TESTIMONY OF

ELIZABETH GOITEIN
SENIOR DIRECTOR, LIBERTY AND NATIONAL SECURITY PROGRAM
BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

HEARING ON

FIXING FISA, PART II

JULY 14, 2023

Introduction

Section 702 of the Foreign Intelligence Surveillance Act ("FISA") allows the government to target foreigners abroad and obtain their communications and other personal information without obtaining an individualized court order. Congress passed the law in 2008 to give our government more powerful tools to address international terrorism and other foreign threats. Consistent with this purpose, the law has been used (according to the government) to obtain information about terrorist plots and the intentions of hostile foreign powers, and — more recently — to gain insight into international fentanyl trafficking activities and investigate foreign threats to cybersecurity.

Needless to say, these activities are not why Section 702 has become so deeply controversial, leading many lawmakers to demand either sunset or reform. If the government were using Section 702 solely to spy on hostile foreign actors, there would be little to debate in this year's reauthorization. The fundamental problem with Section 702 is that the government is also using it as a rich source of warrantless access to *Americans*' communications. According to the government, the FBI conducted more than *two hundred thousand* searches of Section 702 data in 2022 for the purpose of finding Americans' communications and other personal information. This outcome is contrary, not only to the original intent of Section 702 and to basic Fourth Amendment principles, but to Americans' expectations and their trust that Congress will protect their privacy and freedoms.

Moreover, with every new release of an opinion issued by the Foreign Intelligence Surveillance Court ("FISA Court"), 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 a small subset of investigations. As of the most recent statistical report issued by the government, the FBI had *never* complied with this requirement.

Congress should not reauthorize Section 702 without sweeping reforms to ensure that it cannot be used as a domestic spying tool. At a minimum, that means closing the back door search loophole that enables government officials to access Americans' phone calls, text messages, and emails without a warrant. It also means strengthening the law's reverse-targeting prohibition and shoring up minimization requirements, as well as ending so-called "abouts" collection, to more strictly limit the collection, retention, and use of Americans' data. And it means narrowing the scope of surveillance to reduce "incidental" collection while still preserving the ability to target foreigners abroad who pose a threat to the United States.

Addressing the problems with Section 702 will also necessitate reforms to FISA more generally — starting with its judicial review provisions. Despite changes that Congress made in 2015, the FISA Court still hears only from the government in too many cases, and recent audits have shown that the government's submissions to the Court are riddled with errors and omissions. At the same time, the government has thrown up artificial barriers to judicial review

in civil litigation and criminal prosecutions, thwarting Congress's express intent to provide for such review. Congress must strengthen these mechanisms to ensure that the government can be held accountable for violations of the rule of law and Americans' civil liberties.

In addition, Congress should finish the job of modernizing FISA that it began in 2008. Generally speaking, FISA (including Section 702) applies when the collection of information takes place inside the United States or from a U.S. company; overseas surveillance, with few exceptions, is subject to neither legislative limits nor judicial oversight. In the digital era, however, communications and other personal information are often routed or stored in places around the globe. Overseas surveillance can therefore have just as great an impact on Americans' privacy as domestic surveillance, if not greater. Reforms to Section 702 will have limited effect if large swathes of overseas surveillance continue to be carved out of foreign intelligence surveillance legislation.

Indeed, it critical to recognize Section 702 as one authority within an ecosystem of often-overlapping surveillance authorities, many of which contain gaps and loopholes that are increasingly allowing warrantless access to Americans' most sensitive information. Reform of any single statute, on its own, is unlikely to make a serious dent in the broader problem: the government could evade any new restrictions by using other, more permissive authorities — or, in some cases, by simply purchasing the information from data brokers. Moreover, Section 702 is one of the few surveillance authorities that includes a sunset. Congress should thus view the expiration of Section 702 this year as a rare and vital opportunity to reverse the broader drift, in the law and in practice, toward warrantless surveillance.

I. History and Design of Section 702

Congress passed FISA in 1978 following revelations that the government had engaged in extensive surveillance abuses, including spying on civil rights activists, anti-war protesters, and political opponents, throughout the early decades of the Cold War.[1] The purpose of the law was to ensure that Americans' rights were protected when the government conducts foreign intelligence surveillance.

Under Title I of FISA, the government was required to obtain an order from a special court (the FISA Court) to conduct "electronic surveillance." To obtain the order, the government had to show probable cause that the target of surveillance — whether that target was a foreigner or a "U.S. person" (an American citizen or legal permanent resident) — was a foreign power or an agent of a foreign power.[2] For non-U.S. persons, the terms "foreign power" and "agent of a foreign" power are defined quite broadly,[3] but for U.S. persons, "agent of a foreign power" is defined to require potential involvement in certain criminal activities, including espionage,

[1] *See* Lee Lacy, *Curtailment of the National Security State: The Church Senate Committee of 1975 – 1976*, BOISE STATE, FRANK CHURCH INSTITUTE (May 13, 2019), https://www.boisestate.edu/sps-frankchurchinstitute/2019/05/13/curtailment-of-the-national-security-state-the-church-senate-committee-of-1975-1976/.
[2] 50 U.S.C. § 1805.
[3] 50 U.S.C. § 1801(a), (b)(1).

sabotage, and terrorism.[4] This requirement remains in place today for electronic surveillance that is not targeted at foreigners abroad.

The term "electronic surveillance" is defined in a complex manner keyed to the communications technologies and government surveillance programs that existed at the time.[5] In practice, the definition means that most surveillance activities conducted inside the United States are covered by FISA, whereas most surveillance activities conducted outside the United States — other than those intentionally targeted at U.S. persons — are not covered by FISA and are not subject to any of the law's privacy protections for people in the United States. Overseas collection of communications between foreign targets and Americans, for instance, takes place without any statutory authority or FISA Court involvement.

After 9/11, Congress raced to loosen restrictions on surveillance, including some contained in FISA. The 9/11 Commission later determined that U.S. intelligence agencies had ample intelligence about the planned attacks; they simply failed to share and act on that intelligence.[6] But in the attacks' immediate aftermath, lawmakers assumed otherwise. Congress passed the USA PATRIOT Act, a 341-page bill that made extensive changes to over a dozen federal statutes, only one day after introduction — before many members had even had time to read it.[7]

The law's sweeping new surveillance powers did not satisfy the government, however. President George W. Bush authorized a set of secret programs, code-named Stellar Wind, to collect communications and other personal data without congressional authorization.[8] One of these programs involved the domestic warrantless collection of the content of communications between suspected foreign terrorists and Americans in the United States. This was a clear violation of FISA: although the Patriot Act expanded the purposes for which the government could seek a Title I order, it did not eliminate the requirement to obtain one.

After investigative journalists exposed the program,[9] the government attempted to obtain legal cover by securing the FISA Court's approval. When the court balked,[10] the government

---

[4] 50 U.S.C. § 1801(b)(2).
[5] 50 U.S.C. § 1801(f).
[6] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U. S., THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 254-77, 339-60 (2004).
[7] *See* Electronic Privacy Information Center, *PATRIOT Act* (accessed Jun. 11, 2023), https://epic.org/issues/surveillance-oversight/patriot-act/; Kate Tummarello, *Debunking the Patriot Act as It Turns 15*, EFF (Oct. 26, 2016), https://www.eff.org/deeplinks/2016/10/debunking-patriot-act-it-turns-15.
[8] *See* OFF. INSPECTORS GEN., DEP'T OF DEFENSE, DEP'T OF JUSTICE, CENTRAL INTELLIGENCE AGENCY, NAT'L SEC. AGENCY & OFF. DIR. NAT'L INTELLIGENCE, REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM (2009), *available at* https://int.nyt.com/data/documenttools/savage-foia-stellarwind-ig-report/fd1368590db24fe1/full.pdf; Jake Laperruque, *Secrets, Surveillance, and Scandals: The War on Terror's Unending Impact on Americans' Private Lives,* POGO (Sept. 7, 2021), https://www.pogo.org/analysis/2021/09/secrets-surveillance-and-scandals-the-war-on-terrors-unending-impact-on-americans-private-lives.
[9] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Court*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.
[10] *See* Charlie Savage, *Documents Shed New Light on Legal Wrangling Over Spying in U.S.*, N.Y. TIMES (Dec. 12, 2014), https://www.nytimes.com/2014/12/13/us/politics/documents-shed-new-light-on-legal-wrangling-over-spying-in-us-.html?ref=politics.

turned to Congress. Officials observed that changes in communications technology had altered which communications qualified as "electronic surveillance." As a result, the government was being required to obtain a FISA Title I order to collect foreigners' communications handled by U.S. service providers. Officials argued that this was impeding counterterrorism efforts, and they asked Congress to "modernize" FISA by loosening its restrictions.[11]

Congress responded by enacting the Protect America Act in 2007,[12] soon to be replaced by the FISA Amendments Act — which created Section 702 of FISA — in 2008.[13] Section 702 allows the government to target any foreigner abroad for foreign intelligence collection. Under this authority, the government may collect all of the target's communications, including those with Americans, without obtaining any individualized court order. The only substantive restriction is that a significant purpose of the collection must be the acquisition of foreign intelligence information, defined extremely broadly to include information "related to . . . the conduct of U.S. foreign affairs."[14] The FISA Court must approve general procedures for the surveillance on an annual basis, but it has no role in approving individual targets.[15]

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.[16] 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.[17]

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.[18] Because agencies generally store Section 702 data for at least five years, a yearly intake of 250 million Internet communications would result in at least 1.25 billion such communications residing in government databases at any given time. Given the growth in the program — from

---

[11] *Modernizing the Foreign Intelligence Surveillance Act, Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. (May 17, 2007) (statement for the record of J. Michael McConnell, Dir. Nat'l Intelligence), https://www.dni.gov/files/documents/Newsroom/Testimonies/20070501_testimony.pdf.
[12] Pub. L. 110-55 (2007).
[13] Pub. L. 110-261 (2008).
[14] 50 U.S.C. § 1801(e)(2).
[15] 50 U.S.C. § 1881a.
[16] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 36-41 (2014) [hereinafter PCLOB 702 REPORT], *available at* https://www.pclob.gov/library/702-report.pdf.
[17] *Id.* at 33–34.
[18] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).

89,138 targets in 2013[19] to 246,073 targets in 2022[20] — the number of communications collected today is likely closer to one billion annually, with several billion sitting in storage.

II. The Impact on Americans' Privacy

Although Section 702 may only be targeted at foreigners overseas, it inevitably sweeps in Americans' communications, for the simple reason that Americans communicate with foreigners. The government does not deny that Section 702 results in the collection of Americans' communications in large numbers, although it has rebuffed lawmakers' requests[21] to provide a rough estimate of how many Americans' communications are collected.[22] Given the prevalence of international communication, however, it is safe to assume that the billions of communications acquired under Section 702 include millions of communications involving Americans.

The government refers to the collection of Americans' communications as "incidental," to signify that Americans are not the intended targets of the surveillance. Indeed, if the government's purpose were to spy on those Americans, the program would be unlawful. Such surveillance would require either a warrant (in a criminal investigation) or a FISA Title I order (in a foreign intelligence investigation). To prevent the government from using Section 702 as an end-run around these constitutional and statutory requirements, Congress included two key provisions in the law. First, it required the government to "minimize" the collection, retention,

---

[19] 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.

[20] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2022 at 18 (Apr. 2023) [hereinafter OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2023)], *available at* https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf.

[21] *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; 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; 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.

