

[136] WILLIAM BARR, U.S. DEP'T OF JUSTICE, QUERYING PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § IV.A (Sept. 16, 2019), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_CIA%20Querying%20Procedures_10.19.2020.pdf.

[137] WILLIAM BARR, U.S. DEP'T OF JUSTICE, QUERYING PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § IV.A.1 (Sept. 16, 2019), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_FBI%20Querying%20Procedures_10.19.2020.pdf.

[138] U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 13 (accessed Oct. 31, 2022), *available at* https://www.justice.gov/archive/opa/docs/guidelines.pdf.

EO 12333.[139] Accordingly, it reasonable to expect that there is more "incidental" collection of Americans' information under EO 12333 than under Section 702, even when such surveillance is targeted. And, of course, bulk collection has the potential to sweep in Americans' data in amounts that far exceed what normally occurs during targeted surveillance.

V. Projects PCLOB Should Undertake

After fourteen years of Section 702 surveillance operating in violation of the statute, the Constitution, and the legitimate privacy expectations of Americans, it is time for Congress to reform Section 702. In many cases, the necessary reforms are clear; these are discussed in Part VI. Nonetheless, concrete information about the impact of Section 702 on Americans would help frame the debate over reauthorization. In addition, certain information regarding targeting practices and the use of Section 702 for cybersecurity investigations would assist in developing appropriate reforms.

The PCLOB should undertake three projects designed to elicit information on these matters. In its previous investigation of Section 702, culminating in a 191-page report issued in 2014, the PCLOB was remarkably successful in securing the declassification of extensive information about the program's workings. That information continues to inform the public debate over Section 702 today. The PCLOB can perform a similar service here — and can enhance its own ability to issue substantive recommendations — with respect to key aspects of Section 702 surveillance that remain obscure.

A. Obtain Estimate of the Scope of "Incidental" Collection

The government has resisted calls to produce an estimate of how many communications involving a U.S. person are collected under Section 702. However, that is no reason to abandon this important inquiry. Circumstances have changed since Section 702 was last reauthorized. There is a new administration in place, including a Director of National Intelligence who has pledged to prioritize transparency.[140] In addition, computer scientists have proposed a new solution to the problem of how to generate such an estimate without compromising personal privacy.

It is important to bear in mind that lawmakers have requested an *estimate* of the scope of incidental collection — not an exact number. Surely, if our national security depended on the intelligence community producing a rough approximation of Section 702's impact on Americans, it would be produced. Even if all the government could provide was an order of magnitude (e.g., "millions" or "tens of millions"), that would richly inform the debate over Section 702 by

---

[139] Nat'l Sec. Agency, *Legal Fact Sheet: Executive Order 12333* (Jun. 19, 2013), *available at* https://www.aclu.org/sites/default/files/field_document/Legal%20Fact%20Sheet%20Executive%20Order%2012333_0.pdf.

[140] *Nomination of Avril Haines to be the Director of National Intelligence, Hearing Before the S. Comm. on Intelligence*, 117th Cong. 2 (Jan. 19, 2021) (statement of Avril Haines), *available at* https://www.intelligence.senate.gov/sites/default/files/documents/os-ahaines-011921.pdf.

helping to dispel the misconception that the term "incidental" has created among lawmakers and the American public.

The PCLOB should work with the intelligence community to identify and implement a method for generating this estimate. The estimate should be made public before the deadline for reauthorization. As noted above, if the government itself has literally *no* sense of how many Americans' communications it is collecting — and no way to acquire such a sense — Congress should reconsider whether to entrust the government with this powerful authority.

B. Investigate Targeting Decisions

As discussed above, the statutory restrictions on the permissible targets Section 702 surveillance are minimal, given FISA's expansive definition of "foreign intelligence information." Moreover, the legitimate objectives of surveillance identified in the recent executive order do not necessarily translate into a smaller pool of surveillance targets. The scope of permissible targets significantly impacts Americans' civil liberties, as it determines the breadth of "incidental" collection. The PCLOB accordingly should undertake an investigation of Section 702 targeting decisions with an eye toward recommending reforms that would narrow collection.

