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

HEARING ON

OVERSIGHT OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

DECEMBER 11, 2025

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 drug 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 next 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 Office of the Director of National Intelligence ("ODNI"), the government conducted more than thirteen thousand *known* searches of Section 702 data in 2024 for the purpose of finding Americans' communications and other personal information — though the FBI's failure to track all of its searches means that the actual number may be much higher. 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.

Recent changes to Section 702 have heightened the program's impact on Americans' privacy. The Reforming Intelligence and Securing America Act ("RISAA"), enacted in April 2024, authorized the government to compel surveillance assistance from a dizzying range of U.S. companies and organizations, vastly expanding the potential reach of Section 702 surveillance. The Foreign Intelligence Surveillance Court ("FISA Court") also recently approved the government's request to collect data related to international narcotics trafficking — collection that the Court acknowledged is likely to result in acquisition of a larger volume of Americans' communications. Additionally, RISAA authorized entirely suspicionless searches of Section 702 data for the purpose of vetting individuals seeking to travel to the United States, increasing the number of overall searches that in turn risk retrieving Americans' data for review.

Moreover, since the inception of the program, the rules designed to protect Americans' privacy have been 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. Breaches in recent years have involved baseless searches for the communications of protesters, journalists, campaign contributors, and members of Congress. Between 2018 and 2024, Section 702 required the FBI to obtain a warrant before accessing Section 702 data about Americans in a subset of criminal investigations; over the six years this requirement was in place, the FBI *never* complied with it.

Since RISAA was passed, FISA Court opinions and a Department of Justice Office of Inspector General ("OIG") report suggest that the rate of violations by the FBI has decreased.

However, OIG cautions that it is much too soon to conclude that the pattern of violations is in the past. More fundamentally, there is an enormous caveat to these bodies' findings. For one of the methods it was using to search Section 702 data, the FBI failed to follow the procedural requirements mandated by law, including the requirements to obtain attorney approval and record the factual basis for searches that target U.S. persons. Because the government did not track or audit these queries, the number of U.S. person searches and the rate of violations that took place when FBI agents used this method remain unknown.

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 backdoor search loophole that enables government officials to access Americans' phone calls, text messages, and emails without a warrant. It also means walking back RISAA's radical expansion of the types of U.S. entities that may be obligated to assist in the government's Section 702 surveillance; ending suspicionless travel-vetting queries; strengthening Section 702's reverse-targeting and minimization requirements; and right-sizing the scope of Section 702 surveillance targets.

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. RISAA compounded the problem by limiting the issues *amici curiae* are permitted to address and weighting *amici* selection towards former government personnel. Congress must strengthen *amici* participation at the FISA Court — and other mechanisms for judicial review — to ensure that there is meaningful oversight of the government's surveillance.

Finally, it is 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 next 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.

[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/.

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, 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 targeting 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 ("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

---

[2] 50 U.S.C. § 1805.
[3] 50 U.S.C. § 1801(a), (b)(1).
[4] 50 U.S.C. § 1801(b)(2).
[5] 50 U.S.C. § 1801(f).
[6] National Commission 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, July 22, 2004.
[7] *See* Electronic Privacy Information Center, "PATRIOT Act," Electronic Privacy Information Center, accessed June 11, 2023, https://epic.org/issues/surveillance-oversight/patriot-act/; Kate Tummarello, "Debunking the Patriot Act as It Turns 15," Electronic Frontier Foundation, October 26, 2016, https://www.eff.org/deeplinks/2016/10/debunking-patriot-act-it-turns-15.
[8] *See* Offices of Inspectors General, Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency and Office of the Director of National Intelligence, *Report on the President's Surveillance Program*, July 10, 2009, 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," Project on Government Oversight, September 7, 2021, https://www.pogo.org/analysis/2021/09/secrets-surveillance-and-scandals-the-war-on-terrors-unending-impact-on-americans-private-lives.

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 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 the foreign affairs of the United States."[14]

The Attorney General and the Director of National Intelligence make annual certifications, which historically have included broad categories of foreign intelligence information the government seeks to acquire, and submit general procedures for the surveillance to the FISA Court.[15] The Court approves the certifications and procedures but has no role in approving individual targets.[16] Currently, the government may obtain foreign intelligence information under four certifications covering the following topics: foreign governments and related entities; counterterrorism; combating the proliferation of weapons of mass destruction; and protecting against certain types of international drug activity.[17]

---

[9] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," New York Times, December 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.," New York Times, December 12, 2014, https://www.nytimes.com/2014/12/13/us/politics/documents-shed-new-light-on-legal-wrangling-over-spying-in-us-.html.

[11] *Modernizing the Foreign Intelligence Surveillance Act, Hearing Before the S. Select Comm. on Intelligence*, 110th Cong., May 1, 2007 (statement for the record of J. Michael McConnell, Director of National Intelligence), https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-hearings-110399.pdf.

[12] Protect America Act of 2007, Pub. L. 110-55, 121 Stat. 552 (2007), https://uscode.house.gov/statutes/pl/110/140.pdf.

[13] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (2008), https://uscode.house.gov/statutes/pl/110/261.pdf.

[14] 50 U.S.C. § 1801(e)(2).

[15] 50 U.S.C. § 1881a(h); Office of the Director of National Intelligence, "ODNI Releases February 2025 FISC Certification D Opinion and April 2025 FISC Amended Certification D Opinion and Agency Procedures," August 19, 2025, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2025/4099-pr-23-25.

[16] 50 U.S.C. § 1881a.

[17] Memorandum Opinion and Order, *In re DNI/AG 702(h) Certifications 2025-A, 2025-B, 2025-C, and Predecessor Certifications*, Nos. 702(j)-25-01, 702(j)-25-02, 702(j)-25-03, and predecessor dockets (FISA Ct. March 18, 2025),

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 foreign targets. 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.[18] The second type of Section 702 surveillance is "downstream collection," also known as "PRISM," under which the government provides selectors, such as e-mail addresses, to U.S.-based electronic communication service providers, who must turn over any communications to or from the selector.[19]

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.[20] 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 89,138 targets in 2013[21] to 291,824 targets in 2024[22] — 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'

---

https://www.intelligence.gov/assets/documents/702-documents/declassified/2025/FISC_Opinion_Cert_ABC_03182025_Redacted.pdf; Memorandum Opinion and Order, *In re DNI/AG 702(h) Certification 2024-D*, Nos. 702(j)-24-04 (FISA Ct. April 9, 2025), https://www.intel.gov/assets/documents/702-documents/declassified/2025/FISC_Opinion_2_Apr_2025_2024_Cert_D_Redacted_8-19-25_final.pdf; Office of the Director of National Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2023* at 16, April 2024, https://www.intelligence.gov/assets/documents/702-documents/statistical-transparency-report/2024_ASTR_for_CY2023.pdf [hereinafter ODNI, Annual Statistical Transparency Report: Calendar Year 2023].

[18] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 174–78, 2023, https://documents.pclob.gov/prod/Documents/OversightReport/d21d1c6b-6de3-4bc4-b018-6c9151a0497d/2023%20PCLOB%20702%20Report,%20508%20Completed,%20Dec%203,%202024.pdf [hereinafter 2023 PCLOB 702 Report].

[19] *Id.* at 64–65.

[20] Memorandum Opinion and Order, [Redacted], No. [Redacted], 2011 WL 10945618, at *29 (FISA Ct. October 3, 2011). In addition, the Privacy and Civil Liberties Oversight Board reported that, "as of 2021, NSA acquired approximately 85.3 million internet transactions per year in upstream collection, which constitutes a small percentage of NSA's Section 702 collection." 2023 PCLOB 702 Report, *supra* note 18, at 178.

[21] Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities: Annual Statistics for Calendar Year 2013*, June 2014, https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.

[22] Office of the Director of National Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2024* at 22, May 2025, https://www.intelligence.gov/assets/documents/702-documents/statistical-transparency-report/ASTR_CY24.pdf, [hereinafter ODNI, Annual Statistical Transparency Report: Calendar Year 2024].

communications in large numbers, although it has rebuffed lawmakers' requests[23] to provide a rough estimate of how many Americans' communications are collected.[24] 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.[25] 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, and sharing of U.S. person information.[26] 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 to gain access to the communications of "particular, known" Americans.[27]

---

[23] *See* Senators Ron Wyden and Mark Udall to I. Charles McCullough III (Inspector General of the Intelligence Community, Office of the Director of National Intelligence), and Dr. George Ellard (Inspector General, National Security Agency), May 4, 2011, 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," July 12, 2012, https://www.wyden.senate.gov/news/press-releases/senators-seek-answers-from-dni-on-how-many-of-americans-communications-have-been-monitored; Rep. John Conyers, Jr., et al., to James Clapper (Director Of National Intelligence), April 22, 2016, https://www.brennancenter.org/sites/default/files/legal-work/Letter_to_Director_Clapper_4_22.pdf; Reps. Bob Goodlatte and John Conyers to Daniel Coats (Director of National Intelligence), April 7, 2017, https://drive.google.com/file/d/1uaCE_5atwxhh0opdXdtekdHaZ7FqPI4V/view.

[24] Initially, the government claimed that providing such an estimate would itself violate Americans' privacy. *See* I. Charles McCullough, III (Inspector General of the Intelligence Community, Office of the Director of National Intelligence), to Sens. Ron Wyden and Mark Udall, June 15, 2012, https://www.wyden.senate.gov/download/?id=E5DEF293-A8D6-4014-A23A-909C82A3C510&download=1. After privacy experts and advocates refuted that claim, *see* Brennan Center for Justice, et al., to James Clapper (Director of National Intelligence), October 29, 2015, 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* U.S. House Comm. on the Judiciary Democrats, "Bipartisan House Coalition Presses Clapper for Information on Phone & Email Surveillance," December 16, 2016, https://democrats-judiciary.house.gov/media-center/press-releases/bipartisan-house-coalition-presses-clapper-for-information-on-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, June 12, 2017, http://www.reuters.com/article/us-usa-intelligence-idUSKBN19031B, and the Biden administration took a similar approach.

[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. § 1881a(e).

[27] 50 U.S.C. § 1881a(b)(2), (h)(2)(A)(iii).