[22] Initially, the government claimed that providing such an estimate would itself violate Americans' privacy. *See* Letter from The Honorable I. Charles McCullough, III, Inspector General of the Intelligence Comm., to Senators Ron Wyden and Mark Udall (Jun 15, 2012), *available at* https://www.wyden.senate.gov/download/?id=E5DEF293-A8D6-4014-A23A-909C82A3C510&download=1. After privacy experts and advocates refuted that claim, *see* 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, the Obama administration agreed to provide an estimate in early 2017. *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. The Trump administration then reneged on that promise, *see* 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, and there is no sign that the current administration intends to take a different approach.

and sharing of U.S. person information.[23] Second, it required the government to certify to the FISA Court, on an annual basis, that it is not engaged in "reverse targeting"—i.e., using Section 702 as a way to gain access to the communications of "particular, known" Americans.[24]

Over the past 15 years, it has become abundantly clear that these protections have failed. Rather than actually "minimize" the retention and use of Americans' communications, as Congress directed, the government retains such data for years on end — and routinely searches it for Americans' communications to use against them in both criminal and foreign intelligence investigations. The government also has engaged in so-called "abouts" collection, a practice that inevitably results in the acquisition of purely domestic communications. These problems are exacerbated by the broad scope of surveillance authorized by the law, which not only increases the potential volume of "incidental" collection, thus directly implicating Americans' privacy, but also is creating legal headaches for U.S. businesses.[25]

A. Minimization and Its Loopholes

While the concept behind minimization is fairly simple, the statutory language 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."[26] 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."[27]

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 the National Counterterrorism Center (NCTC).[28] All four agencies generally may

---

[23] 50 U.S.C. § 1881a(e).
[24] 50 U.S.C. § 1881a(b)(2), (h)(2)(A)(iii).
[25] In this statement, I use quotation marks for the terms "target," "incidental," and "minimize," to underscore that they are terms of art with particular legal meanings. Legal and policy defenses of Section 702 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."
[26] 50 U.S.C. § 1801(h)(1).
[27] 50 U.S.C. § 1801(h)(3).
[28] MATTHEW G. OLSEN, ASS'T ATT'Y GEN., NAT'L SEC. DIV., U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE

keep unreviewed raw data — including data about U.S. persons — for five years after the certification expires;[29] they also can seek extensions from a high-level official,[30] 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."[31] The agencies may keep indefinitely any U.S. person information that has foreign intelligence value or is evidence of a crime.[32]

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.[33] 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."[34] This is an impossibly high bar, and so, "in practice, this requirement rarely results in actual purging of data."[35]

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

---

INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 9 (Mar. 14, 2022) [hereinafter NSA 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_NSA_Minimization_Procedures-Amended.pdf.

[29] *Id.* at § 4(c)(1)-(2) (2020); LISA O. MONACO, DEPUTY ATT'Y GEN., 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. 14, 2021) [hereinafter FBI 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_FBI_Minimization_Procedures.pdf; LISA O. MONACO, DEPUTY ATT'Y GEN., 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 (Oct. 14, 2021) [hereinafter CIA 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_CIA_Minimization_Procedures.pdf; LISA O. MONACO, DEPUTY ATT'Y GEN., 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. 14, 2021) [hereinafter NCTC 702 MINIMIZATION PROCEDURES], *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_NCTC_Minimization_Procedures.pdf.

[30] PCLOB 702 REPORT, *supra* note 16, at 60; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § B.2.a.

[31] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 7(a)(1).a; FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § I.4; CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at § 3.c.

[32] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at §§ 6(1), 7(a); FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § III.A.3, C.1.b; CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at §§ 3.a, 7.d; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § B.3.

[33] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 4(b)(1), (c).

[34] PCLOB 702 REPORT, *supra* note 16, at 62.

[35] *Id.*

of a crime, the 5-year limit evaporates, and the FBI may keep the data for 15 years.[36] A similar rule applies to the NCTC.[37]

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.[38]

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 commonsense understanding of the term.

B. Back Door Searches

Perhaps the most glaring failure of the protections Congress put in place for Americans' privacy is the practice of "back door searches." Before conducting Section 702 surveillance, the government must certify that it does *not* intend to target particular, known Americans (which would constitute "reverse targeting"). Immediately upon obtaining the data, however, all four agencies have procedures in place that allow them to sort through the data looking for the communications of particular, known Americans — the very people in whom the government just disclaimed any interest. [39] 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 requirements of the Fourth Amendment and Title I of FISA.

According to the Privacy and Civil Liberties Oversight Board (PCLOB), the FBI routinely conducts these searches at the "assessment" phase of its investigations[40] — i.e., before agents have a factual basis to suspect criminal activity, let alone probable cause and a warrant. 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, in 2021 alone, the FBI conducted up to *3.4 million* U.S. person queries of federated

---

[36] FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § III.D.4.c.
[37] [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.
[38] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 8(2), (9); FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § IV.A.1–2, B; CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at §§ 5, 7.d; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, 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 29, at § IV.E.
[39] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 4(b)(4); FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § III.D.3; CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at § 4; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § C.1.
[40] PCLOB 702 REPORT, *supra* note 16, at 59.

data systems that included Section 702 data.[41] In 2022, after the FBI made changes to its data systems that required FBI agents to "opt in" to receiving Section 702 data in response to queries rather than having to "opt out," that number dropped to around 200,000,[42] which is likely to be a more typical number going forward. While that represents a sizeable decrease, it is still an enormous number by any standard, comprising more than 500 warrantless searches for Americans' communications each day.

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.[43]

Government officials have defended back door searches, claiming that as long as information is lawfully acquired, agencies may use the information for any legitimate government purpose.[44] This legal defense entirely misses the point. The staggering figure of 200,000 U.S. person queries per year (plus the several thousand U.S. person queries conducted annually by the NSA, CIA, and NCTC[45]), even with all the government's caveats,[46] 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."[47] Whatever merit the government's defense might

---

[41] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2021 at 21 (Apr. 2022) [hereinafter OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022)], *available at* https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf.

[42] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2023), *supra* note 20, at 24. The government has provided a "de-duplicated" number of 119,383, which represents the number of unique identifiers used to perform queries. *Id*. That is likely a more accurate proxy for the number of Americans affected, but it fails to capture situations in which the FBI performs repeated searches of the same account to find additional information. Each of those searches is a distinct privacy intrusion. Accordingly, the number of total searches (204,090) is a better indicator of the cumulative privacy impact of this practice.

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

[44] *See, e.g., FISA Reauthorization, Hearing Before the S. Comm. on the Judiciary*, 115th Cong. (Jun. 27, 2017), *available via* CSPAN, 44:02, https://www.c-span.org/video/?430549-1/fisa-reauthorization (testimony of Stuart J. Evans, Deputy Ass't Att'y Gen. for Intelligence, Nat'l Sec. Div., Dep't of Justice).

[45] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2023), *supra* note 20, at 20.

[46] ODNI notes that its figures likely overstate the number of Americans affected for a variety of reasons — for instance, batch queries are reported as U.S. person queries even if they involve a mix of U.S. persons and non-U.S. persons. But even if ODNI's numbers are off by an order of magnitude, 20,000 warrantless searches for Americans' communications each year would still be an alarming number.

[47] [Redacted], 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011).

or might not have in other contexts,[48] it is contrary to the constitutional and statutory grounding of the Section 702 program.

Despite these principles, the FISA Court has held that backdoor searches are lawful. But among the handful of regular federal courts outside the FISA Court that have had the opportunity to weigh in on this question, a divide has emerged, with several judges — including a unanimous panel of the Second Circuit Court of Appeals, the only federal appellate court to rule on this question — raising constitutional concerns.[49] Notably, the judges on the other side of this divide have relied heavily on a misrepresentation that the Department of Justice made in litigation, i.e., that government officials need to review Americans' communications anyway as part of the minimization process.[50] Outside of the courts, constitutional scholars have argued that backdoor searches must be treated as a separate Fourth Amendment event than the underlying collection, [51] thus triggering (in most cases) the warrant requirement.[52] In short, the constitutionality of backdoor searches is anything but settled.

---

[48] In fact, 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. *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). The fact that the data was lawfully obtained does not give the government permission to conduct a fishing expedition that goes beyond the authorized purpose for the seizure. In an analogous 2014 ruling, the Supreme Court held that police officers must obtain a warrant to search the contents of a cell phone even after they lawfully seized that cell phone without a warrant during a search incident to arrest. Riley v. California, 573 U.S. 373 (2014); *see also* Walter v. United States, 447 U.S. 649, 654 (1980) ("The fact that FBI agents were lawfully in possession of the boxes of film did not give them authority to search their contents."); United States v. Odoni, 782 F.3d 1226, 1237-38 (11th Cir. 2015) ("We . . . must analyze the search and the seizure separately, keeping in mind that the fact that police have lawfully come into possession of an item does not necessarily mean they are entitled to search that item without a warrant.").

[49] *See* United States v. Hasbajrami, 945 F.3d 641, 669-73 (2d Cir. 2019). The Second Circuit remanded to the district court for further factual development about the search that occurred in that case. Judge Carlos Lucero of the U.S. Court of Appeals for the Tenth Circuit, in a dissenting opinion, similarly expressed constitutional concerns about backdoor searches, opining that such searches must be analyzed as separate Fourth Amendment events from the original collection; the majority did not reach the issue, as they held that the record did not establish that a backdoor search occurred. *See* United States v. Muhtorov, 20 F.4th 558, 678-80 (10th Cir. 2021).

[50] *See* United States v. Mohamud, 2014 WL 2866749, at *26 (D. Oregon 2014); United States v. Hasbajrami, 2016 WL 1029500, at *12n.20 (E.D.N.Y. 2016); United States v. Al-Jayab, No. 16 CR 181, at 55-6 (N.D. Ill. June 28, 2018), *available at* https://storage.courtlistener.com/recap/gov.uscourts.ilnd.324196/gov.uscourts.ilnd.324196.115.0.pdf; *see also* Elizabeth Goitein, *Americans' Privacy at Stake as Second Circuit Hears Hasbajrami FISA Case*, JUST SEC. (Aug. 24, 2018), https://www.justsecurity.org/60439/americans-privacy-stake-circuit-hears-hasbajrami-fisa-case/ (explaining the misrepresentation on which the court relied).

[51] *See* Orin Kerr, *The Fourth Amendment and querying the 702 database for evidence of a crime*, WASH. PO. (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/.

[52] The Supreme Court has held that warrantless searches are *per se* unreasonable unless they fall within an established exception to the warrant requirement. City of Los Angeles v. Patel, 576 U.S. 409, 419-420 (2015). A few circuit courts have held than there is a narrow "foreign intelligence" exception to the warrant requirement in at least some cases; the Fourth Circuit, for instance, recognized such an exception in cases where the surveillance is for the primary purpose of obtaining foreign intelligence and the target is a foreign power or agent of a foreign power. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980). The Supreme Court has not recognized such an exception, however. Accordingly, it would be a stretch to say that there is an established foreign intelligence exception to the Fourth Amendment's warrant requirement, let alone one that is broad enough to support the

C. "Abouts" Collection

The government and the FISA Court have interpreted Section 702 to allow the collection of any communications to, from, *or about* the target.[53] 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, the Chinese government, or a wide array of other individuals and groups who are common topics of conversation. Although Section 702 prohibits the intentional acquisition of purely domestic communications, such acquisition is an inevitable result of so-called "abouts" collection.[54]

The NSA's failure to comply with special minimization rules for "abouts" collection (discussed later in this statement), which delayed the FISA Court's approval of the program in 2016, led the agency to stop the practice in April of 2017.[55] 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.