One reform that has been recommended by multiple organizations, including the Brennan Center, is to require the government to have a reasonable belief, based on specific and articulable facts, that targets are foreign powers (FP) or agents of foreign powers (AFP), as defined in FISA. (This would still be a lower bar than the pre-Section 702 requirement, under which the FISA Court had to find probable cause that each target was a FP/AFP.) To assess the likely impact of such a change, the PCLOB should work with the relevant agencies to determine what proportion of Section 702 targets, if any, is comprised of persons who do *not* qualify as FPs/AFPs. This will likely involve sampling, as analyzing more than 200,000 targets might not be feasible.

If analysis of the sample indicates that the vast majority of targets are reasonably suspected to be FPs/AFPs, that suggests that advocates' proposed reform is appropriate and workable. On the other hand, if PCLOB's analysis indicates that a significant percentage of targets do not fall within those definitions, PCLOB should ask agency officials to articulate why surveillance of these targets, in each instance, is likely to produce information that is directly relevant to one of the twelve objectives identified in President Biden's executive order.[141] If officials cannot satisfactorily answer this question and support their answer with documentation,

[141] In conducting this inquiry, PCLOB should rely on a slightly modified version of the objectives. First, with respect to the goal of "understanding or assessing the capabilities, intentions, or activities of . . . a foreign-based political organization," PCLOB should interpret the term "foreign-based political organization" to exclude civil society non-governmental organizations. Second, the goal of protecting against "transnational criminal threats" should apply only to serious crimes that significantly impact the lives, safety, or property of U.S. persons or the national security of the United States. Third, the goal protecting the integrity of U.S. "government property" should apply only where there is a threat of significant property damage involving a risk to the personal safety of persons on or near the property. *See* Elizabeth Goitein, *The Biden Administration's SIGINT Executive Order, Part I: New Rules Leave Door Open to Bulk Surveillance*, JUST SEC. (Oct. 31, 2022), https://www.justsecurity.org/83845/the-biden-administrations-sigint-executive-order-part-i-new-rules-leave-door-open-to-bulk-surveillance/.

then those targets should be considered inappropriate. If, however, officials are able to make such a showing, PCLOB should identify the *narrowest* substantive criteria that would capture the non-FPs/AFPs (or categories of non-FPs/AFPs) in question.[142] These can then serve as the basis for a legislative reform recommendation.

C. Investigate the Use of Section 702 for Cybersecurity Purposes

The number of U.S. person queries the FBI conducted in 2021 was more than twice that of the previous year. The ODNI explained the fluctuation as follows: "In the first half of the year, there were a number of large batch queries related to attempts to compromise U.S. critical infrastructure by foreign cyber actors. These queries, which included approximately 1.9 million query terms related to potential victims — including U.S. persons — accounted for the vast majority of the increase in U.S. person queries conducted by FBI over the prior year."[143]

Although this statement was intended to allay concerns, it raises alarm bells. In no domestic cybersecurity investigation could the FBI obtain warrants to search 1.9 million Americans' communications simply because they might be victims of the crime. The fact that these Americans' communications may already have been collected through Section 702 does not change the privacy calculus. Even if the search is performed only to identify malicious code embedded in the victims' communications, the result is to expose their personal information to manual review. As Professor Orin Kerr has explained, collection constitutes a seizure, while querying constitutes a search — separate Fourth Amendment events, each of which constitutes a distinct intrusion on privacy.[144]

The PCLOB should investigate how Section 702 is used for cybersecurity purposes,[145] and the degree to which cybersecurity investigations result in extensive targeting or querying of persons not suspected of any wrongdoing. The risk of overbroad surveillance is particularly high in such investigations; as noted above, protecting cybersecurity could in theory justify constant monitoring of the Internet. The role of the PCLOB, however, is to ensure that the government's

---

[142] Under this approach, the *broadest* possible criterion would be a reasonable likelihood that the target is communicating information that is directly relevant to one of the legitimate objectives. Such a criterion, general as it is, would provide an additional constraint on the standard currently set forth in NSA targeting procedures — i.e., "[T]he targeted is expected to possess, receive, and/or is likely to communicate foreign intelligence information" concerning one of the foreign powers or territories identified in the agency's certifications. WILLIAM BARR, U.S. DEP'T OF JUSTICE, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 4 (Oct. 19, 2020), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Targeting%20Procedures_10.19.2020.pdf.

[143] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 16, at 20.

[144] Orin Kerr, *The Fourth Amendment and querying the 702 database for evidence of crimes*, WASH. POST (Oct. 20, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/10/20/the-fourth-amendment-and-querying-the-702-database-for-evidence-of-crimes/.