Over the past 17 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 runs electronic searches designed to locate and retrieve the communications of particular Americans. The resulting privacy intrusion is exacerbated by recent changes in the law that further expanded the scope of surveillance authorized by Section 702 and the purposes for which Section 702 data may be searched.

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."[28] 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."[29]

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 downstream collection under three of the four current certifications with the FBI, the CIA, and the National Counterterrorism Center ("NCTC").[30] All four agencies generally may keep unreviewed raw data — including

---

[28] 50 U.S.C. § 1801(h)(1).

[29] 50 U.S.C. § 1801(h)(3).

[30] *See* Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department of Justice, *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § 9, January 13, 2025, https://www.intel.gov/assets/documents/702-documents/declassified/2025/NSA_MPs_2025_Cert_ABC_01172025_Redacted.pdf [hereinafter 2025 NSA 702 Minimization Procedures] (minimization procedures for three of the four current certifications, i.e., Certifications A, B, and C). The minimization procedures for Certification D, adopted in April 2025, allow the NSA to share raw data with the CIA but not the FBI or the NCTC. Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department of Justice, *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Concerning the International Production, Distribution, or Financing of Certain Illicit Drugs Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended* § 9, December 11, 2024, https://www.intel.gov/assets/documents/702-documents/declassified/2025/NSA_MPs_2024_Cert_D_12-16-24_Redacted_8-19-25_final.pdf [hereinafter 2025 NSA 702 Cert D Minimization Procedures]. Because the procedures for this new certification differ from those for prior certifications, this Part's discussion is limited to the minimization procedures for Certifications A, B, and C. Certification D is discussed in more detail *infra* in Part II.C.1.

data about U.S. persons — for five years after the certification expires;[31] they also can seek extensions from a high-level official,[32] and the NSA and FBI expressly exempt encrypted communications (which are becoming increasingly common among ordinary users of mobile devices) from the 5-year limit.[33] The agencies may keep indefinitely any U.S. person information that has foreign intelligence value or is evidence of a crime.[34]

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.[35] The NSA, however, maintains that data with no apparent foreign intelligence value "may have foreign intelligence value in the future or for another concurrent investigation." [36] Accordingly, "communications are rarely purged before their designated age-off date."[37]

The FBI, CIA, and NCTC have no affirmative requirement to purge irrelevant U.S. person data on detection, relying instead on age-off requirements.[38] Moreover, if the FBI reviews U.S. person information and *does not identify it* as foreign intelligence information or evidence

---

[31] 2025 NSA 702 Minimization Procedures, *supra* note 30, at § 4(c)(1)–(2) ; Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department 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, January 13, 2025, https://www.intel.gov/assets/documents/702-documents/declassified/2025/FBI_MPs_2025_Cert_ABC_01172025_Redacted.pdf [hereinafter 2025 FBI 702 Minimization Procedures]; Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department 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, January 13, 2025, https://www.intel.gov/assets/documents/702-documents/declassified/2025/CIA_MPs_2025_Cert_ABC_01172025_Redacted.pdf [hereinafter 2025 CIA 702 Minimization Procedures]; Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department 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, January 13, 2025, https://www.intel.gov/assets/documents/702-documents/declassified/2025/NCTC_MPs_2025_Cert_ABC_01172025_Redacted.pdf [hereinafter 2025 NCTC 702 Minimization Procedures].

[32] 2023 PCLOB 702 Report, *supra* note 18, at 78; 2025 NCTC 702 Minimization Procedures, *supra* note 31, at § B.2.a.; 2025 FBI 702 Minimization Procedures, *supra* note 31, at §III.I.1; 2025 NSA 702 Minimization Procedures, *supra* note 30, at § 7(1); 2025 CIA 702 Minimization Procedures, *supra* note 31, at § 2.a.

[33] 2025 NSA 702 Minimization Procedures, *supra* note 30, at § 7(1)a; 2025 FBI 702 Minimization Procedures, *supra* note 31, at § III.I.4. The CIA has also historically permitted communications to be retained indefinitely if they are "enciphered or contain[] secret meaning." *See* Lisa O. Monaco, Deputy Attorney General, U.S. Department 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* § 3.c, October 14, 2021, https://www.intelligence.gov/assets/documents/702-documents/declassified/2024/2024_Cert_CIA_MPs_for_Public_Redacted_3-13-23.pdf [hereinafter 2024 CIA 702 Minimization Procedures].

[34] 2025 NSA 702 Minimization Procedures, *supra* note 30, at §§ 6(2), 7(3); 2025 FBI 702 Minimization Procedures, *supra* note 31, at §§ III.A.3, III.C.1.b; 2025 CIA 702 Minimization Procedures *supra* note 31, at §§ 2.a, 3, 8; 2025 NCTC 702 Minimization Procedures, *supra* note 31, at §§ B.2.a, B.3, B.4, C.4.

[35] 2025 NSA 702 Minimization Procedures, *supra* note 30, at § 4(b)(1).

[36] 2023 PCLOB 702 Report, *supra* note 18, at 78.

[37] *Id.*

[38] *Id.* at 78–80.

of a crime, the 5-year limit evaporates, and the FBI may keep the data for 15 years.[39] A similar rule applies to the NCTC.[40]

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.[41]

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. Backdoor Searches

Perhaps the most glaring failure of the protections Congress put in place for Americans' privacy is the practice of "backdoor 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 who the government just certified were not intended targets.[42] 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 "pre-assessment" and "assessment" phases of its investigations[43] — i.e., before agents have a factual basis to suspect a national security threat or criminal activity, let alone probable cause and a warrant.[44] 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,

---

[39] 2025 FBI 702 Minimization Procedures, *supra* note 31, at § III.D.4.c.
[40] 2025 NCTC 702 Minimization Procedures, *supra* note 31, § B.2.b.
[41] 2025 NSA 702 Minimization Procedures, *supra* note 30, at § 8(2), (9); 2025 FBI 702 Minimization Procedures, *supra* note 31, at § IV.A.1–2, B; 2025 CIA 702 Minimization Procedures, *supra* note 31, at §§ 5.a, 7.d; 2025 NCTC 702 Minimization Procedures, *supra* note 31, at § D.1–2. In addition, the FBI may disseminate unminimized Section 702 data to the NSA, CIA, and in some cases the NCTC. 2025 FBI 702 Minimization Procedures, *supra* note 31, at § IV.E.
[42] 2025 NSA 702 Minimization Procedures, *supra* note 30, § 4(b)(4); 2025 FBI 702 Minimization Procedures, *supra* note 31, at § III.D.3; 2025 CIA 702 Minimization Procedures, *supra* note 31, at § 4; 2025 NCTC 702 Minimization Procedures, *supra* note 31, at § C.1.
[43] 2023 PCLOB 702 Report, *supra* note 18, at 11.
[44] *Id.* at 38–39.

the FBI conducted up to *3.4 million* U.S. person queries of federated data systems that included Section 702 data.[45]

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," the number of U.S. person queries reportedly conducted by the FBI dropped to around 200,000;[46] following additional changes to internal querying procedures, the number dropped further in 2023 to 57,094.[47] While that represents a sizeable decrease, it is still an enormous number by any standard, comprising more than 150 warrantless searches for Americans' communications each day.

The number of backdoor searches conducted by the FBI in 2024 is unknown. In September 2024, the Department of Justice's National Security Division ("NSD") notified the FISA Court that it was evaluating the FBI's use of a particular tool known as an "advanced filter function."[48] When using this tool to retrieve the communications of particular targets, FBI agents could select from a list of "participants" who were in contact with those targets and review those participants' communications. Although this functionality enabled FBI to search for U.S. persons' communications, the FBI did not consider these searches to be queries and therefore did not track them or, presumably, follow required querying procedures (such as obtaining attorney approval and providing a written justification for U.S. person queries). After the NSD determined that these searches constituted queries, it informed the FISA Court that it "'does not presently have access to historical data' . . . and is coordinating with FBI to assess what records of the use of this functionality may have been generated and maintained."[49] Without such records, data on the number of U.S. person queries in 2024 — and perhaps other years — is incomplete.

This failure to track an entire category of queries could help to explain an otherwise perplexing drop in the number of *reported* queries to 5,518 in 2024.[50] Both the FISA Court and the OIG attribute this drop in part to reforms made by RISAA. Yet, as OIG acknowledges

---

[45] Office of the Director of National Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2021* at 21, April 2022, https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf, [hereinafter ODNI, Annual Statistical Transparency Report: Calendar Year 2021].

[46] Office of the Director of National Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2022* at 24, April 2023, https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf [hereinafter ODNI, Annual Statistical Transparency Report: Calendar Year 2022]. 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.

[47] ODNI, Annual Statistical Transparency Report: Calendar Year 2023, supra note 17, at 25.

[48] Memorandum Opinion and Order, *In re DNI/AG 702(h) Certifications 2025-A, 2025-B, 2025-C*, Nos. 702(j)-25-01, 702(j)-25-02, 702(j)-25-03, supra note 17, at 40.

[49] *Id.*

[50] ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 6.

elsewhere in the report,[51] most of those reforms — including several of those highlighted by OIG as being the most significant — simply codified changes the FBI had already implemented well before RISAA's enactment.[52] The few additional changes made by RISAA might explain some portion of the subsequent drop in reported queries, but it is highly implausible that they alone caused a decline of more than 90%.

Even if the number of U.S. person queries reported by the FBI in 2024 could be taken at face value, 5,518 warrantless searches of private communications would still represent a gross intrusion on U.S. persons' privacy and civil liberties. The government is able to present that number as a success story only because the FBI conducted *3.4 million* U.S. person queries in 2021. But a burglar should not escape condemnation for robbing a house — let alone be applauded for his restraint — simply because he robbed an entire neighborhood three years ago. The shockingly low bar the government set in 2021 cannot be used as the measure of Americans' rights. Moreover, there was a significant *increase* in the number of U.S. person queries conducted by the CIA, NSA, and NCTC during this period — from 4,684 in 2022 to 7,845 in 2024.[53] In total, the U.S. government conducted 13,363 known warrantless searches of Americans' emails, text messages, and phone calls in 2024.