D. Scope of Surveillance

The permissible scope of surveillance under Section 702 is exceedingly broad. Other than the foreignness and location criteria (and certain requirements designed to reinforce them), the only substantive 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.[56]

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 conduct of the foreign affairs of the United States."[57] 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.[58] Finally, the statute requires the FISA Court to accept the government's

---

government's current practice with regard to U.S. person queries. *See* ELIZABETH GOITEIN & FAIZA PATEL, WHAT WENT WRONG WITH THE FISA COURT 11-12 (Brennan Ctr. for Justice 2015), https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court (discussing case law on foreign intelligence exception).

[53] PCLOB 702 REPORT, *supra* note 16, at 37.

[54] PCLOB 702 REPORT, *supra* note 16, at 119-122.

[55] 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.

[56] 50 U.S.C. § 1881a(g)(2)(A)(v).

[57] 50 U.S.C. § 1801(e)(2).

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

certifications under Section 702 as long as they contain the required elements.[59] These factors greatly weaken the force of the "foreign intelligence purpose" limitation.

Going forward, Section 702 surveillance might be somewhat constrained by President Biden's executive order establishing new rules for the collection of signals intelligence. The order sets forth twelve legitimate objectives for signals intelligence collection, [60] 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 overbroad scope of permissible Section 702 surveillance not only disregards the privacy rights of foreigners who pose no threat to the United States; it has significant implications for Americans' privacy, as well. The larger the pool of foreigners who may be targeted, the larger the pool of Americans whose communications are subject to "incidental" collection. Moreover, the ability to target ordinary private citizens of other nations greatly increases the likelihood of the government acquiring entirely innocent conversations between Americans and their friends, relatives, and business colleagues overseas.

Section 702's expansive reach is also causing significant legal and economic problems for U.S. businesses. 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.[61] 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 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.[62] More than 5,000 U.S. companies rely on a U.S.-EU data-sharing agreement to do business.[63] Highlighting the risk to U.S. companies, Meta was recently fined $1.3 billion by Irish privacy regulators for transferring EU citizens' data to the United States without a valid agreement in place.[64]

---

[59] 50 U.S.C. § 1881a(i)(3)(A).
[60] Exec. Order 14086, § 2(b)(i)(A), 87 Fed. Reg. 62283-4 (Oct. 7, 2022).
[61] *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.
[62] 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.
[63] *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.
[64] Hanna Ziady, *Meta slapped with record $1.3 billion EU fine over data privacy*, CNN (May 22, 2033), https://www.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html.

III. Violations of Statutory and Court-Ordered Privacy Protections

Section 702 has been marked since its inception by repeated, often systemic violations of the rules Congress and the FISA Court have put in place to protect Americans' privacy. The extent of this non-compliance is alarming in its own right. Any unauthorized collection, search, or dissemination can result can result in Americans being investigated without proper legal basis or sensitive information falling into the hands of people who could misuse it. But recent violations raise even more acute concerns: the targeting of Americans based on race, ethnicity, politics, or journalistic activity.

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

Congress and the FISA Court have attempted to place some modest limits on the FBI's use of backdoor searches. The FBI, however, has routinely violated those limits.

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 very small subset of cases, i.e., predicated criminal investigations unrelated to national security.[65] This provision is rarely triggered, both because "related to national security" is a subjective and malleable criterion and because the FBI, according to the PCLOB, routinely performs U.S. person queries at the "assessment" stage — i.e., before the FBI has sufficient information to open a predicated investigation.[66] Nonetheless, according to the ODNI's statistical transparency reports, this requirement has been triggered on approximately 100 occasions over the past four years.[67] 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).[68] Specifically, systems would display query results in a summary field that showed 100 characters of text around the query term within the records

---

[65] 50 U.S.C. § 1881a(f)(2)(A).

[66] PCLOB 702 REPORT, *supra* note 16, at 59.

[67] 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) [hereinafter OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2021)], *available at* https://www.dni.gov/files/CLPT/documents/2021_ASTR_for_CY2020_FINAL.pdf; OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 41, at 22; OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2023), *supra* note 20, at 26. Before 2021, rather than reporting the number of times the court-order requirement (which appears in Section 702(f)(2)) was triggered, the government reported a slightly broader number, i.e., how many times the government reported to the FISA Court that FBI agents had accessed Section 702 data in response to queries not designed to return foreign intelligence. (Congress had required this reporting in 2018.) However, in its 2020 report, the government noted that "a Section 702(f)(2) order should have been obtained . . . in nearly all of [these] queries." OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT at 20 (2021). The government also stated that, "in some instances, a single report to the Court involved multiple queries on the same day by the same user that returned and displayed Section 702 content." *Id.* at 21. Accordingly, the total number of cases in which the government should have obtained a court order before accessing queries is almost certainly higher than 100.

[68] [Redacted], at 69 (FISA Ct. Dec. 6, 2019), *available at* https://repository.library.georgetown.edu/bitstream/handle/10822/1060343/gid_c_00282.pdf?sequence=1&isAllowed=y.

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."[69] In any event, this feature of the FBI systems did not account for all of the violations.

The vast majority of U.S. person queries fall outside this narrow court-order requirement. In those cases, the only substantive restriction on queries is the standard set forth in the FBI's querying procedures (and previously in its minimization procedures, before Congress required agencies to develop separate querying procedures when it reauthorized Section 702 in 2018). Under that standard, "[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."[70] This is a fairly low bar, to be sure. Even so, government reports and FISA Court opinions issued in recent years show that the FBI has engaged in "widespread violations" of this rule.[71]

A recently declassified April 2022 FISA Court opinion and two 2022 compliance reports reveal a series of particularly disturbing violations. In 2021, FBI agents conducted more than a hundred backdoor searches for the communications of people arrested during protests in the spring of June 2020 — i.e., following the police killing of George Floyd. The agents said they wanted to find out whether the protesters had ties to foreign terrorists, but they had no reason to suspect any such connections.[72] That same year, agents ran thousands of searches relating to the January 6th attack on the U.S. Capitol, also on a baseless hunt for evidence of foreign ties.[73] Agents ran additional searches for information about a sitting U.S. congressman;[74] a local political party;[75] multiple U.S. government officials, journalists, and political commentators;[76]

---

[69] *Id*. at 70.
[70] [Redacted], 402 F. Supp. 3d 45, 75 (FISA Ct. 2018).
[71] [Redacted], at 44 (FISA Ct. Nov. 18, 2020), *available at* https://repository.library.georgetown.edu/bitstream/handle/10822/1061209/gid_c_00289.pdf?sequence=1&isAllowed=y.
[72] [Redacted], at 27 (FISA Ct. Apr. 21, 2022), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf.
[73] *Id*. at 28-9.
[74] *See* DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE 58 (Dec. 2021) [hereinafter DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT (Dec. 2021)], https://www.intelligence.gov/assets/documents/702%20Documents/declassified/24th-Joint-Assessment-of-FISA-702-Compliance.pdf.
[75] DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT 58 (Dec. 2021).
[76] DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE 60 (Aug. 2021), https://www.intel.gov/assets/documents/702%20Documents/declassified/22nd_Joint_Assessment_of_FISA_702_Compliance_CLEARED_REDACTED_FOR_PUBLIC_RELEASE.pdf.

19,000 donors to a political campaign;[77] and two "Middle Eastern" men who were reported by a witness because they were loading boxes labeled "Drano" into a vehicle.[78]

These incidents carry echoes of the politically and racially motivated surveillance abuses that occurred under the reign of J. Edgar Hoover. That's alarming, but it should not be surprising. When government officials are not required to show probable cause of criminal activity to a court, it dramatically increases the risk that searches will be driven by improper considerations — including officials' conscious or subconscious prejudices or political leanings.

Other reported violations are disturbing simply because they violated the privacy of ordinary Americans who should never have come under law enforcement scrutiny. They include searches for the communications of:

- people who came to the FBI to perform repairs;[79]
- victims who approached the FBI to report crimes;[80]
- business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy";[81]
- college students participating in a "Collegiate Academy";[82]
- police officer candidates;[83] and
- colleagues and relatives of the FBI agent performing the search.[84]

The FISA Court expressed "serious concern" about "the large number of queries evidencing a misunderstanding of the querying standard — or indifference to it."[85] 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."[86] The Court wrote, "[I]t 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."[87]

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."[88] The FBI claims to have addressed this problem through new training requirements, internal oversight measures, and data systems adjustments that were implemented in 2021 and 2022. This response would be more reassuring if the standard

---

[77] [Redacted] (FISA Ct. Apr. 21, 2022), *supra* note 72, at 29.
[78] DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT 61 (Dec. 2021).
[79] [Redacted] (FISA Ct. Nov. 18, 2020), *supra* note 71, at 40.
[80] *Id.* at 40.
[81] *Id*. at 39.
[82] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 68, at 66.
[83] *Id.*
[84] [Redacted], 402 F. Supp. 3d 45, 78 (FISA Ct. 2018).
[85] *Id*.
[86] *Id*. at 79.
[87] *Id*. at 79–80.
[88] *Id*. at 77.

in question were a new one. But that standard has been in place for well over a decade,[89] and throughout that period, the government has been touting its rigorous training and oversight,[90] assuring lawmakers that these protections were more than adequate to safeguard Americans' rights. The notion that the FBI simply needs a little more time to get its house in order is both difficult to credit and far too dismissive of the constitutional rights that have been violated.

Indeed, the recent FISA Court opinions are only the latest in a string of opinions dating back to 2009 that reveal an unbroken pattern of violations — by the FBI, NSA, and CIA — of the rules designed to protect Americans' privacy. On numerous occasions, the government has responded by pledging to improve its training and/or bolster internal oversight. None of these efforts has been sufficient to disrupt the pattern for any significant length of time. In the words of surveillance expert Julian Sanchez, the FISA Court and the government have been engaged in a game of "compliance whackamole."[91]

In any event, the FBI's own data suggest that an unacceptable number of violations are still occurring, despite the changes it has put in place. A report of the FBI's newly-created Office of Internal Audits found that the FBI's adjustments reduced the non-compliance rate from 18% to 4%.[92] There are serious questions about the report's methodology; among other things, FBI agents were asked to justify their queries long after they had taken place, and they were aware that their answers were being considered as part of a compliance audit. Even accepting the 4% number on its face, however, applying it to the 200,000 U.S.-person-query figure yields more than *8,000 searches each year* that violate even the FBI's own low internal standard.

The additional changes the FBI announced last month will not solve the problem. FBI agents who are found to engage in "performance incidents involving negligence" will now face escalating consequences for each incident. The first incident will result in a temporary loss of access to FISA data while the agent undergoes retraining and one-on-one counseling, while subsequent incidents would prompt "further measures, up to and including indefinite loss of FISA access, reassignment to a new role, and/or referral to the FBI's Inspection Division." In

---

[89] *See* [Redacted], at 26-7 (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 (noting that foreign-intelligence and evidence-of-a-crime queries "have been explicitly permitted by the FBI Minimization Procedures since 2009."). Indeed, a similar standard is part of the minimization rules for FISA generally, so the standard actually predates the Section 702 procedures. *See* MICHAEL MUKASEY, U.S. DEP'T OF JUSTICE, STANDARD MINIMIZATION PROCEDURES FOR FBI SURVEILLANCE AND PHYSICAL SEARCH CONDUCTED UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT § 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.