[145] The Brennan Center recognizes that the PCLOB's statutory mandate is to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties. Much like Section 702 itself, cybersecurity sometimes involves terrorism and sometimes does not. It therefore should be understood to fall within the PCLOB's jurisdiction.

efforts to keep the nation safe are balanced with the need to protect privacy and civil liberties. The query numbers reported by ODNI suggest that the government is not striking the right balance in this area.

The PCLOB should release a public report with its findings. One goal of the investigation should be to inform the PCLOB's recommendations for reforming targeting and U.S. person query practices, as discussed in Part VI.A & B. In developing any recommendations that relate specifically to cybersecurity investigations, the PCLOB should consult with experts in the field of privacy and technology as well as relying on its own staff technologists. Conducting this investigation and, if necessary, issuing cybersecurity-specific reform recommendations might well require hiring additional staff with technological expertise.

VI. Reforms that PCLOB Should Recommend

There are several reforms that would go far toward mitigating the privacy risks posed by Section 702, while retaining the core functionality of the statute: the ability of the government to conduct warrantless surveillance of foreigners overseas who may pose a threat to the U.S. or its interests. These reforms include narrowing the scope of Section 702 collection; shoring up protections for "incidentally" acquired U.S. person information by requiring agencies to obtain a warrant, court order, or subpoena before running U.S. person queries of Section 702 data, and by placing stricter limits on retention; modernizing FISA by establishing basic rules and requiring FISA Court oversight for EO 12333 surveillance; and increasing transparency and accountability in the operations of Section 702 and EO 12333. Given the troubled history of Section 702 surveillance, the PCLOB should recommend that Congress make these changes as a precondition to reauthorization of the statute.

A. Narrow the Scope of Collection

Congress should narrow the scope of permissible Section 702 targets, which will in turn reduce the volume of "incidental" collection and increase the likelihood of a U.S.-EU data-sharing agreement withstanding European courts' scrutiny. Currently, the statute allows the government to target anyone reasonably believed to be a foreigner overseas, as long as the purpose of collection is to acquire information "that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States."[146] Although President Biden's recent executive order further restricts surveillance by defining legitimate objectives, those objectives may be expanded in secret or revoked by a future president, and they do not necessarily limit the scope of collection.

The PCLOB should recommend two measures in this area. First, subject to the findings of the investigations proposed above, it should recommend that Congress require the government to have a reasonable belief, based on specific and articulable facts, that the target of surveillance is a foreign power or an agent of a foreign power, as broadly defined in FISA. The FP/AFP determination would be an internal one; it would not have to be submitted to the FISA Court for

[146] 50 U.S.C. § 1801(e)(2).

case-by-case approval or meet a "probable cause" standard. However, Congress should require the FISA Court to review a sample of targeting decisions as part of its annual approval process.

Second, in addition to imposing a FP/AFP requirement, Congress should codify the legitimate objectives identified in President Biden's executive order (with a small number of revisions[147]) and prohibit the adoption of additional objectives without congressional authorization. It also should translate these objectives into constraints on targeting. Specifically, Congress should require the government to have a reasonable belief, based on specific and articulable facts, that surveillance of each target is likely to provide information that is directly relevant to one or more of the objectives. The statute should make clear that the absence of information cannot itself be deemed relevant for this purpose — i.e., it is not permissible to target groups or individuals simply to "rule them out" as sources of useful information.

Congress also should codify the current cessation of "abouts" collection. This type of surveillance greatly increases the chances of pulling in wholly domestic communications, not to mention other completely innocent communications between people who are not themselves permissible targets of surveillance. Moreover, although "abouts" collection poses uniquely significant risks to privacy, it was a relatively small part of the upstream program, which itself comprises less than one tenth of Section 702 collection.[148] This is clearly a situation in which the privacy risks outweigh the benefits — a point the NSA effectively acknowledged when it stopped "abouts" collection in April 2017.[149]

B. Shore Up Protections for "Incidentally" Acquired U.S. Person Information

Narrowing the scope of surveillance will reduce the amount of "incidental" collection of Americans' communications that can take place, but it will not and cannot eliminate "incidental" collection altogether. It is thus critical that Congress breathe life into its statutory command to agencies to "minimize" the retention, use, and sharing of Americans' information acquired through Section 702 surveillance.