Government officials have defended backdoor searches, claiming that as long as information is lawfully acquired, agencies may use the information for any legitimate government purpose.[54] This argument 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 one FISA Court judge 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."[55] Whatever merit the government's

---

[51] *See* Oversight and Review Division, Office of the Inspector General, Department of Justice, *A Review of the Federal Bureau of Investigation's Querying Practices Under Section 702 of the Foreign Intelligence Surveillance Act* 13–14, October 2025, https://oig.justice.gov/sites/default/files/reports/26-002_0.pdf [hereinafter 2025 OIG Report].

[52] *Compare* Reforming Intelligence and Securing America Act, Pub. L 118-49, § 2(b), (d), 138 Stat. 862, 862–65 (2024), https://www.congress.gov/118/plaws/publ49/PLAW-118publ49.pdf [hereinafter RISAA], *with Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities, Hearing Before the S. Comm. on the Judiciary*, 118th Cong., June 13, 2023 (joint statement for the record of Chris Fonzone, General Counsel, Office of the Director of National Intelligence, et al.), https://www.judiciary.senate.gov/imo/media/doc/2023-06-13%20-%20Joint%20statement%20-%20ODNI,%20NSA,%20CIA,%20FBI,%20DOJ%20(1).pdf, *and* ODNI, Annual Statistical Transparency Report: Calendar Year 2022, *supra* at note 46, at 22.

[53] ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 25.

[54] *See, e.g.*, *The FISA Amendments Act: Reauthorizing American's Vital National Security Authority and Protecting Privacy and Civil Liberties Reauthorization, Hearing Before the S. Comm. on the Judiciary*, 115th Cong. (June 27, 2017), C-SPAN, 44:02, (testimony of Stuart J. Evans, Deputy Assistant Attorney General for Intelligence, National Security Division, Department of Justice), https://www.c-span.org/program/senate-committee/fisa-reauthorization/481407; *Oversight of Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities, Hearing Before the S. Comm. on the Judiciary*, 118th Cong. 14, 27 (June 13, 2023) (testimony of Matthew G. Olsen, Assistant Attorney General for National Security, Department of Justice), https://www.congress.gov/118/chrg/CHRG-118shrg58969/CHRG-118.

[55] [Redacted], 2011 WL 10945618, *supra* note 20, at *27.

defense might or might not have in other contexts,[56] 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.[57] In December 2024, a district court judge held that the Fourth Amendment applies to backdoor searches and that the searches at issue in the case were unconstitutional.[58] Outside of the courts, constitutional scholars have assessed that

[56] 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); United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010) ("[O]fficers and others involved in searches of digital media [must] exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described."). 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. *See* 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.").

[57] *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).

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. *See* United States v. Mohamud, 2014 WL 2866749, at *26 (D. Oregon 2014); United States v. Hasbajrami, 2016 WL 1029500, at *12 n.20 (E.D.N.Y. 2016); United States v. Al-Jayab, No. 16 CR 181, at 55–56 (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 Security*, August 24, 2018, https://www.justsecurity.org/60439/americans-privacy-stake-circuit-hears-hasbajrami-fisa-case/ (explaining the misrepresentation on which the court relied). In fact, none of the agencies' minimization procedures require them to review communications to determine whether they must be minimized. *See generally* 2025 NSA 702 Minimization Procedures, *supra* note 30; 2025 FBI 702 Minimization Procedures, *supra* note 31; 2025 CIA 702 Minimization Procedures, *supra* note 31; 2025 NCTC 702 Minimization Procedures, *supra* note 31. Indeed, such a review would be literally impossible, given that the government collects close to a billion communications per year under Section 702. *See* Part I, *supra.*

[58] United States v. Hasbajrami, No. 1:11-CR-623 (LDH), 2025 WL 447498, at *5–9, *16 (E.D.N.Y. February 10, 2025)

backdoor searches must be treated as a Fourth Amendment event that is separate from the underlying collection,[59] thus generally triggering the warrant requirement.[60]

C. Recent Expansions of Section 702 Surveillance

Recent changes to the collection of communications under Section 702 have heightened the program's impact on Americans' privacy, underscoring the need for reform. RISAA dramatically (and unnecessarily) expanded the types of entities that can be compelled to assist the government in Section 702 surveillance. It also amended the definition of "foreign intelligence" to include information relating to international narcotics trafficking, and it authorized suspicionless queries of Section 702 for the purpose of vetting individuals seeking to travel to the United States. The first change creates massive potential for abuse, while all three changes increase the volume of Americans' communications that may be collected "incidentally" and/or retrieved through warrantless searches.

1. Expanded Definition of "Electronic Communication Service Provider"

The government conducts Section 702 surveillance with the compelled assistance of "electronic communication service providers" ("ECSPs"),[61] generally by requiring them to turn over the communications of targets identified by the government.[62] In 2023, the FISA Court ruled that FISA's definition of "electronic communication service provider" did not cover a specific type of provider[63] — reportedly, a data center for cloud computing.[64] The Biden

---

[59] *See* Barry Friedman and Danielle Keats Citron, "Indiscriminate Data Surveillance," *Virginia Law Review* 110, no. 6 (2024): 1403–04, 1410 n.258; *see also* Orin Kerr, "The Fourth Amendment and Querying the 702 Database for Evidence of Crimes," Washington Post, October 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/.

[60] 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). In addition, the district court that ruled certain backdoor searches unconstitutional recognized a much broader version of this exception. *See Hasbajrami,* 2025 WL 447498, *supra* note 58, at *13–16; *see also* Hannah James, "The Dangerous Foreign Intelligence Exception Loophole in the Hasbajrami Decision," *Just Security*, April 7, 2025, https://www.justsecurity.org/109879/foreign-intelligence-exception-hasbajrami/. The Supreme Court has not recognized any such 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 government's current practice with regard to U.S. person queries. *See* Elizabeth Goitein and Faiza Patel, *What Went Wrong with the FISA Court* 11-12, Brennan Center for Justice, March 14, 2015, https://www.brennancenter.org/our-work/research-reports/what-went-wrong-fisa-court (discussing case law on foreign intelligence exception).

[61] 50 U.S.C. § 1881a(i).

[62] *See* 2023 PCLOB 702 Report, *supra* note 18, at 34, 54.

[63] *See* Opinion and Order, *In re: Petition to Set Aside or Modify Directive Issued to [Redacted]*, Nos. [Redacted], (FISA Ct. Rev. 2023), https://www.intel.gov/assets/documents/702-documents/declassified/2023_FISC-R_ECSP_Opinion.pdf.

[64] *See* Charlie Savage, "Secret Rift Over Data Center Fueled Push to Expand Reach of Surveillance Program," New York Times, April 16, 2024, https://www.nytimes.com/2024/04/16/us/fisa-surveillance-bill-program.html.

administration solicited an amendment to RISAA that would expand the ECSP definition. Because the type of provider was (and remains) classified, however, the amendment was deliberately drafted using vague and broad language to conceal the type of provider at issue. It was unveiled three days before the House voted on it, leaving members with little time to investigate assurances that the amendment was a narrow fix to address a specific FISA Court decision.[65] In reality, while the issue the amendment sought to address was a narrow one, the amendment itself, enacted in RISAA, is a truly breathtaking expansion of surveillance authority.

The provision expands the ECSP definition to include not only providers of communication services, like Verizon and Gmail, but providers of *any service* (with certain narrow exceptions), as long as they have access to equipment on which communications are transmitted or stored.[66] This change vastly inflates the universe of entities that can be compelled to assist the government in Section 702 collection. Almost every public-facing business or organization, large or small, provides some type of "service," and they all have access to communications equipment (e.g., phones and computers). The new definition sweeps in grocery stores, barber shops, fitness centers, places of worship, and a host of other establishments frequented by the American public. It also encompasses the commercial landlords that lease office space where tens of millions of Americans go to work every day.[67]

Although the government is still limited to collecting the communications of foreign targets, this sea change in the law has direct consequences for, and poses alarming risks to, Americans' privacy. For one thing, expanding the range of entities from which the government may compel assistance increases the volume of communications it can collect, which in turn increases the number of Americans' communications that may "incidentally" be obtained. Moreover, unlike Verizon or Gmail, many of the businesses covered by the expanded definition lack the ability to isolate and turn over particular communications. Their only option may be to give NSA personnel access to the relevant equipment. That, in turn, would give the NSA access to *all* the communications transmitted through or stored on the equipment, including purely domestic communications between and among Americans. NSA would be on the "honor system" to pull out and retain only the communications of valid foreign targets.

Put simply, this provision potentially gives the NSA the authority to directly access the communications equipment of nearly every business and organization in the United States. The potential for abuse in a system that provides such broad access is difficult to overstate. It is for this reason that Senator Ron Wyden described the amended ECSP definition as "one of the most

---

[65] *See* Rebecca Beitsch, "Intelligence Community Largely Won House FISA Fight. Now Comes the Senate," The Hill, April 16, 2024, https://thehill.com/homenews/house/4596017-intelligence-community-largely-won-house-fisa-fight-now-comes-the-senate/; 170 Cong. Rec. H2354 (daily ed., April 12, 2024) (statement of Rep. Mike Turner).

[66] *See* RISAA, supra note 52, at § 25(a)(3). In response to criticism of an earlier version of the amendment, *see, e.g.*, Marc Zwillinger and Steve Lane, "House Intelligence Committee FISA 'Reform' Bill Would Greatly Expand the Class of Businesses and Other Entities Required to Assist in FISA 702 Surveillance," *ZwillGenBlog,* December 8, 2023, https://www.zwillgen.com/law-enforcement/fisa-reform-bill-702-surveillance/, its drafters excluded hotels, residential buildings, food service establishments, and community facilities (such as libraries and hospitals) in the final version. *See* 50 U.S.C. § 1881(b)(4)(E).

[67] *See* Elizabeth Goitein, "The FISA Expansion Turning Cable Installers Into Spies Cannot Stand," The Hill, April 17, 2024, https://thehill.com/opinion/technology/4599695-the-fisa-expansion-turning-cable-installers-into-spies-cannot-stand/.

dramatic and terrifying expansions of government surveillance authority in history."[68] Tacitly conceding the danger of the expanded definition, the Biden administration made a public commitment to apply it only to the specific type of provider at issue in the FISC opinion and to notify Congress when requiring such providers' assistance.[69] However, that commitment is not binding on the current administration nor on future ones.