[90] *See, e.g.,* Off. Dir. Nat'l Intelligence, *Section 702 Overview,* at 8-9 (accessed Jun. 16, 2023), https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf.

[91] *See* Privacy & Civil Liberties Oversight Bd., *PCLOB Public Forum on FISA Section 702*, YOUTUBE (Jan. 12, 2023), 57:50, https://www.youtube.com/watch?v=AZvaimMTqio&t=357s (comments of Julian Sanchez).

[92] FEDERAL BUREAU OF INVESTIGATION, OFF. OF INTERNAL AUDITING, FISA QUERY AUDITING at slide 6 (May 10, 2023), *available at* https://int.nyt.com/data/documenttools/fisa-query-audit-5-10/d9d8e20bafef27c8/full.pdf.

addition, performance ratings of field office leaders will eventually incorporate the offices' FISA compliance.[93]

It is frankly shocking that such basic accountability measures were not in place before. It is unclear, however, what conduct the FBI would consider to be "negligent" for purposes of triggering remedial measures. In the same announcement, the FBI notes that "instances of intentional or reckless behavior have been extremely rare, and there have been none identified since 2018."[94] Yet the FISA Court's April 2022 opinion recounts a 2021 incident in which an agent admitted that "he always recorded queries as not involving U.S.-person query terms even if the facts indicated otherwise, *e.g.,* identifiers for local businesses and mosques."[95] An agent also queried *19,000* campaign donors to find evidence of foreign ties, when there was reason to suspect such ties in only eight cases. The fact the FBI does not consider these and similar incidents to reflect "recklessness" raises serious questions about how it evaluates agents' conduct. When one also considers that compliance audits reach only a small fraction of U.S. person queries;[96] that the consequences of the first infraction are fairly minor; and that even repeated violations seemingly will not lead to suspension or termination, it is hard to imagine that these belated measures will result in the dramatic behavior change that is necessary.

B. Other Violations

On multiple other occasions in the past fifteen years, the FISA Court has had occasion to rebuke the government for repeated, significant, and sometimes systemic failures to comply with statutory requirements or 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 of 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."[97]

---

[93] *See* Federal Bureau of Investigation, *FBI Deputy Director Highlights Bureau's New FISA Query Accountability Procedures* (Jun. 13, 2023), https://www.fbi.gov/news/press-releases/fbi-deputy-director-highlights-bureau-s-new-fisa-query-accountability-procedures#Fact-Sheet.

[94] *Id.*

[95] [Redacted] (FISA Ct. Apr. 21, 2022), *supra* note 72, at 48.

[96] *See* [Redacted], 402 F. Supp. 3d 45, 79 (FISA Ct. 2022) (noting that "some [field] offices go for periods of two years or more between oversight visits" and that oversight personnel "review only a small portion of the queries conducted").

[97] *In re* Production of Tangible Things from [Redacted], No. BR 08-13, at 10–11 (FISA Ct. Mar. 2, 2009).

- "The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions . . . to the FISC."[98]
- "[T]he NSA continues to uncover examples of systematic noncompliance."[99]
- "Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures."[100]
- "[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."[101]
- "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions [under Section 702] mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[102]
- "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."[103]
- "As far as can be ascertained, the requirement was simply ignored."[104]
- "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 . . . ."[105]
- "The government has provided no comprehensive explanation of how so substantial an overcollection occurred."[106]
- "[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."[107]
- "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."[108]
- "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

---

[98] *Id.* at 6.
[99] *Id.* at 10.
[100] *Id.* at 15.
[101] *Id.* at 16.
[102] [Redacted], 2011 WL 10945618, at *5 n. 14 (FISA Ct. Oct. 3, 2011).
[103] [Redacted], Docket No. PR/TT [Redacted], at 4 (FISA Ct. [Redacted]), *available at* https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[104] *Id.* at 19.
[105] *Id.* at 20.
[106] *Id.* at 21.
[107] *Id.* at 22.
[108] *Id.* at 77.

that widespread ignorance of the rules was a contributing factor."[109]

- "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."[110]
- "[The] cases in which the FBI had not established the required review teams seemed to represent a potentially significant rate of non-compliance."[111]
- "The Court was extremely concerned about these additional instances of non-compliance."[112]
- "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 . . . ."[113]
- "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 . . . ."[114]
- "[A] non-compliance rate of 85% raises substantial questions about the appropriateness of using [a redacted tool] to query FISA data."[115]
- "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."[116]
- "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."[117]
- "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."[118]
- "It must be noted, however, that the government has unjustifiably disregarded the current reporting requirement [with respect to retention of raw Section 702 data]. Instead of taking concrete steps to comply even partially with the Court's directive (or timely seeking relief from it), it chose to wait while the FBI reportedly worked on guidance to instruct its personnel on how to handle unminimized Section 702 information on these archival systems."[119]

---

[109] *Id.* at 95.
[110] *Id.* at 115.
[111] [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.
[112] *Id.* at 50.
[113] *Id.* at 58.
[114] [Redacted] (FISA Ct. Apr. 26, 2017), *supra* note 37, at 80.
[115] *Id.* at 82.
[116] *Id*. at 19 (internal quotation marks omitted).
[117] [Redacted], 402 F. Supp. 3d 45, 56 (FISA Ct. 2018).
[118] *Id.* at 104.
[119] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 68, at 44.

- "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."[120]
- "The government has not reported such instances [of misuse of Section 702-acquired information] in timely fashion. Rather, they have been reported to the Court belatedly, usually after they were uncovered during oversight reviews."[121]
- "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."[122]
- "[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 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."[123]

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."[124] 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.

---

[120] *Id.* at 45.
[121] *Id.* at 71-72.
[122] *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.
[123] *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.
[124] [Redacted] (FISA Ct. Apr. 26, 2017), *supra* note 37, at 19.

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."[125] The Court chided the government for this "institutional lack of candor."[126] 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,"[127] and as of March, "continued to . . . investigate potential root causes of non-compliant querying practices."[128] With no resolution in sight, and with the Court unwilling to certify the program 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 the NSA's queries using identifiers of U.S. persons targeted under Sections 704 and 705(b) resulted in improper querying of Section 702 data.[129] 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.[130] 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.[131]

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."[132] 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.[133]

Another revelation of NSA non-compliance came last November, 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.[134] The report details how one NSA analyst launched a surveillance project in early 2013 that targeted Americans' communications without a

[125] *Id.* at 20.
[126] *Id.* at 19.
[127] *Id.* at 21.
[128] *Id.* at 23.
[129] *Id.* at 82.
[130] *Id.* at 84.
[131] *Id.* at 87–9.
[132] [Redacted] (FISA Ct. Dec. 6, 2019), *supra* note 68, at 13.
[133] [Redacted] (FISA Ct. Nov. 18, 2020), *supra* note 71, at 37–8.
[134] 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.

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."[135] 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.[136]

Most recently, the April 21, 2022 FISA Court opinion (which the government did not publicly release until May 2023) confirms that improper U.S. person queries continue at the NSA. The Court reported that a flawed processing system used by the NSA resulted in 18 identified instances of improper U.S. person queries, and that "other improper U.S.-person queries also likely occurred."[137] Separately, the NSA conducted 77 U.S. person queries that had not been properly approved.[138] Given that internal audits review only a fraction of agents' queries—and therefore detect only a fraction of violations—it is likely that the NSA is conducting hundreds of backdoor searches each year that violate applicable limits.

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 widespread failures to honor privacy protections should give lawmakers pause as the government once again asks Congress to entrust the government with immense quantities of Americans' private data.

IV. Needed Reforms

The above discussion makes clear that Congress should not reauthorize Section 702 without far-reaching reforms. Section 702 itself should be amended to close the backdoor search loophole, strengthen the reverse-targeting prohibition and minimization requirements, prohibit "abouts" collection, and narrow the scope of surveillance. For these reforms to be effective, however, Congress must go beyond Section 702. It also must address broader problems in FISA by bolstering judicial oversight and by completing the modernization of FISA to ensure

---

[135] 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.
[136] *Id.*
[137] [Redacted] (FISA Ct. Apr. 21, 2022), *supra* note 72, at 70.
[138] *Id*.

protections for Americans' communications regardless of where they are routed or stored. Finally, Congress should address statutory gaps and outdated laws that could allow warrantless surveillance of Americans to migrate from backdoor searches of Section 702 data to other methods.

A. Section 702

1. Close the Backdoor Search Loophole

The starting point for any reauthorization of Section 702 must be an end to warrantless searches of Americans' "incidentally" obtained communications. Specifically, Congress should require all government agencies to obtain either a warrant (for criminal investigations) or a Title I FISA Court order (for foreign intelligence investigations) 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. What makes warrantless surveillance under Section 702 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 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 information in question, the government ordinarily may be required to obtain a court order (e.g., under 18 U.S.C. §2703(d) or Section 215 of the USA Patriot Act[139]) 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.

Importantly, this requirement should apply to all agencies that conduct U.S. person queries, not just the FBI, and it should apply regardless of whether the underlying investigation pertains to purely domestic criminal activity or to cases that involve a national security or foreign intelligence component. The Supreme Court has made clear that warrants are required to conduct surveillance in domestic national security investigations.[140] Moreover, even when an American is acting on behalf of a foreign entity and is engaged in international terrorism or other transnational crimes, FISA prohibits surveillance of that American unless the government obtains a FISA Title I order, which requires a showing of probable cause that the target is an agent of a foreign power.[141] Allowing the government to perform a U.S. person query of Section 702 data without that showing creates an end-run around the protections of the law.[142]

---

[139] 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)).

[140] United States v. U.S. Dist. Court for E. Dist. of Mich. (Keith), 407 U.S. 297 (1972).

[141] 50 U.S.C. §1805.

[142] In addition, as noted above, there is no firmly established "foreign intelligence" exception that would justify warrantless U.S. person queries for foreign intelligence purposes. *See supra* note 52.

Moreover, exempting foreign intelligence queries from the court-order requirement would allow the worst abuses we have seen thus far to continue unchecked. In attempting to justify queries of more than 100 people involved in the protests against the police killing of George Floyd, the FBI maintained (wrongly) that there was a "reasonable basis to believe the queries would return foreign intelligence."[143] The FBI's batch query for the communications of more than 19,000 donors to a single congressional campaign was based on an allegation that the campaign was a target of "foreign influence."[144] The FBI's query using the name of U.S. Congressman Darrin LaHood was reportedly based on concerns that "a foreign government had targeted him as part of an espionage or covert influence intelligence operation."[145] FBI agents ran thousands of queries aimed at people or groups suspected of involvement in the January 6, 2001 attack on the U.S. Capitol seeking evidence of "foreign influence."[146] The FBI ran a query using the names of a "local political party" to determine "if the party had connections to foreign intelligence."[147] None of these violations would have been prevented by a warrant requirement that was limited to queries in purely domestic criminal investigations.