First and foremost, the PCLOB should recommend that Congress require all government agencies to obtain a warrant or a Title I FISA Court order before using U.S. person identifiers to query the contents of communications or other Fourth Amendment-protected information (such as geolocation data) obtained under Section 702. This would close the loophole that currently allows the government to read Americans' e-mails and listen to their phone calls without any factual predicate to suspect wrongdoing, let alone a warrant. What makes the warrantless surveillance lawful in the first instance is the government's certification that it is targeting *only* foreigners. That representation becomes a semantic sleight of hand when the government

---

[147] See *supra* note 141 and accompanying text.
[148] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).
[149] *See* Nat'l Sec. Agency, *NSA Stops Certain 702 "Upstream" Activities* (Apr. 28, 2017), *available at* https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml ("NSA previously reported that, because of the limits of its current technology, it is unable to completely eliminate 'about' communications from its upstream 702 collection without also excluding some of the relevant communications directly 'to or from' its foreign intelligence targets. That limitation remains even today. Nonetheless, NSA has determined that in light of the factors noted, this change is a responsible and careful approach at this time.").

simultaneously adopts procedures allowing it to search the data for particular Americans' communications.

Section 702 surveillance also can result in the "incidental" collection of other types of sensitive data that do not receive full Fourth Amendment protection but that Congress has chosen to protect by statute. Depending on the data in question, the government may be required to obtain a court order (e.g., under 18 U.S.C. §2703(d) or Section 215 of the U.S.A. Patriot Act[150]) or a subpoena (e.g., under §2703(c)(2) or with a National Security Letter) to obtain it. Before performing a U.S. person query of such data, agencies should be required to follow the legal process that would apply if the agencies were collecting the data in the first instance.

The FBI has pointed out that its databases contain information from multiple sources, and other agencies may also conduct federated searches that run against multiple data sets. Section 702 data, however, is specially tagged to enable compliance with notification requirements as well as legal limitations on who may access it. Currently, if an FBI agent performs a query that returns Section 702 data, the agent is notified of its 702 status. The systems could instead be configured not to return Section 702 data at all, unless the agent enters into the system a certification, accompanied by supporting documentation, that one of two conditions is met: (1) the query term is associated with someone reasonably believed to be a foreigner overseas, or (2) the government has obtained the required warrant, court order, or subpoena.

Indeed, with or without a warrant requirement, the system should be configured not to return Section 702 data unless agents, at the time they perform the query, enter a certification and supporting documentation indicating that they have complied with the applicable restrictions. It is unclear whether this technical barrier will succeed in preventing violations of querying limits. What is clear is that nothing short of such a barrier has any chance of doing so. The record establishes that if a query returns Section 702 information in the first instance, FBI agents will frequently access that information regardless of any rules prohibiting such access.

Based on the fact that the FBI ran 1.9 million U.S. person queries relating to potential victims of cyberattacks in 2021, the government will likely argue that a warrant requirement would be unworkable for cybersecurity investigations. If a search of non-contents information could suffice in these instances, however, agencies could proceed with something less than a warrant. In any event, as part of the proposed investigation into the uses of Section 702 for cybersecurity purposes, the PCLOB should thoroughly probe any claim of unworkability. For queries of communications content and other Fourth Amendment-protected information, an exception to the warrant requirement should be made only if there is an applicable exemption under Fourth Amendment jurisprudence. In addition, any such exception — along with any exception from the court order/subpoena requirement when accessing other types of sensitive data — should be as narrowly drawn as possible, and it should be combined with protections to ensure that non-pertinent content is not subject to manual review.

---

[150] Although Section 215 expired in 2020, it is still available for investigations commenced before the provision expired, as well as investigations into actions that took place before the expiration. *See* USA Patriot Act Improvement and Reauthorization Act, Pub. L. 109-177, 109th Cong. § 102(b)(2) (2005) (as amended by Pub. L. 116-69, 116th Cong. § 1703(a) (2019)).