2. International Narcotics Trafficking

RISAA also amended the definition of "foreign intelligence information" to include "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . international production, distribution, or financing of illicit synthetic drugs, opioids, cocaine, or other drugs driving overdose deaths, or precursors of any aforementioned."[70] Pursuant to this change, the government in April 2025 obtained FISA Court approval of a new certification authorizing acquisition of foreign intelligence information "concerning the international production, distribution, or financing of illicit opioids [redacted] or cocaine."[71]

Both the collection and the querying authorized under this certification have significant implications for Americans' privacy. As the FISA Court observed, the threat sought to be addressed under this certification "encompasses a domestic component . . . [i]ndeed, the domestic impact . . . is what makes the threat posed by international trafficking so significant."[72] This domestic nexus increases the likelihood that Americans' communications will be "incidentally" collected. Moreover, because information at the collection stage "need only bear on, or have some relation to" the ability of the United States to protect against the threat of drug trafficking,[73] the FISA Court expressed "concern[] that the NSA and CIA might acquire a larger number of communications of or concerning U.S. persons, including those engaged in purely legitimate business" under this certification.[74]

This certification also poses unique concerns regarding the use of Section 702 data for ordinary crime control. As the FISA Court recognized, there is "inherent overlap" between what constitutes foreign intelligence information as defined in the certification and evidence of ordinary drug crime.[75] As a result, the government is more likely both to acquire evidence of ordinary crime under this certification and to retrieve such evidence through its foreign-

---

[68] Ron Wyden, "Wyden: 'I Will Do Everything In My Power' to Stop Bill Expanding Government Surveillance Under FISA 702," April 12, 2024, https://www.wyden.senate.gov/news/press-releases/wyden-i-will-do-everything-in-my-power-to-stop-bill-expanding-government-surveillance-under-fisa-702.
[69] Carlos Felipe Uriarte (Assistant Attorney General, U.S. Department of Justice) to Sen. Mark Warner, (Chairman, Senate Select Comm. on Intelligence), April 17, 2024, https://www.justice.gov/opa/media/1348621/dl?inline.
[70] 50 U.S.C. § 1801(e)(1)(D).
[71] *See In re DNI/AG 702(h) Certification 2024-D*, Nos. 702(j)-24-04 (April 9, 2025), *supra* note 17, at 2.
[72] Memorandum Opinion and Order, *In re DNI/AG 702(h) Certification 2024-D*, Nos. 702(j)-24-04, at 49–50 (FISA Ct. February 20, 2025), https://www.intelligence.gov/assets/documents/702-documents/declassified/2025/FISC_Opinion_1_Feb_2025_2024_Cert_D_Redacted_8-19-25_final.pdf.
[73] *Id.* at 25.
[74] *In re DNI/AG 702(h) Certification 2024-D*, No. 702(j)-24-04 (April 9, 2025), *supra* note 17, at 6.
[75] *In re DNI/AG 702(h) Certification 2024-D*, Nos. 702(j)-24-04 (February 20, 2025), *supra* note 72, at 7.

intelligence queries.[76] The statute then permits the government to disseminate that information for law enforcement purposes.[77]

In short, the certification facilitates scenarios in which "evidence of drug-related crime will have been collected without a warrant, identified through a subsequent query using a U.S. person identifier . . . and then used for a non-foreign intelligence law-enforcement purpose."[78] Such scenarios stray far from the intent of Section 702 and from the constitutional safeguards ordinarily present in domestic criminal investigations.

3. Suspicionless Queries for Travel Vetting

The primary substantive restriction on queries of Section 702 data is that they must be reasonably likely to retrieve foreign intelligence information. RISAA created an exception to that restriction in a provision that requires agencies' querying procedures to "enable the vetting of all non-United States persons who are being processed for travel to the United States using terms that do not qualify as United States person query terms."[79] The provision permits entirely suspicionless searches of individuals seeking to travel to the United States — whether on student or work visas or as tourists and business travelers — even when the multiple other vetting mechanisms used by the government have not revealed any basis for believing that the individual poses a threat to the United States.

The provision has an obvious and significant impact on non-U.S. persons, whose private communications can now be searched simply because they apply to travel to the United States. The provision impacts Americans' privacy, too. Any query of Section 702 information runs the risk of returning communications that involve Americans. Because querying for the purposes of travel vetting increases the number of queries run — presumably by a significant amount, considering the United States issued more than 11 million visas in 2024[80] — it increases the chance that Americans' private communications will be accessed as a result of those queries.[81] Moreover, given the suspicionless nature of the queries, any U.S. person communications that are retrieved are highly likely to contain innocuous private conversations rather than foreign intelligence.

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,

---

[76] *Id*. at 7, 60.
[77] 50 U.S.C. § 1801(h)(3).
[78] *In re DNI/AG 702(h) Certification 2024-D*, Nos. 702(j)-24-04 (April 9, 2025), *supra* note 17, at 60.
[79] *See* RISAA, *supra* note 52, at § 24.
[80] *See* U.S. Department of State, *Summary of Visas Issued by Issuing Office Fiscal Year 2024* at 6, 2025, https://travel.state.gov/content/dam/visas/Statistics/AnnualReports/FY2024AnnualReport/Table%20IV.pdf.
[81] Visa applicants are unlikely to be Section 702 targets themselves, so any communications retrieved by travel vetting queries are likely to be communications between the applicants and targets, both of whom must be non-U.S. persons. However, such communications could involve U.S. persons as additional participants (e.g., in group emails or text chats).

or dissemination can result in Americans being investigated without proper legal basis or sensitive information falling into the hands of people who could misuse it. But violations in recent years raise even more acute concerns: the use of foreign intelligence surveillance powers against Americans based on their race, ethnicity, politics, or journalistic activity. The government has been quick to celebrate improved rates of compliance since 2023, glossing over the potentially significant gaps in compliance information and the serious compliance incidents that have occurred.

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 not designed to extract foreign intelligence information in a very small subset of cases, i.e., predicated criminal investigations unrelated to national security.[82] This provision was 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 "pre-assessment" and "assessment" stages — i.e., before the FBI has sufficient information to open a predicated investigation.[83] Nonetheless, according to the ODNI's statistical transparency reports, the requirement was triggered on at least 100 occasions over six years.[84] Incredibly, the FBI did not obtain a FISA Court order in a *single one* of those cases.[85]

---

[82] FISA Amendments Reauthorization Act of 2017, Pub. L. 115-118, § 101(a)(1)(B), 132 Stat. 3, 4 (2017), https://www.govinfo.gov/content/pkg/PLAW-115publ118/pdf/PLAW-115publ118.pdf.

[83] 2023 PCLOB 702 Report, *supra* note 18, at 11.

[84] Office of the Director of National Intelligence, *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2020* at 21, April 2021, https://www.dni.gov/files/CLPT/documents/2021_ASTR_for_CY2020_FINAL.pdf [hereinafter ODNI, Annual Statistical Transparency Report: Calendar Year 2020]; ODNI, Annual Statistical Transparency Report: Calendar Year 2021, *supra* note 45, at 22; ODNI, Annual Statistical Transparency Report: Calendar Year 2022, *supra* note 46, at 26; ODNI, Annual Statistical Transparency Report: Calendar Year 2023, *supra* note 17, at 27. 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." ODNI, Annual Statistical Transparency Report: Calendar Year 2020, *supra* note 84, at 20. 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.

[85] *See* ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 27; ODNI, Annual Statistical Transparency Report: Calendar Year 2020, *supra* note 84, at 21. 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." Memorandum Opinion and Order, [Redacted], No. [Redacted], at 69–70 (FISA Ct. December 6, 2019), https://www.intelligence.gov/assets/documents/702-documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf (emphasis added). Specifically, systems would display query results in a summary field that showed 100 characters of text around the query term within the records identified as responsive to the query. According to the FISA Court, however, "FBI personnel are known to

In 2024, Congress replaced the court order requirement with an outright prohibition on queries "solely designed to find and extract evidence of criminal activity."[86] There are two exceptions to the prohibition: (1) queries to retrieve information that could assist in mitigating a threat to life or serious bodily harm; and (2) queries to identify information that must be produced or preserved in connection with litigation, including criminal matters. Though touted as a significant reform,[87] this prohibition in fact impacts a very small number of queries — of the more than 57,000 U.S. person queries conducted in 2023, this provision would have prohibited the FBI from accessing Section 702 data in only four cases.[88] Moreover, because the FBI did not track all of its queries in 2024 (as discussed further below), there is no way to determine whether the FBI has fully complied with the prohibition. What official statistics *do* show is a conspicuous six-fold increase in the querying and accessing of Section 702 data for the ostensible purpose of meeting litigation obligations[89] — one of the two circumstances under which the FBI may still perform evidence-of-a-crime only queries.

For the vast majority of U.S. person queries (those that are not solely designed to find and extract evidence of criminal activity), the only substantive restriction on queries is the standard set forth in the FBI's querying procedures. 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, unless otherwise specifically excepted in these procedures."[90] This is a fairly low bar, to be sure. Even so, government reports and FISA Court opinions show that the FBI has engaged in a pattern of "widespread violations" of this rule.[91]

In 2018, the FISA Court expressed "serious concern" about "the large number of [FBI] queries evidencing a misunderstanding of the querying standard — or indifference to it."[92] The Court posited that the reported violations were likely the tip of the iceberg. It noted that Department of Justice overseers, at that time, "review[ed] only a small portion of the queries conducted," making it "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."[93] The Court ultimately found that the FBI's querying and minimization procedures,

---

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." *Id.* at 70. In any event, this feature did not account for all of the violations.

[86] 50 U.S.C. § 1881a(f)(2)(A).

[87] *See, e.g.*, 170 Cong. Rec. H2329 (daily ed. April 12, 2024) (statement of Rep. Jim Himes).

[88] *See* ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 27, 31.

[89] *See* ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 31.

[90] *See* Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department 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., January 17, 2025, https://www.intel.gov/assets/documents/702-documents/declassified/2025/FBI_QPs_2025_Cert_ABC_01172025_Redacted.pdf.

[91] Memorandum Opinion and Order, [Redacted], No. [Redacted], at 44 (FISA Ct. November 18, 2020), https://www.intel.gov/assets/documents/702-documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf.