The government has stated that the FBI sometimes uses U.S. person queries to identify potential victims or targets of foreign cyberattacks, foreign influence campaigns, or foreign efforts to recruit spies, and that a warrant requirement would prevent the government from doing this. Indeed, the government has asserted that it performed 1.9 *million* warrantless U.S. person queries in 2021 for the purpose of identifying potential victims of foreign cyberattacks.[148] Notably, government officials did not mention this "defensive" practice when testifying before Congress during the 2017-2018 reauthorization of Section 702, despite the fact that backdoor searches were the subject of intense debate. This new justification raises more questions than it answers, given that the government has provided no public information about how this technique operates or its relative utility.[149]

In any event, the need to protect victims is hardly unique to the Section 702 context. Domestic law enforcement agencies are routinely faced with this task. They manage to keep the American public safe using investigative techniques that comport with the Fourth Amendment — including obtaining the consent and cooperation of potential victims themselves, or invoking the "exigent circumstances" exception to the warrant requirement in cases where victims are in imminent danger. There is no blanket "victim" exception to the Fourth Amendment, however; nor does the Constitution draw any distinction between "offensive" or "defensive" searches or seizures.

---

[143] [Redacted] (FISA Ct. Apr. 21, 2022), *supra* note 72, at 27.
[144] *Id*. at 29.
[145] Charlie Savage, *FBI Feared Lawmaker Was Target of Foreign Intelligence Operation*, N.Y. TIMES (Apr. 13, 2023), https://www.nytimes.com/2023/04/13/us/politics/fbi-darin-lahood.html.
[146] [Redacted] (FISA Ct. Apr. 21, 2022), *supra* note 72, at 29.
[147] DEP'T OF JUSTICE & OFF. DIR. NAT'L INTELLIGENCE, SEMIANNUAL ASSESSMENT (Dec. 2021), *supra* note 74, at 58.
[148] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT (2022), *supra* note 41, at 20.
[149] For instance, with respect to the use of backdoor searches to identify potential cyberattack victims in 2021, how did the FBI identify the 1.9 million U.S. persons in question? Of those 1.9 million queries, how many resulted in the identification of a potential victim and the implementation of successful evasive measures? Was there no probable cause to suspect malicious cyber activity in those cases?

There is good reason for that. Whatever the *purpose* of the search, the *result* is to expose an American's personal information to manual review by an FBI agent, with all the potential for abuse such access entails. Indeed, the line between victim and suspect, particularly when it comes to foreign actors' efforts to recruit spies or exert influence, can be extremely murky. Throughout the FBI's darkest decades, the Bureau spied on anti-war protesters and racial justice activists, including Martin Luther King, Jr., on the ostensible grounds that they had been targeted and potentially infiltrated by foreign communists. Claims of potential foreign influence were also used to justify government monitoring of Muslim American communities after 9/11 and, more recently, the Movement for Black Lives and Antifa.[150]

The government is also attempting to ward off a warrant requirement by promising that the FBI's recent changes to its training, oversight, and data-access procedures will put an end to agents' "widespread violations" (as the FISA Court described them) of the FBI's court-approved rules for conducting U.S. person queries. As noted above, the FBI's own data suggest that violations are continuing to occur at a rate of over 8,000 per year, despite these changes. But even if the FBI could ensure perfect compliance, that would not obviate the need for a warrant. An agency's internal determination that a search of Fourth Amendment-protected data is reasonably likely to yield foreign intelligence or evidence of a crime is not the same as, and cannot substitute for, a showing of probable cause before a neutral magistrate. As the Supreme Court stated in a Fourth Amendment case where the government had argued that its protocols for searching cell phones were sufficient to protect Americans' privacy: "The founders did not fight a revolution to gain the right to government agency protocols."[151]

Finally, FBI officials have occasionally suggested that requiring a warrant or FISA Title I order for U.S. person queries would be tantamount to re-building "the wall."[152] This notion is utterly baseless. "The wall" refers to a set of pre-9/11 procedures that — in practice, if not on paper[153] — restricted intelligence officials' ability to share identified threat information with criminal prosecutors. The information in question was obtained under Title I of FISA, which

---

[150] Martin Luther King, Jr. Research & Education Institute, Stanford University, *Federal Bureau of Investigation (FBI)* (accessed Jun. 16, 2023), https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi; SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT OF THE SENATE SELECT COMM. TO STUDY GOVERNMENT OPERATIONS: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 69-70 (1976); American Civil Liberties Union, *Factsheet: The NYPD Muslim Surveillance Program* (accessed Jun. 16, 2023), https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program; Micah Lee, *How Northern California's Police Intelligence Center Tracked Protests*, INTERCEPT (Aug. 17, 2020), https://theintercept.com/2020/08/17/blueleaks-california-ncric-black-lives-matter-protesters/; Devan Cole, *FBI director says bureau is looking into possible foreign influence in Floyd protests*, CNN (Jun. 24, 2020), https://www.cnn.com/2020/06/24/politics/christopher-wray-fbi-protests-foreign-influence/index.html; Sarah N. Lynch & Andy Sullivan, *Attorney General Barr says foreign groups, extremists stoking divisions in U.S. protests*, REUTERS (Jun. 4, 2020), https://www.reuters.com/article/uk-minneapolis-police-barr-idAFKBN23B35B.

[151] Riley v. California, 573 U.S. 373, 398 (2014).

[152] *See* Christopher Wray, Dir., Federal Bureau of Investigation, *Defending the Values of FISA Section 702* (Oct. 13, 2017), https://www.fbi.gov/news/speeches/defending-the-value-of-fisa-section-702; Privacy & Civil Liberties Oversight Bd., *PCLOB Public Forum on FISA Section 702, supra* note 91, at 2:00:55 (comments of Mike Herrington, Senior Operations Advisor, FBI).

[153] *See* Barbara A. Grewe, Senior Counsel for Special Projects, Comm'n on Terrorist Attacks Upon the United States, *Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations* (Aug. 20, 2004), https://irp.fas.org/eprint/wall.pdf.

means the government had *already* secured a probable-cause order at the point in the case where "the wall" kicked in.[154] Moreover, requiring a warrant for U.S. person queries would in no way inhibit the sharing of threat information — including information about Americans — that officials encountered in the course of querying and reviewing *foreigners'* communications. Any such discovery would be analogous to the "plain view" exception to the Fourth Amendment's warrant requirement.[155] What the Fourth Amendment cannot tolerate is the government collecting information without a warrant or Title I order with the intent of mining it for use against Americans.

Some government officials have questioned why FBI agents should be prohibited from using U.S. person queries when they could theoretically access the same information through the much less efficient process of reviewing each and every communication obtained under Section 702. The answer is that manual review of the tens of millions of Section 702-obtained communications residing in FBI databases — or even a relatively small fraction of those communications — would not just be inefficient; it would be impossible. The Supreme Court has made clear that where technology enables a privacy intrusion that would not be possible or practicable with more traditional techniques, the Fourth Amendment may be triggered. Thus, for instance, the government must obtain a warrant to attach a GPS device to a car for 28 days[156] or to obtain a week's worth of cell phone location information,[157] even though a police department could *theoretically* (but not realistically) obtain the same information without a warrant by deploying multiple police officers to follow the person in question twenty-four hours a day for days or weeks on end.

Recognizing the acute privacy and civil liberties concerns raised by U.S. person queries, 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.[158] Many in Congress have already embraced this approach. Senators Diane Feinstein, Mike Lee, Patrick Leahy, and Kamala Harris cosponsored an amendment requiring the government to obtain a probable-cause order for U.S. person queries the last time Section 702 was reauthorized,[159] although it didn't receive a vote. And the House has twice passed a similar amendment (in 2014[160] and 2015[161]) with both Democratic and Republican support.

---

[154] *See id.* at 29.
[155] For a discussion of the "plain view" exception, *see* Coolidge v. New Hampshire, 403 U.S. 443 (1971); Horton v. California, 496 U.S. 128 (1990).
[156] *See* United States v. Jones, 565 U.S. 400 (2012). Although the plurality opinion rested on the property intrusion caused by attaching the GPS device to the car, five justices concluded that the GPS tracking itself violated a reasonable expectation of privacy.
[157] *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).
[158] *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.
[159] *See* S. Amdt. 1875, S. 139, 115th Cong. (2018).
[160] *See* H. Amdt. 935, H.R. 4870, 113th Cong. (2014).
[161] *See* H. Amdt. 503, H.R. 2685, 114th Cong. (2015).

2. Strengthen the Reverse-Targeting Prohibition and Minimization Requirements

In addition to ending the backdoor search loophole, Congress should shore up the provisions designed to minimize the collection, retention, sharing, and use of Americans' information. It should start by strengthening the bar on "reverse targeting." Currently, this provision states that the government may not conduct Section 702 surveillance if "the purpose" of the surveillance is to target a "particular, known" American. The clear intent behind this provision was to prohibit the use of Section 702 as a domestic spying tool. But Congress's wording would in theory allow the government to conduct Section 702 surveillance even if its *primary* purpose was to acquire a particular, known American's communications, as long as its secondary purpose was to target a foreigner abroad. The provision also could be construed to allow collection where the *sole* purpose was to acquire Americans' communications, as long as the government did not know those Americans' identity (i.e., they were not "known" Americans).

The warrantless collection of Americans' communications under Section 702 should truly be "incidental"; it should never be purposeful. Congress accordingly should tighten the language of the reverse-targeting provision by prohibiting the use of Section 702 if "a purpose" of the collection is to "acquire the communications or information of U.S. persons."

Congress also should 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 must 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.[162]

3. Prohibit "Abouts" Collection

Congress 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 legitimate 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

[162] 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.

comprises less than one tenth of Section 702 collection.[163] 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.[164]

4. Narrow the Scope of Surveillance

Congress should narrow the scope of permissible Section 702 targets in a way that preserves the government's ability to address foreign threats to the nation, while reducing the volume of "incidental" collection of Americans' communications and increasing the likelihood of a U.S.-EU data-sharing agreement withstanding European courts' scrutiny. Congress can accomplish this task using one of three approaches — or, better yet, some combination of the three.

The first approach consists of requiring 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. These terms are broadly defined in FISA and give the government ample leeway to target a wide range of malign foreign actors. Moreover, the determination of whether a target is a foreign power or agent of a foreign power would be an internal one; it would not have to be submitted to the FISA Court for 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. (Indeed, Congress should impose this review requirement regardless of whether it creates new criteria for targeting.)

The second approach is to amend the definition of "foreign intelligence" information. The current definition has two parts. The first part encompasses any information about an extensive list of threats that may posed by foreign powers or agents of foreign powers, including actual or potential attacks, actual or potential "grave hostile acts," sabotage, international terrorism, proliferation of weapons of mass destruction, and clandestine intelligence activities.[165] The second part of the definition is a catch-all, extending to any 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."[166] As discussed above, the latter part of the definition is far too broad, enabling surveillance of everyday conversations about current events, and Congress should eliminate it. If the government can identify specific threats that would be excluded by such an approach, Congress can accommodate these concerns by adding those threats to the first part of the definition.

---

[163] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).
[164] *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.").
[165] 50 U.S.C. § 1801(e)(1).
[166] 50 U.S.C. § 1801(e)(2).

The third approach is to codify the legitimate objectives identified in President Biden's executive order (with a small number of revisions[167]) and prohibit the adoption of additional objectives without congressional authorization. Because purpose-based restrictions are difficult to enforce, however, Congress should translate the 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.

B. FISA

Section 702 is a part of FISA and is directly affected by many of FISA's other provisions, such as the mechanisms FISA establishes for judicial review of electronic surveillance and the geographic limitations on FISA's reach. Moreover, recent events have revealed serious problems with the operation of FISA Title I, a permanent authority that has no sunset. Congress should therefore address FISA more broadly in the course of enacting reforms to Section 702.