In addition to these limits on querying, the PCLOB should recommend that Congress add specificity to its definition of "minimization." In the absence of objective statutory criteria, there has been a predictable steady slide toward wider sharing of raw data, greater access to the data by agency personnel, and more exceptions to retention limits. On retention in particular, Congress should clarify that keeping Americans' information for five years, and for even longer in cases where that information has been reviewed and no determination of its status has been made, is not "minimization." Congress should specify that all information not subject to a "litigation hold" shall be destroyed within three years of the authorization for the acquisition, unless it has been reviewed and determined to be foreign intelligence or evidence of a crime.[151]

C. Modernize FISA by Establishing Basic Rules and Requiring FISA Court Oversight for Executive Order 12333 Surveillance

The fact that EO 12333 surveillance is subject to almost no legislative limits and no judicial oversight is a constitutionally untenable anachronism, rooted in modes and methods of communication that no longer exist. Overseas surveillance today — whether targeted or in bulk — results in the collection of Americans' communications and other personal information, almost certainly in massive amounts. And there are holes in FISA's coverage that allow the government to target Americans under EO 12333 and collect sensitive non-contents information within the United States. The Supreme Court has made clear that the Constitution "most assuredly envisions a role for all three branches [of government] when individual liberties are at stake."[152] That is undeniably the case here.

The PCLOB should recommend that Congress bring certain aspects of EO 12333 surveillance within FISA. Reauthorization of Section 702 is the best vehicle for accomplishing this. After all, the primary distinction between Section 702 surveillance and EO 12333 surveillance is the location of the collection (or of the companies from which the information is collected), and that has become a distinction without a difference when it comes to Americans' privacy. Any reauthorization of Section 702 should recognize this reality and address EO 12333 surveillance as well.

As a threshold matter, Congress should provide that existing FISA authorities constitute the exclusive means by which the government may conduct any type of foreign intelligence collection (not just "electronic surveillance") that targets U.S. persons, obtains wholly domestic communications, takes place inside the United States, or obtains information from U.S. companies. This would prevent the government from evading FISA's legal processes for

---

[151] In its review of the NSA's bulk collection program, the PCLOB concluded that the collected metadata began to lose its usefulness after three years. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., 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 170 (2014), *available at* https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf. It seems likely that this would also be true for the data obtained under Section 702. Of course, information that has been reviewed and determined to constitute foreign intelligence information or evidence of a crime could be retained for longer periods.

[152] Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004).

obtaining sensitive non-contents information by purchasing that information from data brokers or employing similar workarounds.[153] Congress should then establish basic rules for foreign intelligence collection that does not target U.S. persons or obtain wholly domestic communications, that takes place outside the United States, and that does not involve collection from U.S. companies — collection that currently takes place solely under EO 12333.

The first such rule should be to prohibit bulk collection. The dangers of bulk collection are discussed in Part IV. In brief, as the Court of Justice for the European Union has recognized, bulk collection cannot be reconciled with respect for the privacy rights of foreign nationals. It also opens the door to the "incidental" collection of vast quantities of Americans' personal data, including purely domestic communications and related records. Notably, even though Section 702 has a targeting requirement, the intelligence community has consistently described it as one of the most effective tools in its arsenal; the government has never suggested that the targeting requirement makes Section 702 less effective or results in the loss of vital intelligence.

Next, Congress should address the permissible targets of EO 12333 surveillance. Congress should codify the legitimate objectives set forth in President Biden's recent executive order (with modifications[154]) and require the government to have a reasonable belief, based on specific and articulable facts, that surveillance of each target is likely to produce information directly relevant to one or more objectives. Congress also should specify that, unless the surveillance is highly unlikely to result in the acquisition of U.S. person information, the target must be a foreign power or agent of a foreign power.

As for U.S. person information "incidentally" collected under EO 12333, there is no principled justification for giving this information less protection than similar information "incidentally" acquired through Section 702. In both cases, Congress should require agencies to obtain a warrant, court order, or subpoena to perform a U.S. person query, depending on the type of data being queried. And Congress should tighten the existing statutory limits on retention of incidentally-collected EO 12333 data — the only aspect of EO 12333 surveillance that has ever been made subject to legislation[155] — by changing the retention period from five years to three years and eliminating the many exemptions.

Finally, surveillance activities under EO 12333, with the exception of activities that are highly unlikely to result in the acquisition of U.S. person information, should be subject to oversight by the FISA Court. When it comes to protecting and preserving Americans' constitutional rights, judicial review is indispensable. The fact that the government has been able to collect, store, and access Americans' communications for decades without the possibility of judicial review in any forum is a glaring departure from the rule of law and constitutional principles.