[92] Memorandum Opinion and Order, [Redacted], No. [Redacted], 402 F. Supp. 3d 45, 72 (FISA Ct. October 18, 2018).

[93] *Id*. at 74.

as implemented, were inconsistent with both the requirements of FISA and the Fourth Amendment.[94]

The FBI responded by implementing several measures designed to improve compliance through enhanced training, oversight and approval requirements, and changes to data systems access. Many of these measures were later codified in RISAA. Nonetheless, over the next four years, the FISA Court continued to observe "widespread violations of the querying standard by the FBI."[95] The "[l]arge-scale, suspicionless queries of Section 702 information [that] contributed to a finding of deficiency in the FBI's querying and minimization procedures . . . remained a concern . . . in April 2022."[96] Indeed, in March 2022, the government submitted a notice to the FISA Court in which it reported more than 278,000 non-compliant FBI queries of raw FISA-acquired information.[97]

The violations that took place during this period are memorialized in FISA Court opinions, compliance reports, and the PCLOB's report on Section 702. In 2020, for instance, FBI agents conducted 141 backdoor searches for the communications of people who had protested the police killing of George Floyd, despite having "no information connecting the individuals or the conduct to information that would be contained in FBI's Section 702-acquired information."[98] The following year, agents ran thousands of searches relating to the January 6 attack on the U.S. Capitol, also on a baseless hunt for evidence of foreign ties.[99] In total, between November 2020 and December 2021, "non-compliant queries related to civil unrest numbered in the tens of thousands."[100] Agents ran additional searches for information about members of Congress;[101] a congressional candidate;[102] a congressional chief of staff;[103] a local political

---

[94] *Id.* at 133–34.
[95] [Redacted], No. [Redacted] (FISA Ct. December 6, 2019), *supra* note 85, at 65.
[96] Memorandum Opinion and Order, *In re DNI/AG 702(h) Certification 2023-A and its Predecessor Certifications*, Nos. 702(j)-23-01, 702(j)-23-02, 702(j)-23-01, and predecessor dockets, at 87 (FISA Ct. April 11, 2023), https://www.intelligence.gov/assets/documents/702-documents/declassified/2023/FISC_2023_FISA_702_Certifications_Opinion_April11_2023.pdf.
[97] *See* Memorandum Opinion and Order, [Redacted], No. [Redacted], at 31 (FISA Ct. April 21, 2022), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf.
[98] 2023 PCLOB 702 Report, *supra* note 18, at 150–51.
[99] [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 28–29.
[100] 2023 PCLOB 702 Report, *supra* note 18, at 151.
[101] *See* Department of Justice and Office of the Director of National 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, December 2021, https://www.intelligence.gov/assets/documents/702%20Documents/declassified/24th-Joint-Assessment-of-FISA-702-Compliance.pdf [hereinafter DOJ & ODNI, Semiannual Assessment December 2021]; 2023 PCLOB 702 Report, *supra* note 18, at 155.
[102] *See* Department of Justice and Office of the Director of National 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* 48 n.89, March 2023, https://www.intel.gov/assets/documents/702-documents/declassified/27th_Joint%20Assessment_for%20PUBLIC_1.15.25.pdf [hereinafter DOJ & ODNI, Semiannual Assessment March 2023].
[103] *Id.*

party;[104] multiple U.S. government officials, journalists, and political commentators;[105] 19,000 donors to a political campaign;[106] and two "Middle Eastern" men who were reported by a witness because they were loading boxes labeled "Drano" into a vehicle.[107]

These incidents carry echoes of the politically and racially motivated surveillance abuses that occurred under the reign of J. Edgar Hoover. That is alarming, but it should not be surprising. When government officials are not required to show probable cause of criminal activity to a court, it greatly 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;[108]
- victims who approached the FBI to report crimes;[109]
- business, religious, and community leaders who applied to participate in the FBI's "Citizens Academy";[110]
- college students participating in a "Collegiate Academy";[111]
- police officer candidates;[112]
- colleagues and relatives of the FBI agent performing the search;[113]
- people traveling through an airport during a particular date range who were either traveling to or returning from a foreign country;[114]
- registered competitors in an athletic event;[115]
- visitors to a government facility;[116]
- potential FBI sources;[117] and

[104] DOJ & ODNI, Semiannual Assessment December 2021, *supra* note 101, at 58.
[105] Department of Justice and Office of the Director of National 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, August 2021, https://www.intel.gov/assets/documents/702%20Documents/declassified/22nd_Joint_Assessment_of_FISA_702_Compliance_CLEARED_REDACTED_FOR_PUBLIC_RELEASE.pdf.
[106] [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 29.
[107] DOJ & ODNI, Semiannual Assessment December 2021, *supra* note 101, at 61.
[108] [Redacted], No. [Redacted] (FISA Ct. November 18, 2020), *supra* note 91, at 40.
[109] *Id.*
[110] *Id*. at 39.
[111] [Redacted], No. [Redacted] (FISA Ct. December 6, 2019), *supra* note 85, at 66.
[112] *Id.*
[113] [Redacted], 402 F. Supp. 3d 45, *supra* note 92, at 78.
[114] 2023 PCLOB 702 Report, *supra* note 18, at 148.
[115] *Id.* at 149.
[116] *Id.*; [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 32.
[117] 2023 PCLOB 702 Report, *supra* note 18, at 149–50; [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 27–28.

- an individual who invited the agent that conducted the search to speak at their company.[118]

The government has heralded "significant improvement" in FBI compliance in the past two years,[119] but the reality is much more nuanced. For one thing, even after the FBI implemented many of the reforms that were ultimately codified in RISAA and compliance rates began to increase, serious abuses continued. For instance, the FISA Court's April 2023 opinion revealed that FBI agents had conducted improper queries for the communications of a U.S. Senator, a state senator, and a state court judge who contacted the FBI to report civil rights violations by a local police chief.[120] In light of the FBI's poor compliance history, OIG stated in its October 2025 report that it was "not able to conclude . . . that FBI's querying compliance issues are entirely in the past."[121]

More fundamentally, FBI has not produced complete data on its queries. As discussed above, the FBI in 2024 (and possibly before then) employed at least one querying tool that agents wrongly treated as exempt from the statutory and court-ordered requirements applicable to queries. At a minimum, as OIG found, the queries conducted using this tool "likely did not comply with the pre-approval, written justification, and recordkeeping requirements for U.S. person queries" because the system did not prompt users to take these steps.[122] Nor did NSD conduct the statutorily required audit of these queries. These failures alone constitute significant and possibly extensive violations of RISAA.

Moreover, because the system "had not been configured to record each use of the participants filter, NSD did not have historical data that would enable NSD to determine whether each use of the function complied with the query standard."[123] It is possible, as OIG acknowledged, that "these queries may have included sensitive queries or queries designed solely to retrieve evidence of a crime," as well as "an unspecified number of [other] compliance incidents."[124] Indeed, given that FBI agents were not following the pre-approval, written justification, and recordkeeping requirements — requirements that the government itself credits for improved compliance rates — one would expect to see a higher rate of violations among

---

[118] See Department of Justice and Office of the Director of National Intelligence, *28th 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* 54, February 2024, https://www.intel.gov/assets/documents/702-documents/declassified/28th_Joint_Assessment_for_PUBLIC_1.15.25.pdf.

[119] *See, e.g.*, Federal Bureau of Investigation, "Release of 2023 Foreign Intelligence Surveillance Court Opinion Highlights FBI's Improved Section 702 Query Compliance," July 21, 2023, https://www.fbi.gov/news/press-releases/release-of-2023-foreign-intelligence-surveillance-court-opinion-highlights-fbis-improved-section-702-query-compliance.

[120] *In re DNI/AG 702(h) Certification 2023-A*, Nos. 702(j)-23-01, 702(j)-23-02, 702(j)-23-01, *supra* note 96, at 86.

[121] 2025 OIG Report, *supra* note 51, at 51.

[122] *Id*. at 49.

[123] *Id.*

[124] *Id.* at 48, 49.

these queries.[125] And the fact that all of these queries have escaped review means that significant abuses could well have gone undetected.

Without complete data on how many queries were conducted in 2024 or whether these queries complied with applicable standards, Congress cannot evaluate the FBI's querying record post-RISAA. As of the March 2025 FISA Court opinion, NSA was "coordinating with FBI to assess what records of the use of this functionality may have been generated and maintained."[126] Congress should exercise active oversight to ensure that the FBI is providing any and all information in its possession about the use of this querying tool, and it should not reauthorize Section 702 until it is has a more complete picture of the FBI's querying practices since RISAA's enactment.

B. Other Violations

The FBI's querying violations in recent years are merely one subset of the compliance problems that have attended the government's implementation of Section 702. The program's seventeen-year history has been marked by repeated, significant, and sometimes systemic failures to comply with statutory requirements or court orders. These failures have taken place under multiple foreign intelligence collection authorities (including Section 702) and at all points of the programs: collection, access, dissemination, and retention.

My written testimony before this Committee in July 2023 highlighted several of the most notable compliance failures that occurred between 2008-2023. These include the NSA's systemic violations of querying restrictions over a period of nearly a decade; the FBI's over-retention of Section 702 data in violation of minimization requirements; the NSA's "institutional lack of candor" (as described by the FISA Court); and the FBI's widespread non-compliance with procedures designed to ensure the accuracy of its FISA Court submissions.[127] Since that testimony, serious compliance incidents have only continued to emerge.

One such incident involved repeated misapplication of the NSA's tasking standards (the rules governing when the NSA can target someone and collect their communications).[128] A review by the NSA Office of the General Counsel and NSD identified at least 571 tasking errors

---

[125] U.S. person queries conducted using this tool run against a pool of communications obtained through an initial query that retrieves communications associated with a particular case file or target. The government asserts that *if* that initial query was compliant, "most, but not necessarily all, queries conducted through the [participants filter] likely would have satisfied the applicable query standard" because the second query is "narrower" than the first. 2025 OIG Report, *supra* note 51, at 49. This reasoning makes little sense. While the retrieval of *all* of a foreign target's communications (through the initial query) might reasonably be expected to yield some foreign intelligence, it does not follow that communications with specific U.S. person participants can be assumed to contain foreign intelligence.