1. Remove Artificial Barriers to Judicial Review

Congress provided three different mechanisms by which courts could review electronic surveillance conducted under FISA. First, the FISA Court reviews applications to conduct electronic surveillance and engage in other types of collection of Americans' information; it also approves Section 702 certifications and procedures and conducts general oversight of that program. Second, Congress required the government to disclose any use of FISA-derived information in criminal prosecutions or other legal proceedings, thus enabling challenges by the non-government party. Third, Congress expressly provided for civil lawsuits to challenge unlawful surveillance under FISA.

None of these mechanisms is working as Congress intended. The FISA Court's effectiveness is hampered by one-sided proceedings and inaccurate government submissions. The government is evading its notice obligations to criminal defendants through "parallel construction." And civil litigation has been thwarted by misapplications of the standing and state secrets doctrines. Congress must amend the law to ensure that there is effective judicial review and accountability for violations of Section 702 and other FISA authorities.

---

[167] First, with respect to the goal of "understanding or assessing the capabilities, intentions, or activities of . . . a foreign-based political organization," Congress should interpret the term "foreign-based political organization" to exclude civil society non-governmental organizations. *See* Exec. Order 14086, *supra* note 60, at § 2(b)(i)(A)(1). 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/.

a. Increase Adversariality and Improve Accuracy in FISA Court Proceedings

The secrecy and one-sided nature of FISA proceedings are inherently problematic. When judges hear only from one party and their decisions in favor of that party are never subject to appeal, there is a higher risk of skewed and erroneous decisions — as evidenced by the FISA Court's approval of the NSA's program to collect Americans' phone records in bulk, which three regular federal courts subsequently ruled unlawful.[168]

Congress attempted to address this problem in the 2015 USA FREEDOM Act by creating a panel of security-cleared *amici curiae* who could provide a perspective other than the government's in significant cases. This was an important step, but various factors have limited its effectiveness. Amici are still left out of too many important cases. In those cases in which they do participate, they lack sufficient access to the underlying materials. And they have no means of securing an appeal if the Court decides in favor of the government.

At the same time, there has been a troubling pattern of the government presenting inaccurate or incomplete information to the FISA Court. In December 2019, a report from the Department of Justice Inspector General reviewed four FISA Title I surveillance applications submitted as part of the FBI's investigation into alleged Russian interference in the 2016 presidential election.[169] The report identified 17 separate errors or omissions in these applications. This prompted the Inspector General to review FISA Title I applications more broadly. Reviewing a sample of 29 applications, the Inspector General found that 25 of the 29 applications contained "apparent errors or inadequately supported facts";[170] for the remaining four applications, the FBI could not even locate the files containing the documentation on which the applications were ostensibly based. The FISA Court has broadly observed that the government "has exhibited a chronic tendency" to provide inaccurate, incomplete, or materially misleading information to the FISC in its filings.[171]

To address both these problems, Congress should enact the reforms to FISA Court proceedings set forth in the "Lee-Leahy" amendment — an amendment offered by Senators Mike Lee and Patrick Leahy to the USA FREEDOM Reauthorization Act of 2020.[172] Although Congress failed to pass the reauthorization bill, the amendment passed by an overwhelming bipartisan vote of 77-19.[173]

---

[168] United States v. Moalin, 973 F.3d 977 (9th Cir. 2020); American Civil Liberties Union v. Clapper, 785 F.3d 787 (2d Cir. 2015); Klayman v. Obama, 957 F.Supp.2d 1 (D.D.C. 2013).

[169] *See* OFF. INSPECTOR GENERAL, DEP'T OF JUSTICE, REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION (Dec. 2019), *available at* https://www.justice.gov/storage/120919-examination.pdf.

[170] *See* OFF. INSPECTOR GEN., DEP'T OF JUSTICE, MANAGEMENT ADVISORY MEMORANDUM FOR THE DIRECTOR OF THE FBI REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FISC RELATING TO U.S. PERSONS 3 (Mar. 2020), *available at* https://oig.justice.gov/sites/default/files/reports/a20047.pdf.

[171] [Redacted], No. [Redacted], at 13-14 (FISA Ct. [Date Redacted]), *available at* https://www.dni.gov/files/documents/icotr/51117/.

[172] S. Amdt. 1584, H.R. 6172, 116th Cong. (2020).

[173] *Id.* (as agreed to in Senate, May 13, 2020).

The amendment seeks to ensure that amici can weigh in on the most significant cases, including those that involve public officials, political candidates, religious or political organizations, or the media; that amici have access to the materials they need to do their job; that amici can petition the FISA Court to certify questions for appeal; 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.

b. End the Government's Use of "Parallel Construction" to Evade FISA's Notice Requirement

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 ten years since the government's approach reportedly changed,[174] 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 more than two thousand terrorism and national security convictions during this time.[175]

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.[176] This is a well-documented practice that the government has used in a variety of settings, including foreign intelligence surveillance cases.[177] 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.

---

[174] 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.

[175] *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 2022 at 14 (280 guilty dispositions); 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).

[176] *See* Toomey, *supra* note 174; 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.

[177] *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.

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. This definition will remove the government's ability to evade its notice obligations through parallel construction.

c. Clarify Application of Standing and State Secrets Doctrines

Congress clearly intended for civil lawsuits to serve as a means to challenge electronic surveillance activities — indeed, Congress authorized the award of actual and punitive damages in such lawsuits.[178] Congress also was aware that much of the information at issue in such lawsuits — and any other legal proceedings involving evidence derived from FISA — would be classified. It therefore included a provision that carefully directs courts how to handle sensitive information in such cases. In short, if the government claims that the disclosure of information through litigation would harm national security, the court must review the information *in camera* and *ex parte* to determine whether the surveillance was lawful.[179]

Despite Congress's intent to permit civil litigation, civil lawsuits have consistently been derailed by the misapplication of two legal doctrines. First, courts have taken an overly rigid review of the standing doctrine, refusing to allow plaintiffs to bring lawsuits unless they can prove they have been surveilled.[180] Because FISA surveillance is always conducted in secret, even plaintiffs who have ample reason to suspect they have been surveilled generally require discovery to confirm these suspicions. The courts' interpretation of standing presents a Catch-22 in which plaintiffs cannot move to the discovery phase of litigation without providing the evidence that can only be acquired through discovery.

Second, the Supreme Court recently ruled that Congress, in establishing special procedures for the handling of sensitive information in FISA cases, did not intend to displace the operation of the state secrets privilege.[181] The Court's reasoning was that FISA's special procedures and the procedures courts currently use when the government claims the state secrets privilege are not incompatible — but that is clearly false. At the most basic level, some courts have interpreted the state secrets privilege to permit the dismissal of cases at the pleadings stage, which would not be permitted under the special FISA procedures.[182] As a result of the Court's ruling, the government can almost always avoid an adjudication on the merits of any civil lawsuit challenging unlawful surveillance.

Congress must take action to ensure that its intent to make civil litigation available is honored. To that end, Congress should specify that a person has standing to bring a civil lawsuit

---

[178] 50 U.S.C. §1810.
[179] 50 U.S.C. §1806(f).
[180] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
[181] FBI v. Fazaga, 142 S. Ct. 1051 (2022).
[182] *See* Elizabeth Goitein, *The State Secrets Sidestep:* Zubaydah *and* Fazaga *Offer Little Guidance on Core Questions of Accountability*, CATO S. CT. REV. 193 (2022), *available at* https://www.cato.org/sites/cato.org/files/2022-09/Supreme-Court-Review-2022-Chapter-8.pdf.

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. In addition, Congress should amend the provision that establishes special procedures for handling sensitive information in FISA cases to clarify that these procedures govern how courts should resolve any governmental claims of the state secrets privilege.

2. Complete the Modernization of FISA by Eliminating Obsolete Geographical Distinctions in the Protection of Americans' Communications

As a general matter, FISA applies when the government collects foreign intelligence inside the United States or from U.S.-based companies. (A significant exception to this rule is discussed in Part IV.C of this statement.) When the government collects foreign intelligence abroad, it usually relies on claims of inherent presidential authority, as regulated by Executive Order (EO) 12333 and related executive branch policies. The distinction has critical consequences; as explained further below, there are exceedingly few legislative protections for Americans' privacy when the government conducts surveillance under EO 12333, and such surveillance is not subject to any judicial oversight whatsoever.

A geographic limitation on FISA's reach might have made some sense in 1978, when FISA was enacted. At the time, surveillance inside the United States generally meant surveillance of Americans and surveillance overseas generally meant surveillance of foreigners. To be sure, FISA did not restrict the government's ability to collect communications between foreigners and Americans when the surveillance took place overseas or was accomplished by satellite. Nonetheless, the volume of international communications in 1978 was exponentially smaller than it is today. Communications were generally ephemeral and had to be captured in transit; they did not rest in electronic storage for years or decades. And there were significant technological limitations on storing, processing, and analyzing data. These factors greatly limited overseas collection of Americans' international communications.[183]

As for purely domestic communications, they were transmitted almost entirely through wires inside the United States (and therefore covered by FISA). Today, communications are routinely routed and stored all over the world, in places far removed from the points of origin and receipt. Indeed, the fact that purely foreign communications were being handled 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 — is one of the main reasons the government sought to "modernize" FISA in 2008 through the enactment of Section 702.[184]

---

[183] *See* ELIZABETH GOITEIN & FAIZA PATEL, WHAT WENT WRONG WITH THE FISA COURT 19–21 (Brennan Ctr. for Justice 2015), https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court.

[184] *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

But Section 702 failed to address the other half of this problem: the fact that purely domestic communications and other personal data are routinely routed and stored abroad, which can in some cases remove them from FISA's protections and expose them to EO 12333 surveillance. Congress did extend FISA to cover the intentional targeting of Americans who are themselves located overseas,[185] and EO 12333 policies generally prohibit targeting Americans or intentionally collecting domestic communications.[186] These limits, however, are subject to various caveats and exceptions. Moreover, they have little practical effect when the government engages in bulk collection — a dragnet approach in which the government does not identify particular targets. Bulk collection is prohibited under FISA, but it is permitted under EO 12333.

In February 2022, through the efforts of Senators Ron Wyden and Martin Heinrich, Americans learned that the CIA has for years been conducting bulk collection programs under EO 12333 that pull in Americans' data.[187] One set of activities includes the bulk acquisition of information about financial transactions involving Americans and others. [188] Another program collects an unspecified type of data, but the CIA's sparse public statements on the program suggest that it impacts "Americans who are in contact with foreign nationals," [189] which implies that it involves communications records. A document partially declassified by the CIA shows that CIA analysts query the data acquired under this program for information about U.S. persons, and that they do so without recording the justification for the queries[190] — making it virtually impossible to conduct even internal oversight.

Even when EO 12333 surveillance is targeted at specific foreigners (rather than used to conduct bulk collection), it results in the "incidental" collection of Americans' communications, just as Section 702 does. Yet protections for this data are left entirely to executive branch policies, with no judicial review to ensure that these policies comport with the Constitution — or

---

communicants). The government also argued that technological changes restricted its ability to collect foreigners' communications with Americans in a way that undermined Congress's original intent in passing FISA. As I explained in congressional testimony in 2017, this reading of Congress's original intent is incorrect. *See The FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties, Hearing Before the S. Comm. on the Judiciary*, 115th Cong. 2–3n.4 (Jun. 27, 2017) (testimony of Elizabeth Goitein, Co-Dir., Liberty & Nat'l Sec. Program, Brennan Ctr. for Justice), *available at* https://www.judiciary.senate.gov/imo/media/doc/06-27-17%20Goitein%20Testimony.pdf.

[185] 50 U.S.C. §1881c.