---

[153] *See Digital Dragnets: Examining the Government's Access to Your Personal Data, Hearing Before the H. Comm. on the Judiciary*, 117th Cong. (Jul. 19, 2022) (testimony of Elizabeth Goitein), *available at* https://docs.house.gov/meetings/JU/JU00/20220719/115009/HHRG-117-JU00-Wstate-GoiteinE-20220719.pdf.
[154] See *supra* note 141 and accompanying text.
[155] *See* Intelligence Authorization Act for Fiscal Year 2015, Pub. L. 113-293, 113th Cong. § 309 (2014).

EO 12333 surveillance activities affecting U.S. persons should be authorized by the FISA Court on an annual basis, in a manner similar to Section 702 surveillance. Court approval of such surveillance activities would be contingent on a finding that they comport with FISA (as amended), the Constitution, and the relevant executive orders and agency policies. Agencies should be required to report incidents of non-compliance to the FISA Court immediately upon detection and implement any remedies the Court may order. The government should be required to conduct declassification reviews of significant FISA Court opinions and make them public, with redactions as necessary to protect properly classified information.

These changes will help bring FISA fully into the twenty-first century. In 2007 and 2008, the government observed that changes in technology had resulted in purely foreign communications being stored in the United States, forcing the government to obtain a FISA Court order to collect them. But of course, the converse was true as well: Those same changes in technology meant that Americans' communications were being routed and stored overseas in a way that stripped them of FISA's protections. The government sought and obtained a (markedly overbroad) solution to the first half of the problem. Congress must now address the second half, however belatedly. The PCLOB should urge Congress to complete the unfinished business of modernizing FISA by bringing EO 12333 surveillance that affects Americans within its reach.

D. Increase Transparency and Accountability

The PCLOB should recommend that Congress enact various reforms to increase the transparency and accountability of Section 702 and EO 12333 surveillance.

1. Require Reporting on U.S. Person Queries, Additional Reporting on EO 12333 Surveillance, and an Estimate of Incidental Collection Under Section 702

To ensure informed decision-making by lawmakers and the public, more information is needed about the impact of Section 702 and EO 12333 surveillance on Americans. The PCLOB should recommend three reforms in this area.

First, Congress should require *all* agencies that are authorized to perform U.S. person queries, including the FBI, to report how many times they perform such queries on an annual basis. This year, the government voluntarily reported how many U.S. person queries of Section 702 data it conducted in calendar years 2020 and 2021. Congress should make clear that continued reporting of this number is mandatory, and it should extend this requirement to U.S. person queries of information acquired under EO 12333.[156] This obligation should remain in place even if Congress enacts a warrant requirement for U.S. person queries. Lawmakers and the public need this information to understand and evaluate the impact on Americans of surveillance authorities that are nominally directed at foreigners overseas.

[156] Responsibly tracking how U.S. person information acquired under EO 12333 is maintained and accessed might require a reconfiguration of existing data systems. If so, this requirement could be phased in over a reasonable time period.

Second, assuming Congress brings aspects of EO 12333 surveillance under FISA, it should extend existing Section 702 reporting requirements to such surveillance. In particular, the government should report on FISA Court adjudications of EO 12333 surveillance activities (50 U.S.C. § 1873(a)); numbers of targets and queries (50 U.S.C. § 1873(b)(2)); and numbers of notifications in criminal proceedings, as discussed below (50 U.S.C. § 1873(b)(4)).

Third, if intelligence agencies refuse to work with the PCLOB to develop an estimate of how many Americans' communications are obtained under Section 702, the PCLOB should recommend that Congress require the government to provide such an estimate. As noted above, the FBI claimed for years that there was no workable way to count how many U.S. person queries it performs. But after Congress required the Bureau to keep records of such queries, and after the FISA Court made clear that the FBI could not dodge this requirement, the FBI produced the number.

2. Remove Barriers to Review by Regular Article III Courts

The PCLOB should recommend that Congress address the barriers that are blocking legal challenges to unlawful foreign intelligence surveillance.

Even though Congress clearly intended for defendants to be able to challenge the use of Section 702-derived evidence in criminal cases, the government's notification policies are thwarting this intent. Congress should clarify that evidence is "derived" from Section 702 surveillance if the government would not otherwise have possessed this evidence, regardless of any claim that the evidence is attenuated from the surveillance, would inevitably have been discovered, or was subsequently reobtained through other means.