[126] *In re DNI/AG 702(h) Certifications 2025-A, 2025-B, 2025-C*, Nos. 702(j)-25-01, 702(j)-25-02, 702(j)-25-03, *supra* note 17, at 40.

[127] *See Fixing FISA, Part II, Hearing Before the H. Comm. on the Judiciary*, *Subcomm. On Crime and Federal Government Surveillance*, 118th Cong. 17–22, July 14, 2023 (testimony of Elizabeth Goitein, Senior Director, Liberty and National Security Program, Brennan Center for Justice), https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/goitein-testimony.pdf..

[128] *In re DNI/AG 702(h) Certification 2023-A*, Nos. 702(j)-23-01, 702(j)-23-02, 702(j)-23-01, *supra* note 96, at 94–95.

in a single office, errors that the NSA attributed to a "misunderstanding" of tasking guidance provided in 2016 and 2018.[129] The review concluded that "many targeting decisions had been improper because the target was not reasonably expected to possess or receive, and was not likely to communicate, foreign intelligence information related to [redacted]."[130]

The implementation of newly approved travel-vetting procedures has also been accompanied by several compliance incidents, including improper U.S. person queries. The FISA Court recounted one incident involving an undisclosed number of violations of the rules limiting queries related to certain visa applications from individuals "expected to be located in the United States and with United States home addresses."[131] In another incident, the NSA conducted multiple non-compliant queries related to applications submitted by legal permanent residents, who are U.S. persons under the law.[132]

In 2024, the CIA disclosed a significant compliance issue with its main FISA repository. The CIA is required by statute to include a technical procedure to record each U.S. person query term used,[133] and CIA querying procedures require personnel to document the justification for U.S. person queries.[134] For an undisclosed period of time (but at least three years), users were able to conduct certain free-text queries of the CIA's main FISA repository without being prompted to specify whether the query used a U.S.-person term or to enter a justification for any U.S. person queries.[135] The CIA's review of such free-text queries conducted between 2021 and April 2024 identified over 10,000 queries that CIA assessed could have included U.S. person query terms conducted without these prompts.[136]

Perhaps most concerning, the FISA Court's September 2024 opinion, issued five months after RISAA's passage, includes six pages of entirely redacted material under the heading: "Reported Intentional Violations at [Redacted]."[137] Due to the redactions, it is impossible to ascertain the agency at which the violations were reported or which aspect of Section 702 implementation they involved. The FISA Court cautioned that "[t]he underlying facts are still

---

[129] *Id.*
[130] *Id.*
[131] Memorandum Opinion and Order, *In re DNI/AG 702(h) Certifications 2024-A, 2024-B, 2024-C, and Predecessor Certifications*, Nos. 702(j)-24-01, 702(j)-24-02, 702(j)-24-03, and predecessor dockets, at 94 (FISA Ct. September 17, 2024), https://www.intelligence.gov/assets/documents/702-documents/declassified/2024/2024_Sep_702_Cert_FISC_Opinion_9-17-24_Redacted.pdf.
[132] *In re DNI/AG 702(h) Certification 2023-A*, Nos. 702(j)-23-01, 702(j)-23-02, 702(j)-23-01, *supra* note 96, at 51, n.36; *In re DNI/AG 702(h) Certifications 2024-A, 2024-B, 2024-C*, Nos. 702(j)-24-01, 702(j)-24-02, 702(j)-24-03, *supra* note 131, at 69.
[133] 50 U.S.C. § 1881a(f)(1)(B).
[134] *See* Matthew G. Olsen, Assistant Attorney General, National Security Division, U.S. Department 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.B., July 18, 2024, https://www.intel.gov/assets/documents/702-documents/declassified/2024/2024_Sep_702_Cert_Amended_CIA_Querying_Procedures_Redacted.pdf.
[135] *In re DNI/AG 702(h) Certifications 2024-A, 2024-B, 2024-C*, Nos. 702(j)-24-01, 702(j)-24-02, 702(j)-24-03, *supra* note 131, at 102.
[136] *Id.* The FISA Court assessed that "the probable number of actual U.S. person queries was substantially lower." *Id.* at 103 n.75. However, the court's basis for its conclusion is redacted.
[137] *In re DNI/AG 702(h) Certifications 2024-A, 2024-B, 2024-C*, Nos. 702(j)-24-01, 702(j)-24-02, 702(j)-24-03, *supra* note 131, at 96–102.

being investigated" and so the misconduct described in the opinion "should be understood as alleged, not established."[138] Nonetheless, such an extensive recounting of reported *intentional* misconduct is cause for significant concern.

The long, unbroken string of violations detailed here and in my 2023 testimony 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 sustained 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 and continuing 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, narrow the definition of "electronic communication service provider," and end suspicionless queries for travel-vetting, among other changes. For these reforms to be effective, however, Congress must go beyond Section 702. It also must address broader problems in FISA by strengthening the role of *amici curiae* in FISA Court proceedings and otherwise bolstering judicial oversight. 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, such as the purchase of Americans' sensitive information from data brokers.

A. Protecting Americans' Privacy Under 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 a probable-cause order — i.e., either a warrant or a Title I FISA Court order — before running queries designed to extract communications content or other Fourth Amendment-protected information (such as geolocation data) of or concerning U.S. persons. 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

[138] *Id.* at 96.

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.

During the last Section 702 reauthorization, Congress considered an amendment that would have required agency officials to obtain a warrant or a FISA Title I order before accessing the content of U.S. persons' communications, with exceptions for consent, exigent circumstances, and certain cybersecurity-related queries. (The amendment failed by the narrowest possible margin: a tied vote of 212-212.[140]) Those who opposed this reform claimed it would harm national security.[141] They will no doubt make the same claim during the debate over next year's reauthorization. But the program's seventeen-year track record shows otherwise.

The government has provided multiple examples in which *surveillance of foreign targets* provided key information about cyberattacks, espionage, and fentanyl trafficking. By contrast, after a thorough review of all of the relevant classified and unclassified information, the PCLOB found in its 2023 report that "there was little justification provided to the Board on the relative value of the close to 5 million searches [U.S. person queries] conducted by the FBI from 2019 to 2022."[142] The government cited only a handful of instances in which backdoor searches for Americans' communications had been useful. In each of those cases, it appeared that the government could have obtained a warrant, gotten the consent of the subject of the search (for instance, where the search was conducted for the purpose of identifying and protecting potential

---

[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 Improvement and Reauthorization Act of 2005, Pub. L. 109-177, § 102(b)(2), 120 Stat. 192, 195 (2006), https://www.govinfo.gov/content/pkg/PLAW-109publ177/pdf/PLAW-109publ177.pdf (as amended by Pub. L. 116-69, § 1703(a), 133 Stat. 1134, 1143 (2019), https://www.congress.gov/116/plaws/publ69/PLAW-116publ69.pdf).

[140] H. Amdt. 876, H.R. 7888, 118th Cong. (2024), https://www.congress.gov/amendment/118th-congress/house-amendment/876.

[141] In the same vein, 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." *See* Christopher Wray Director, Federal Bureau of Investigation, "*Defending the Values of FISA Section 702,*" October 13, 2017, https://www.fbi.gov/news/speeches/defending-the-value-of-fisa-section-702; Privacy and Civil Liberties Oversight Bd., *PCLOB Public Forum on FISA Section 702,* YouTube, January 12, 2023, at 1:57:28 (comments of Mike Herrington, Senior Operations Advisor, FBI), https://www.youtube.com/watch?v=AZvaimMTqio&t=357s. This notion is utterly baseless. "The wall" refers to a set of pre-9/11 procedures that — in practice, if not on paper — restricted intelligence officials' ability to share identified threat information with criminal prosecutors. *See* Barbara A. Grewe, Senior Counsel for Special Projects, Commission on Terrorist Attacks Upon the United States, *Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations*, August 20, 2004, https://irp.fas.org/eprint/wall.pdf.

The information in question was obtained under Title I of FISA, which means the government had *already* secured a probable-cause order at the point in the case where "the wall" kicked in. *See id.* at 29. 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. *See generally* Coolidge v. New Hampshire, 403 U.S. 443 (1971) (discussing "plain view" exception); Horton v. California, 496 U.S. 128 (1990) (same). 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.

[142] 2023 PCLOB 702 Report, *supra* note 18, at 190.

victims of malicious foreign activity[143]), or invoked the emergency exception — a point confirmed by the Chair of the PCLOB.[144]

Some defenders of warrantless queries may argue that RISAA already closed the backdoor search loophole by prohibiting FBI queries for the sole purpose of retrieving evidence of a crime. As noted above, however, that prohibition applies only to a tiny fraction of U.S. person queries. Indeed, the worst abuses we have seen under Section 702 thus far have been couched as efforts to obtain foreign intelligence, not evidence of a crime — including queries of more than 100 U.S. persons involved in the protests against the police killing of George Floyd;[145] the FBI's batch query for the communications of more than 19,000 donors to a single congressional campaign;[146] the FBI's query using the name of then-U.S. Congressman Darrin LaHood;[147] and the thousands of queries aimed at people or groups suspected of involvement in the January 6, 2021 attack on the U.S. Capitol.[148]

Opponents of reform may claim that RISAA has reduced the FBI's number of U.S. person queries and its rate of non-compliance to acceptable levels. Any such claim would rest on a flawed premise. As noted above, the FBI failed to track all of its queries — itself a major compliance issue. As a result, the number of U.S. person queries and the overall compliance rate for 2024 remain unknown.

But even if the FBI had conducted only a handful of U.S. person queries and committed no violations of its querying procedures last year, 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 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."[149]

---

[143] In opposing the proposed warrant requirement, the government relied heavily on its use of U.S. person queries for "defensive" purposes — i.e., to protect potential victims. But 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 "victim" exception to the Fourth Amendment, however, nor does the Constitution draw any distinction between "offensive" or "defensive" searches or seizures.

[144] 2023 PCLOB 702 Report, *supra* note 18, at A6–A7.

[145] The FBI maintained (wrongly) that there was a "reasonable basis to believe the queries would return foreign intelligence." [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 27.

[146] This batch query was based on an allegation that the campaign was a target of "foreign influence." *Id.* at 29.