[186] DEP'T OF DEFENSE, DOD MANUAL S-5240.01-A, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES: ANNEX GOVERNING SIGNALS INTELLIGENCE INFORMATION AND DATA COLLECTED PURSUANT TO SECTION 1.7(C) OF E.O. 12333 at 2.2.a, 2.4.a (Jan. 7, 2021), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/S-524001-A.PDF?ver=SPh6FZicXc8uH192MI8o3w%3D%3D&timestamp=1610651794685.

[187] *See* Charlie Savage, *C.I.A. Is Collecting In Bulk Certain Data Affecting Amendments, Senators Warn* N.Y. TIMES (Feb. 10, 2022), https://www.nytimes.com/2022/02/10/us/politics/cia-data-privacy.html.

[188] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON CIA FINANCIAL DATA ACTIVITIES IN SUPPORT ON ISIL-RELATED COUNTERTERRORISM EFFORTS (accessed Jun. 16, 2023), *available at* https://www.cia.gov/static/63f697addbbd30a4d64432ff28bbc6d6/OPCL-PCLOB-Report-on-CIA-Activities.pdf.

[189] 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.

[190] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., RECOMMENDATIONS FROM PCLOB STAFF (accessed Jun. 16, 2023), *available at* https://www.cia.gov/static/f61ca00cbcda9b5d46a04e0b53b5f2b9/OPCL-Recommendations-from-PCLOB-Staff.pdf.

that agencies' practices comport with the policies. Inadequate as the protections of Section 702 are, the protections agencies have adopted under EO 12333 are even weaker.[191]

There is no justification for giving lesser protections to Americans' constitutional rights based simply on the accident of where our digital data happens to travel. 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 EO 12333.[192] 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.

To complete the modernization of FISA that began with Section 702, Congress should extend basic protections to Americans' communications and other Fourth Amendment-protected information, regardless of where they are obtained. If it fails to do so, any reforms to Section 702 will have limited effect, as the government will be able to obtain at least some of the same information — with more effort, to be sure, but with far fewer protections for Americans' privacy — entirely outside the FISA framework. At a minimum, Congress should enact measures that:

- prohibit the targeting of Americans under EO 12333;

---

[191] For instance, 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"— 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." *Compare* CENTRAL INTELLIGENCE AGENCY, THE CIA'S UPDATED EXECUTIVE ORDER 12333 ATTORNEY GENERAL GUIDELINES 6 (accessed Jun. 12, 2023), *available at* https://www.cia.gov/static/100ea2eab2f739cab617eb40f98fac85/Detailed-Overview-CIA-AG-Guidelines.pdf *with* 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/21/2021_CIA_Querying_Procedures.pdf. 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." LISA O. MONACO, DEPUTY ATT'Y GEN., 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 (Oct. 14, 2021), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_FBI_Querying_Procedures.pdf. 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." U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 13 (accessed Jun. 12, 2023), *available at* https://www.justice.gov/archive/opa/docs/guidelines.pdf.

[192] 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.

- require the government to minimize the retention, sharing, and use of Americans' information that is "incidentally" acquired under EO 12333;[193]
- close the EO 12333 backdoor search loophole by requiring the government to obtain a warrant or FISA Title I order before conducing U.S. person queries of the data;
- reduce the scope of "incidental" collection of Americans' information by codifying a modified version the legitimate objectives for surveillance set forth in President Biden's recent executive order,[194] and requiring 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; and
- ensure the availability of judicial oversight by requiring the government to inform criminal defendants when using evidence obtained or derived from EO 12333 surveillance.

In addition to these measures, Congress should prohibit bulk collection, or at least tightly limit its availability — e.g., to geographic areas of active or impending hostilities. Bulk collection poses unique risks to Americans' privacy, not to mention the privacy of countless foreign nationals who pose no threat whatsoever to the United States. It is also one reason why European courts have struck down the U.S.-EU agreements that allow EU companies to share customer data with U.S. companies. And the government has never demonstrated the necessity for this highly problematic practice. To the contrary, even though Section 702 has a targeting requirement (i.e., it does not permit bulk collection), intelligence officials have described it as the most effective foreign intelligence surveillance tool in its arsenal;[195] the government has never suggested that the targeting requirement makes Section 702 less effective or results in the loss of vital intelligence.

In implementing these changes, Congress need not call into question the president's constitutional authority to conduct surveillance of foreigners abroad. But where such surveillance extends beyond foreigners and sweeps in the Fourth Amendment-protected information of Americans, there can be no question regarding the necessity and appropriateness of legislative and judicial involvement. As the Supreme Court has made clear, the Constitution "most assuredly envisions a role for all three branches [of government] when individual liberties are at stake."[196]

C. Close Other Statutory Gaps and Update the Law to Prevent Warrantless Surveillance of Americans

It is critical that Congress not consider Section 702, or even FISA itself, in isolation. The authorities provided by FISA are part of a large and complex ecosystem of overlapping

[193] One of the few statutory limits on EO 12333 surveillance is a requirement to delete any unencrypted U.S. person information after 5 years if it does not constitute foreign intelligence or evidence of a crime; however, there is a broad "national security" exception that greatly weakens the force of this provision. *See* 50 U.S.C. §1813.
[194] *See supra note* 167.
[195] *See, e.g.,* Matthew G. Olsen, Ass't Att'y Gen., Dep't of Justice, *Remarks at Brookings Institution on Section 702* (Feb. 28, 2023), https://www.justice.gov/opa/speech/assistant-attorney-general-matthew-g-olsen-delivers-remarks-brookings-institution-section ("In the 15 years since enactment, Section 702 has become the Intelligence Community's most valuable national security legal tool.").
[196] Hamdi v. Rumsfeld, 542 U.S. 507, 536 (2004).

surveillance authorities. In many cases, the government may obtain the same or equivalent information using different techniques (for example, the government may place a wiretap or it may compel production of communications from a service provider) and can choose among them on the basis of convenience. If one avenue of surveillance is closed off or restricted, it is often possible for the government to simply turn to another — or to exploit gaps in the network of surveillance laws to acquire the information without any statutory authorization whatsoever.

Moreover, the problem at the heart of Section 702 in its current form — namely, the government's ability to access Americans' most personal information in ways that undermine statutory and constitutional protections — is present across a range of surveillance authorities and activities today. Yet very few of these authorities or activities are subject to a sunset. Congress would thus be wise to use the scheduled expiration of Section 702 to address other manifestations of the same core problem.

1. Prohibit the Government from Buying Its Way Around FISA and Other Statutory Limits on Surveillance

FISA includes an "exclusivity" provision, which provides that FISA, along with various criminal law provisions authorizing electronic surveillance, "shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted."[197] FISA's highly technical definition of "electronic surveillance,"[198] however, does not cover the collection of many types of records containing communications metadata and other sensitive non-contents information, such as geolocation data. The government can thus claim that certain provisions of FISA — including Section 702 itself, to the extent it authorizes collection activities that do not qualify as "electronic surveillance," as well as the provisions governing physical searches and the collection of some third-party records — are *not* the exclusive means by which such activities may be conducted, and that the government may ignore the restrictions and procedures contained in such provisions.

There's ample reason to believe that's happening now. In 2020, Congress was debating whether to reauthorize Section 215, the so-called "business records" provision of FISA that the NSA relied on to collect Americans' phone records in bulk. Senator Richard Burr — who then chaired the Senate Select Committee on Intelligence — warned that if Section 215 expired, "the president under 12333 authority can do all of this without Congress's permission, with no guardrails."[199] The authority indeed expired (although pending investigations were grandfathered), and the conspicuous absence of any serious government efforts to reinstate it strongly suggests that the government is obtaining the same information through other means.

That's alarming, because the information that the government may obtain under Section 215 and other provisions of FISA not fully covered by the exclusivity provision can be extremely sensitive. Take the phone records that were the subject of the NSA's bulk collection program.

---

[197] 50 U.S.C. §1812.
[198] 50 U.S.C. §1801(f).
[199] *See Sen. Burr claims EO 12333 permits mass surveillance "without Congress's permission"*, C-SPAN (Mar. 12, 2020), 00:18, https://www.c-span.org/video/?c4860932/user-clip-sen-burr-claims-eo-12333-permits-mass-surveillance-without-congresss-permission.

After Edward Snowden's disclosure of the program, experts explained how communications "metadata" — a term many Americans had never encountered — could be crunched to reveal people's associations, activities, and even beliefs.[200] Geolocation information can similarly reveal the most intimate aspects of people's private lives. Indeed, for that very reason, the Supreme Court in *Carpenter v. United States* (2018) held that police need a warrant to obtain a week's worth of geolocation information from a cell phone company.[201]

If the government wanted to obtain such information without adhering to FISA, one workaround would be to purchase it from data brokers. This appears to be an increasingly common practice among federal agencies. In one particularly disturbing example, Vice News reported that "[m]ultiple branches of the U.S. military have bought access to a powerful internet monitoring tool that claims to cover over 90 percent of the world's internet traffic, and which in some cases provides access to people's email data, browsing history, and other information such as their sensitive internet cookies."[202] In addition, multiple agencies have reportedly purchased access to Americans' cell phone location information, including the Federal Bureau of Investigation[203] (as recently confirmed by FBI Director Chris Wray[204]), the Drug Enforcement Administration,[205] multiple components of the Department of Homeland Security (including Immigration and Customs Enforcement[206] and Customs and Border Protection[207]), the Secret Service,[208] and the Department of Defense.[209] Even the Internal Revenue Service, according to the Wall Street Journal, "attempted to identify and track potential criminal suspects by purchasing access to a commercial database that records the locations of millions of American cellphones."[210]

---

[200] Declaration of Professor Edward W. Felten at 16, American Civil Liberties Union v. Clapper, 785 F.Supp.2d 724 (S.D.N.Y. 2013), *available at* https://s3.documentcloud.org/documents/781486/declaration-felten.pdf.
[201] 138 S. Ct. 2206 (2018).
[202] Joseph Cox, *U.S. Military Bought Mass Monitoring Tool that Includes Internet Browsing, Email Data*, VICE (Sept. 21, 2021), https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data.
[203] *See* Sara Morrison, *A surprising number of government agencies buy cellphone data records. Lawmakers want to know why*, VOX (Dec. 2, 2020), https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel.
[204] *See* Ashley Belanger, *FBI finally admits to buying location data on Americans, horrifying experts*, ARS TECHNICA (Mar. 9, 2023), https://arstechnica.com/tech-policy/2023/03/fbi-finally-admits-to-buying-location-data-on-americans-horrifying-experts/.
[205] *See* Morrison, *supra* note 203.
[206] *See* Paul Blest, *ICE Is Using Location Data From Games and Apps to Track and Arrest Immigrants, Report Says*, VICE, (Feb. 7, 2020), https://www.vice.com/en/article/v7479m/ice-is-using-location-data-from-games-and-apps-to-track-and-arrest-immigrants-report-says.
[207] *See id*.
[208] *See* Joseph Cox, *Secret Service Bought Phone Location Data from Apps, Contract Confirms*, MOTHERBOARD (VICE) (Aug. 17, 2020), https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street.
[209] *See* Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Data Without Warrants, Memo Says*, N.Y. TIMES (Jan. 22, 2021), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html.
[210] Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, WALL ST. J. (Jun. 19, 2020), https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815. Although more is known about the practice at the federal level, state and local law enforcement also have been caught buying information about social media users from data vendors. *See* Kristina Cooke, *U.S. police used Facebook, Twitter data to track protestors: ACLU*, REUTERS (Oct. 11, 2016), https://www.reuters.com/article/us-social-media-data-idUSKCN12B2L7.