Congress also clearly intended for civil lawsuits to serve as a means to challenge electronic surveillance activities. Two doctrines are frustrating this intent: standing and the state secrets privilege. With respect to standing, Congress should specify that a person has standing to bring a civil lawsuit if she has a reasonable basis to believe her information has been (or will be) acquired, and if she has expended (or will expend) time or resources in an attempt to avoid acquisition. With respect to the state secrets privilege, Congress should amend section 1806(f) of FISA — which governs courts' review of national security information in electronic surveillance cases — to clarify that this subsection displaces the normal operation of the privilege. Such clarification is needed in light of the Supreme Court's recent ruling in *FBI v. Fazaga*,[157] which held that section 1806(f) does not displace the privilege — a holding that will effectively nullify 1806(f)'s application to civil lawsuits and stymie accountability for unlawful surveillance.[158]

Finally, Congress should ensure that criminal defendants and civil plaintiffs are able to bring challenges when they are victims of unlawful EO 12333 surveillance. To that end, Congress should require the government to notify parties to legal proceedings when it intends to

---

[157] 142 S. Ct. 1051 (2022).

[158] *See* Elizabeth Goitein, *The State Secrets Sidestep:* Zubaydah *and* Fazaga *Offer Little Guidance on Core Questions of Accountability*, CATO S. Ct. Rev. (2022): 193–225, *available at* https://www.cato.org/sites/cato.org/files/2022-09/Supreme-Court-Review-2022-Chapter-8.pdf.

introduce evidence obtained or derived from EO 12333 surveillance (using the above definition of "derived"). It should apply the criteria for standing in Section 702 challenges to EO 12333 challenges. And it should extend the reach of section 1806(f) to proceedings where EO 12333 surveillance is at issue.

3. Improve the functioning of the FISA Court

The PCLOB should recommend that Congress enact the reforms to FISA Court proceedings set forth in the "Lee-Leahy" amendment — an amendment to the USA Freedom Act Reauthorization Act of 2020 offered by Senators Mike Lee and Patrick Leahy.[159] Although Congress failed to pass the reauthorization bill, the amendment passed by an overwhelming bipartisan vote of 77-19.[160]

The amendment seeks to ensure that the panel of *amici* established in the USA Freedom Act provide the FISA Court with a perspective other than the government's —including a presentation of any privacy and civil liberties concerns — in the cases where such a perspective is most needed; that *amici* have access to the materials they need to do their job; that the government has court-approved procedures in place to ensure the accuracy of its submissions to the FISA Court; and that the government informs both the FISA Court and *amici* of any exculpatory evidence in its possession. There is no legitimate argument against such basic accountability-enhancing measures, which is why the amendment received such a strong showing of support in 2020.

***

An important caveat is in order. While reforms that promote transparency and accountability are critical, they are not a substitute for limiting the scope of Section 702 surveillance, shoring up privacy protections for Americans whose communications are "incidentally" collected, and establishing basic rules for EO 12333 surveillance. The most stringent of oversight provisions cannot justify amassing the personal data of ordinary, law-abiding private citizens. Nor can they legitimize the warrantless searching of Americans' phone calls and e-mails. Procedural protections are only as good as the substantive rights and limitations they enforce. That is why Congress should reform Section 702 to bolster those rights and limitations while preserving the core of the statute: warrantless surveillance of foreigners who pose a threat to our nation.

Conclusion

Since Section 702 was last reauthorized, it has become increasingly apparent that its impact on Americans is anything but "incidental." Intelligence agencies are leveraging this authority on a systemic basis to access Americans' communications and other personal information in ways that violate FISA, the Constitution, and court-ordered policies. Congress should not reauthorize Section 702 without sweeping reforms. The PCLOB can play two vital

[159] S. Amdt. 1584, H.R. 6172, 116th Cong. (2020).
[160] *Id.* (as agreed to in Senate, May 13, 2020).

roles in this process: procuring information that will assist in developing reforms, and recommending the changes Congress must enact to bring Section 702 surveillance in line with Americans' constitutional rights and legitimate privacy expectations.

Respectfully submitted,

Elizabeth Goitein
Senior Director
Liberty & National Security Program
Brennan Center for Justice at NYU School of Law
1140 Connecticut Avenue, NW
Eleventh Floor
Washington, DC 20036