[147] The query was reportedly based on concerns that "a foreign government had targeted him as part of an espionage or covert influence intelligence operation." Charlie Savage, "FBI Feared Lawmaker Was Target of Foreign Intelligence Operation," New York Times, April 13, 2023, https://www.nytimes.com/2023/04/13/us/politics/fbi-darin-lahood.html.

[148] The FBI ran these queries seeking evidence of "foreign influence." [Redacted], No. [Redacted] (FISA Ct. April 21, 2022), *supra* note 97, at 29.

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

In fact, if the FBI indeed conducted "only" 5,518 warrantless searches for Americans' private communications in 2024, that would actually bolster the case for a warrant requirement. When the number of annual U.S. person queries stood at more than 200,000, the government argued that a warrant requirement would be unworkable and overwhelm the courts. That argument was unpersuasive, given that most legislative warrant requirement proposals would allow the FBI to determine whether the U.S. person was in communication with a target *before* obtaining the warrant. By the government's own statistics, this step would reduce the number of required warrant applications by 98%.[150] The government's "unworkability" argument is even less persuasive if the actual number of U.S. person queries today is closer to 5,000, thus requiring the FBI to obtain warrants in roughly 110 cases. The number of FISA Title I order applications submitted by the government each year routinely fluctuates by more than this amount.[151]

A warrant requirement would also solve a potential problem identified by the government during OIG's review. FBI employees interviewed by OIG expressed "concern" that "the extensive oversight" put in place in recent years "has caused 'audit fatigue' that has reduced the willingness of some FBI personnel to query Section 702-acquired information altogether."[152] In addition to the "administrative burden" of obtaining attorney approval and keeping records of U.S. person queries, agents are reportedly "concerned that they may be subject to disciplinary actions for running noncompliant queries" and may therefore refrain from conducting queries that would in fact be justified.[153]

The simplest way to address this purported issue[154] without a resurgence of querying violations is by placing the burden of gatekeeping these searches where it belongs: with a court. This would reduce the need for the multiple layers of internal oversight that have been established in a futile effort to replicate the function of judicial approval. It would also take away any motive for excessive caution; the only penalty if an agent submitted an application that turned out to lack sufficient basis would be the court's denial of the application. Agents would be free to do their jobs — i.e., to vigorously pursue their investigations consistent with the law and their professional obligations — while the courts would perform *their* job of determining whether the government has a lawful basis for searching Americans' private communications.

2. Fix the Definition of "Electronic Communication Service Provider"

In addition to closing the backdoor search loophole, Congress should walk back its radical expansion of the definition of "electronic communication service provider." As discussed above, the impetus for expanding the definition was a ruling by the FISA Court that the provision did not cover a particular type of provider.[155] The administration deliberately pressed for an overbroad solution in order to obscure the type of provider at issue. Alarmed at the

[150] 2023 PCLOB 702 Report, *supra* note 18, at 168, B-16.
[151] *See, e.g.*, ODNI, Annual Statistical Transparency Report: Calendar Year 2024, *supra* note 22, at 17.
[152] 2025 OIG Report, *supra* note 51, at 34.
[153] *Id.* at 48.
[154] The extent of this problem is unclear. The witnesses interviewed by OIG were relaying their perceptions of other agents' concerns; none of the witnesses acknowledged limiting their own searches as a result of the new oversight measures. *Id.* at 47.
[155] *See In re: Petition to Set Aside or Modify Directive Issued to [Redacted]*, Nos. [Redacted], *supra* note 63.

change, which the House had hastily adopted, several senators threatened to scuttle the reauthorization of Section 702. With the sunset fast approaching, the then-chair of the Senate Intelligence Committee, Senator Warner, conceded that the provision "could have been drafted better,"[156] but urged his colleagues to vote for reauthorization and promised to work to "improve the definition . . . before the next sunset."[157] No such improvement has passed to date, and the dangerously broad definition remains law.

The optimal solution would be for the administration to declassify the type of provider at issue, which would remove any concerns about Congress limiting the new definition to that type of provider. Declassifying the information would cause no harm to national security because it is already squarely in the public domain. The *New York Times* revealed in April 2024 that the relevant FISA Court decisions involved a data center for cloud computing.[158] That information has been confirmed by authoritative sources: During the Senate debate over this provision, multiple senators with access to classified FISA Court opinions, including Senator Warner himself, [159] either stated or implied that the provision was intended to address data centers.

Even if the administration fails to declassify this information, however, Congress can simply pass legislation stating that the new definition may be applied only to data centers for cloud computing. If the legislation does not expressly tie this change to the FISA Court opinions, it would not directly be revealing classified information. And while people might infer from the change that the FISA Court opinions in question addressed data centers, that inference can already be drawn from other sources, including the public statements of members of Congress.

Alternatively, Congress could adopt language proposed by Senator Warner that would limit the new definition to providers of "the type of service at issue in the covered opinions"—with "covered opinions" defined to include the two specific FISA Court opinions holding that a specific type of provider was not covered.[160] This solution is far from ideal, as incorporating classified opinions by reference creates a type of "secret law."[161] Among other concerns, companies that receive directives from the government requiring them to assist with Section 702 surveillance would face serious limitations in their ability to identify and challenge unlawful directives.[162] It would nonetheless be preferable to the status quo, under which NSA personnel may compel surveillance assistance from nearly every business and organization in the country.

3. End Suspicionless Queries for Travel Vetting

Congress should repeal the provision of RISAA authorizing suspicionless searches of Section 702 data for the communications of anyone seeking to travel to the United States. This invasive measure is wholly unnecessary given the multiple vetting mechanisms already in place

---

[156] 170 Cong. Rec. S2836 (daily ed. April 18, 2024) (statement of Sen. Warner).
[157] 170 Cong. Rec. S2837 (daily ed. April 18, 2024) (statement of Sen. Warner).
[158] *See* Charlie Savage, "Secret Rift," supra note 64.
[159] *See generally* 170 Cong. Rec. S2833–37 (daily ed. April 18, 2024).
[160] S. 4443, 118th Cong. § 1202 (2024).
[161] *See* Elizabeth Goitein, "Secret Law is not the Solution to an Overbroad Surveillance Authority," Brennan Center for Justice, June 11, 2024, https://www.brennancenter.org/our-work/analysis-opinion/secret-law-not-solution-overbroad-surveillance-authority.
[162] *See id.*

to ensure that visitors to this country do not threaten our national security. People should be able to vacation, work, or study in the U.S. without automatically exposing their private communications to U.S. government scrutiny. Allowing suspicionless queries for visa applicants' private communications unnecessarily intrudes on the privacy of such applicants, as well as the privacy of U.S. persons whose communications may be retrieved in response to such queries. Moreover, as noted above, the travel vetting program already has suffered from compliance problems leading to multiple improper U.S. person queries.

B. Bolstering Judicial Review by Restoring and Strengthening the Role of *Amici Curiae*

The FISA Court reviews applications to conduct electronic surveillance under Title I of FISA and to engage in other types of collection of Americans' information. The Court also approves Section 702 certifications and procedures and conducts general oversight of that program.

FISA Court proceedings are non-public and conducted *ex parte*, meaning the government is the only party.[163] The secrecy and one-sided nature of such 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.[164]

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.

RISAA partially addressed one of these problems by creating a presumption of *amicus* participation in Section 702 certification approvals. However, two other changes made by RISAA significantly undermined the effectiveness of *amici*. First, *amici* are now "limited to addressing the specific issues identified by the court."[165] The value of *amici* derives in significant part from their ability to raise issues and arguments the court has not considered. This provision places a handicap on *amici* that defeats the very purpose of their participation.

Second, the Court must "to the maximum extent practicable appoint an individual who possesses expertise in both privacy and civil liberties *and intelligence collection*" (emphasis added).[166] The practical consequence of this provision is that *amici* selection is heavily weighted

---

[163] *See* U.S. Foreign Intelligence Surveillance Court, "About the Foreign Intelligence Surveillance Court," accessed December 4, 2025, https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court.
[164] 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).
[165] 50 U.S.C. § 1803(i)(4)(A).
[166] 50 U.S.C. § 1803(i)(2)(B).

towards former government personnel, who may well come into the proceedings with institutional bias. The views of the government are more than adequately represented in FISA Court proceedings. Indeed, the need for perspectives *other* than the government's is what prompted the creation of the *amici* program in the first place.

Congress should repeal these provisions and strengthen *amici* participation by enacting the reforms to FISA Court proceedings set forth in the "Lee-Welch" amendment (previously known as the "Lee-Leahy" amendment).[167] Senators Mike Lee and Patrick Leahy initially offered this amendment to the USA FREEDOM Reauthorization Act of 2020.[168] Although Congress failed to pass the reauthorization bill, the amendment passed by an overwhelming bipartisan vote of 77-19.[169]

The amendment seeks to ensure that *amici* can weigh in on the most significant cases (in addition to Section 702 certification approvals), 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, including exculpatory materials in the government's possession; that *amici* can petition the FISA Court to certify questions for appeal; and that the government has in place FISA Court-approved procedures to ensure the accuracy of its submissions. 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.

C. Closing the Data Broker Loophole 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 often-overlapping 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.

One such gap exists within FISA's "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."[170] FISA's highly technical definition of "electronic surveillance"[171] 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

[167] S. Amdt. 1840, H.R. 7888, 118th Cong. (2024), https://www.congress.gov/amendment/118th-congress/senate-amendment/1840/text.
[168] S. Amdt. 1584, H.R. 6172, 116th Cong. (2020), https://www.congress.gov/amendment/116th-congress/senate-amendment/1584/text.
[169] *Id.* (as agreed to in Senate, May 13, 2020).
[170] 50 U.S.C. § 1812.
[171] 50 U.S.C. § 1801(f).

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 is 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 [Executive Order] 12333 authority can do all of this without Congress's permission, with no guardrails."[172] 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.