This warrantless collection of Americans' cell phone location information — potentially in massive amounts — would seem to violate the Supreme Court's holding in *Carpenter*. But agency lawyers have found a way around the case law. They have construed *Carpenter* to apply only when the government *compels* companies to disclose location information.[211] When the government merely *incentivizes* such disclosure — by writing a big check — the warrant requirement simply disappears. At that point, the argument goes, the government may obtain this Fourth Amendment-protected information in unlimited quantities without any individualized suspicion of wrongdoing, let alone probable cause and a warrant. This is legal sophistry, but it could take years for the courts to resolve the issue. In the meantime, the government has effectively sidelined the Fourth Amendment when it comes to data purchases.

Another apparent barrier to these purchases — the Electronic Communications Privacy Act (ECPA) — has also proven inadequate. ECPA prohibits phone and Internet companies from disclosing customer records to government agencies unless the government produces a warrant, court order, or subpoena.[212] But it includes broad exemptions for foreign intelligence surveillance.[213] Moreover, the law is woefully outdated. It does not cover digital data brokers or many app developers, for the simple reason that they did not exist in 1986, when the law was passed. This gap creates an easy end-run around the law's protections. Companies that are prohibited from selling their data to the government can simply sell it to a data broker — a disturbingly common practice[214] — and the data broker can resell the same information to the government, at a handsome profit. The information is effectively laundered through a middleman.

These combined gaps — in FISA, in the government's reading of Fourth Amendment case law, and in ECPA — leave the government free to collect some of the most sensitive information Americans generate, and to do so inside or outside the United States, without statutory authorization or judicial oversight. That is presumably how the CIA came to operate a bulk collection program that pulls in Americans' data, to be retrieved through backdoor searches and used for unknown purposes.

For foreign intelligence investigations, there's a simple way to fix the problem: amend FISA's exclusivity rule to encompass all of FISA's provisions. Specifically, Congress could provide that the provisions of FISA, insofar as they authorize the collection of Americans' information or searches of Americans' property, constitute the exclusive means by which such collection or searches may occur for foreign intelligence purposes. Without this modest step, many of the protections Congress wrote into FISA will become largely optional.

---

[211] *See* Savage, *Intelligence Analysts*, *supra* note 209; Hamed Aleaziz & Caroline Haskins, *DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People*, BUZZFEED NEWS (Oct. 30, 2020), https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation.

[212] 18 U.S.C. § 2702.

[213] 50 U.S.C. § 2511(2)(a)(ii), (e), & (f).

[214] In 2020, for example, Federal Communications Commission Chairman Ajit Pai proposed fines totaling $208 million after major mobile phone carriers like T-Mobile, Verizon, and Sprint were caught selling their consumers' real-time location data to data brokers without their knowledge or consent. *See* Jon Brodkin, *Senate Bill Would Ban Data Brokers from Selling Location and Health Data*, ARS TECHNICA (Jun. 15, 2022), https://arstechnica.com/tech-policy/2022/06/senate-bill-would-ban-data-brokers-from-selling-location-and-health-data/.

But Congress should go further and use the opportunity presented by the Section 702 sunset to close the data broker loophole completely — i.e., not just for foreign intelligence investigations. Congress should make clear that the government may not purchase Americans' personal information if compelled disclosure of that information would require a warrant, court order, or subpoena. The Fourth Amendment Is Not For Sale Act,[215] a bill introduced in the last Congress by Senators Ron Wyden and Rand Paul and by Representatives Jerrold Nadler and Zoe Lofgren, would go a long way toward accomplishing this goal.[216]

2. Update the Law to Reflect the Supreme Court's Decision in *Carpenter v. United States*

Since 1967, the Fourth Amendment has been understood to apply whenever the government intrudes on a "reasonable expectation of privacy."[217] For decades, however, the protections that flowed from this analysis were artificially constrained by the "third-party doctrine." First articulated in *United States v. Miller* (1976)[218] and reiterated in *Smith v. Maryland* (1978),[219] the doctrine holds that a person loses any expectation of privacy in information that he or she voluntarily discloses to another — no matter how limited or necessary the disclosure.

Arguably, this doctrine never made much sense. Most of us do not understand "private" to mean "secret"; we don't assume that information is private only if we never share it with another living soul. Rather, we understand privacy to be about controlling when and with whom we share information. The fact that a person might choose to confide in a spouse, relative, or even a group of trusted friends does not mean that she wants or expects the information to be widely available to the public.

Nonetheless, whatever sense the third-party doctrine might have made in the 1970s when it was established, it is wholly untenable today. Documents once stored in a desk at home are now frequently backed up to the cloud, accessible to the cloud service provider. Letters once sealed against inspection by the U.S. Post Office have become texts or emails, sent and stored by the companies that provide those services. Searches through card catalogues in the local library have turned into internet searches, generating search and web browsing records stored by internet service providers. And while it was once possible to pay a private visit, our cell phones — and therefore, our cell phone service providers — know where we are at all times, whether we are visiting a public park, a therapist, or Alcoholics Anonymous. In short, it is effectively impossible to go 24 hours without disclosing highly sensitive information to the multitude of third parties that manage life in the digital world.

The Supreme Court has begun the long process of bringing the Fourth Amendment in line with these new realities. In 2018, in *Carpenter v. United States*,[220] the Court held that police

---

[215] H.R. 2738, 117th Cong. (2021); S. 1265, 117th Cong. (2021).
[216] *See* Elizabeth Goitein, *The government can't seize your digital data. Except by buying it*., WASH. PO. (Apr. 26, 2021), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/.
[217] *See* Katz v. United States, 389 U.S. 347 (1967).
[218] 425 U.S. 435 (1976).
[219] 442 U.S. 735 (1979).
[220] 138 S. Ct. 2206 (2018).

officers need a warrant to compel cell phone companies to turn over historical cell site information for a seven-day period. The Court concluded that individuals retain a reasonable expectation of privacy in that information despite "sharing" it with a third party (their cell phone companies). Its reasoning was essentially twofold. First, comprehensive geolocation information, unlike the items of information at issue in *Miller* (bank deposit slips) and *Smith* (phone numbers transmitted over a particular line), can reveal the most intimate details of a person's associations and activities — what the Court referred to as "the privacies of life."[221] Second, disclosure of one's location though the use of a cell phone cannot fairly be described as "voluntary," given that the only alternative is to forego cell phone use and — along with it — participation in modern life.

Unfortunately, the holding in *Carpenter* is limited to the facts of that case. The Court expressly declined to consider what other types of information might qualify for Fourth Amendment protection despite being disclosed to a third party. There is no way to predict when cases involving other instances of third-party collection might come before the Court. We might well have to wait many years to discover how the Court will apply the principles articulated in *Carpenter* to comprehensive communications metadata, internet search and web browsing histories, DNA analyses, and multiple other categories of highly sensitive data. The Court also refrained from opining on whether warrants would be required to obtain cell site location information in national security or foreign intelligence investigations. To the extent this data collection takes place under Executive Order 12333, courts might never have the opportunity to weigh in on this question.

Americans' Fourth Amendment rights should not hang in the balance for years or longer while each use-case scenario wends its way through the courts. When the Supreme Court held in 1967 that the government needed a warrant to wiretap calls made from a phone booth, Congress moved swiftly to codify the principles articulated in that decision through Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[222] Congress should take similar action now, using the principles set forth in *Carpenter* to identify additional categories of highly sensitive information that merit the protection of a warrant regardless of whether they are held by third parties. In addition to communications content and geolocation data, those categories should include:

- *Communications metadata*. As noted above, accumulated communications metadata can reveal intimate associations, habits, and even beliefs; indeed, it can be every bit as revealing as communications content.
- *Internet search and web browsing records*. These records can provide a window into the most private thoughts of Internet users. In 2020, the Senate voted 59-37 in favor of a bipartisan amendment offered by Senators Steve Daines and Ron Wyden that would have imposed a warrant requirement for such records.[223]

---

[221] *Carpenter*, 138 S. Ct. 2210 (quoting Riley v. California, 573 U.S. 373, 403 (2014) (internal quotation marks omitted)).

[222] Pub. L. 90-351 (1968) (codified at 34 U.S.C. § 10101 *et seq*.).

[223] *See* Niels Lesniewski, *Senate amends surveillance bill to add new oversight*, ROLL CALL (May 13, 2020), https://rollcall.com/2020/05/13/senate-may-have-the-votes-to-limit-surveillance-of-browser-history/.

- *Biometric information*. Governmental access to biometric information (including fingerprints, retinal scans, DNA, etc.) carries extreme risks to privacy and associational rights, and has become a tool of persecution in countries like China and Iran.[224]
- *Health information*. Records pertaining to an individual's mental and physical health are among the most sensitive records that we entrust to third parties, and we reasonably expect the contents of those records to remain private.

In short, there is no reason why Americans' privacy should be held hostage to the slow pace of litigation. Congress should fill in the contours of the picture the Supreme Court began to paint in *Carpenter*, applying the principles the Court set forth to create statutory warrant protections where they are most clearly needed.

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 gain warrantless access to Americans' communications and other personal information in ways that circumvent FISA and the Constitution and violate court-ordered policies. At the same time, anachronistic limitations on FISA's reach and other gaps in the law are rendering Americans' personal information vulnerable to warrantless surveillance outside of any statutory framework and without judicial oversight. With the scheduled expiration of Section 702 this year, Congress has the opportunity — and the responsibility — to bring the law in line with Americans' constitutional rights and legitimate privacy expectations.

---

[224] Isabelle Qian et al., *Four Takeaways From a Times Investigation Into China's Expanding Surveillance State*, N.Y. TIMES (updated Jul. 26, 2022), https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html; Charlie Campbell, *'The Entire System Is Designed to Suppress Us.' What the Chinese Surveillance State Means for the Rest of the World*, TIME (Nov. 21, 2019), https://time.com/5735411/china-surveillance-privacy-issues/; STEVEN FELDSTEIN, THE GLOBAL EXPANSION OF AI SURVEILLANCE (Carnegie Endowment for Int'l Peace 2019), https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847; Frank Hersey, *Surveillance states: life in the facial recognition spotlight in China, Iran, and India*, BIOMETRIC UPDATE (Jan. 12, 2023), https://www.biometricupdate.com/202301/surveillance-states-life-in-the-facial-recognition-spotlight-in-china-iran-and-india; Shrutika Gandhi, *Biometric Identity Cards, Surveillance and Discrimination of Religious Minorities in Iran*, IRAN PRESS WATCH (Mar. 24, 2021), https://iranpresswatch.org/post/22195/biometric-identity-cards-surveillance-discrimination-religious-minorities-iran/. Facial recognition technology is even more problematic, given its inaccuracy when used to identify women and persons of color. *See* Steve Lohr, *Facial Recognition Is Accurate, if You're a White* Guy, N.Y. TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html. For that reason, many advocates and lawmakers have called for a moratorium or even a total ban on the use of this technology. *See* Facial Recognition and Biometric Technology Moratorium Act of 2021, H.R. 3907, 117th Cong. (2021); S. 2052, 117th Cong. (2021); American Civil Liberties Union, *Coalition Letter Calling for a Federal Moratorium on Face Recognition* (Jun. 3, 2019), https://www.aclu.org/letter/coalition-letter-calling-federal-moratorium-face-recognition.