The information that the government may obtain outside of FISA can be extremely sensitive. Take the phone records that were the subject of the NSA's bulk collection program. 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.[173] This understanding led lawmakers to end the bulk collection program and ultimately Section 215 itself. In 2020, the Senate voted overwhelmingly in favor of a bipartisan amendment to impose a warrant requirement for internet search and browsing records, noting that they, too, reveal Americans' private thoughts and preferences.[174] 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.[175]

If the government wanted to obtain such information without adhering to FISA, one workaround would be to purchase it from data brokers. Such purchases have become an increasingly common practice in the federal government.[176] Multiple agencies have reportedly purchased access to Americans' cell phone location information and other sensitive data,

---

[172] *See* Richard Burr, "Sen. Burr Claims EO 12333 Permits Mass Surveillance 'Without Congress's Permission,'" U.S. Senate, streamed live on March 12, 2020, C-SPAN, 00:15, https://www.c-span.org/clip/us-senate/user-clip-sen-burr-claims-eo-12333-permits-all-of-this-without-congresss-permission/4860931.
[173] 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.
[174] 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/.
[175] Carpenter v. United States, 585 U.S. 296 (2018).
[176] *See* Emile Ayoub and Elizabeth Goitein, "Closing the Data Broker Loophole," Brennan Center for Justice, February 13, 2024, https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole.

including the Federal Bureau of Investigation,[177] the Drug Enforcement Administration,[178] the National Security Agency,[179] multiple components of the Department of Homeland Security[180] (including Immigration and Customs Enforcement[181] and Customs and Border Protection[182]), the Secret Service,[183] and the Department of Defense.[184] 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."[185] 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."[186]

---

[177] *See* Sara Morrison, "A Surprising Number of Government Agencies Buy Cellphone Location Data. Lawmakers Want to Know Why," *Vox*, December 2, 2020, https://www.vox.com/recode/22038383/dhs-cbp-investigation-cellphone-data-brokers-venntel; Ashley Belanger, "FBI Finally Admits to Buying Location Data on Americans, Horrifying Experts," *Ars Technica*, March 9, 2023, https://arstechnica.com/tech-policy/2023/03/fbi-finally-admits-to-buying-location-data-on-americans-horrifying-experts/; Byron Tau, "FBI Once Bought Mobile-Phone Data for Warrantless Tracking. Other Agencies Still Do," Wall Street Journal, March 10, 2023, https://www.wsj.com/articles/fbi-once-bought-mobile-phone-data-for-warrantless-tracking-other-agencies-still-do-ad65ebe9.

[178] *See* Morrison, "A Surprising Number," *supra* note 177.

[179] Charlie Savage, "N.S.A. Buys Americans' Internet Data Without Warrants, Letter Says," New York Times, January 25, 2024, https://www.nytimes.com/2024/01/25/us/politics/nsa-internet-privacy-warrant.html. The agency admitted that it purchased Americans' communications metadata from data brokers. Much like geolocation data, this information, when accumulated, can reveal intimate information like associations, habits, and beliefs. *See* American Civil Liberties Union v. Clapper, 785 F. Supp. 2d 724 (S.D.N.Y. 2013).

[180] Joseph Cox, "Airlines Don't Want You to Know They Sold Your Flight Data to DHS," *404 Media*, June 10, 2025, https://www.404media.co/airlines-dont-want-you-to-know-they-sold-your-flight-data-to-dhs/.

[181] *See* Joseph Cox, "ICE to Buy Tool that Tracks Locations of Hundreds of Millions of Phones Every Day," *404 Media*, September 30, 2025, https://www.404media.co/ice-to-buy-tool-that-tracks-locations-of-hundreds-of-millions-of-phones-every-day/; Paul Blest, "ICE Is Using Location Data From Games and Apps to Track and Arrest Immigrants, Report Says," *Vice*, February 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.

[182] *See* Joseph Cox, "ICE to Buy Tool," *supra* note 181; Paul Blest, "ICE Is Using Location Data," *supra* note 181.

[183] *See* Joseph Cox, "Secret Service Bought Phone Location Data from Apps, Contract Confirms," *Vice*, August 17, 2020, https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street.

[184] *See* Charlie Savage, "Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says," New York Times, January 22, 2021, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html.

[185] Byron Tau, "IRS Used Cellphone Location Data to Try to Find Suspects," Wall Street Journal, June 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 Americans' personal information from data vendors. *See* Kristina Cooke, "U.S. Police Used Facebook, Twitter Data to track Protestors - ACLU," Reuters, October 11, 2016, https://www.reuters.com/article/us-social-media-data-idUSKCN12B2L7; Bennett Cyphers, "How Law Enforcement Around the Country Buys Cell Phone Location Data Wholesale," Electronic Frontier Foundation, August 31, 2022, https://www.eff.org/deeplinks/2022/08/how-law-enforcement-around-country-buys-cell-phone-location-data-wholesale.

[186] Joseph Cox, "Revealed: U.S. Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data," *Vice*, September 21, 2021, https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data. The Federal Trade Commission later brought enforcement actions against one of those data brokers, Outlogic (formerly X-mode), for selling location data collected from popular prayer apps. Federal Trade Commission [hereinafter FTC], "FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data," January 9, 2024, https://www.ftc.gov/news-events/news/press-

A declassified report to ODNI released in June 2023 confirmed the extent of this practice, finding that intelligence agencies have been acquiring vast amounts of Americans' personal information from commercial entities.[187] The report explained that this commercially available information "includes information on nearly everyone that is of a type and level of sensitivity that historically could have been obtained, if at all, only through targeted (and predicated) collection."[188] It also warned that intelligence agencies have failed to keep track of the information they are acquiring and how they are using it.[189] Exacerbating these concerns, ODNI earlier this year reportedly proposed consolidating all of this commercially acquired information into a single "data consortium" accessible to intelligence agencies and potentially other agencies.[190]

The 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.[191] 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.

Agencies maintain that warrants are unnecessary even when a data broker obtains location information from mobile applications without the users' awareness.[192] In some instances, agencies have made disingenuous claims that consumers consent to the selling of their data by accepting applications' often-opaque terms of service. In emails obtained by 404 Media, for example, officials argued that the Secret Service could broadly collect location data without a

---

releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data. The FTC followed with enforcement actions against data brokers Gravy Analytics, Venntel, and Mobilewall — all of whom reportedly sold location data to government agencies. *See* FTC, "FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites," December 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers; FTC, "FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data," December 3, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data.

[187] Panel on Commercially Available Information, Office of the Director of National Intelligence Senior Advisory Group, *Report to the Director of National Intelligence*, January 27, 2022, https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf [hereinafter ODNI, *Report to ODNI*].

[188] *Id.* at 2–3, 14.

[189] *Id.* at 2, 21, 36 (finding that the intelligence community "does not currently have sufficient visibility into its own acquisition and use of CAI across its 18 elements" and "cannot understand and improve how it deals with CAI unless and until it knows what it is doing with CAI").

[190] Sam Biddle, "U.S. Spy Agencies are Getting a One-Stop Shop to Buy Your Most Sensitive Personal Data," *The Intercept*, May 22, 2025, https://theintercept.com/2025/05/22/intel-agencies-buying-data-portal-privacy/.

[191] *See* Savage, "Intelligence Analysts," *supra* note 184; Hamed Aleaziz and Caroline Haskins, "DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People," *BuzzFeed News*, October 30, 2020, https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation.

[192] *See* Savage, "Intelligence Analysts," *supra* note 184; Aleaziz and Haskins, "DHS Authorities," *supra* note 191.

warrant based on a theory of user consent, even while acknowledging that terms of service often do not indicate that user data may be sold to the federal government.[193]

The government's attempts to bypass *Carpenter* and to infer consent in the absence of meaningful disclosure to customers are legal sophistry, but it could take years for the courts to resolve these issues. 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.[194] But the law is woefully outdated. It does not cover digital data brokers or many app developers, for the simple reason that they largely did not exist in 1986, when the law was passed. This gap creates an easy end-run around the law's protections.[195] Companies that are prohibited from selling their data to the government can simply sell it to a data broker — a disturbingly common practice[196] — and the data broker can resell the same information to the government, at a handsome profit. The information is effectively laundered through a middleman.

Current agency guidelines are an inadequate replacement for the constitutional and statutory protections that are being sidestepped. For example, ODNI released a framework in May 2024 establishing uniform baseline standards for how intelligence agencies should categorize, acquire, and handle commercially available information ("CAI").[197] Although the framework articulates laudable general principles — e.g., "The protection of privacy and civil liberties, and compliance with procedures governing the conduct of intelligence activities, shall be integral considerations . . . in an IC element's access to and collection and processing of CAI"[198] — its subjective, discretionary, and exception-riddled standards risk making it a box-

---

[193] Joseph Cox, "'FYI. A Warrant Isn't Needed': Secret Service Says You Agreed To Be Tracked With Location Data," *404 Media*, November 12, 2024, https://www.404media.co/fyi-a-warrant-isnt-needed-secret-service-says-you-agreed-to-be-tracked-with-location-data/.

[194] 18 U.S.C. § 2702. The law, however, includes broad exemptions for foreign intelligence surveillance. *See* 18 U.S.C. § 2511(2)(a)(ii), (e), (f).

[195] *See* Ayoub and Goitein, "Closing the Data Broker Loophole," *supra* note 176.

[196] 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*, June 15, 2022, https://arstechnica.com/tech-policy/2022/06/senate-bill-would-ban-data-brokers-from-selling-location-and-health-data/.

[197] Office of the Director of National Intelligence, "ODNI Releases IC Policy Framework for Commercially Available Information," May 8, 2024, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3815-odni-releases-ic-policy-framework-for-commercially-available-information; *see also* James A. Smith, Assistant Director for Policy and Strategy, Office of the Director of National Intelligence, *Intelligence Community Policy 504 (01)*, February 6, 2025, https://www.odni.gov/files/documents/ICPM/ICPM-2024-504-01-IC-Policy-Framework-for-Commerically-Available-Information-Tech-Amendment-Feb2025.pdf [hereinafter Intelligence Community Policy 504].

[198] Intelligence Community Policy 504, *supra* note 197, at 4.

checking exercise for agencies.[199] It also fails to prohibit intelligence agencies from purchasing information that would otherwise be subject to statutory or constitutional requirements to obtain a warrant, court order, or subpoena.[200]

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.

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. In the last Congress, the House passed the bipartisan Fourth Amendment Is Not For Sale Act,[201] a bill that would go a long way toward closing the data broker loophole for certain sensitive types of data.[202] Congress should include that legislation—or similar reforms, such as those contained in the bipartisan Government Surveillance Reform Act[203]—as part of any Section 702 reauthorization.

D. Other Reforms

My testimony before this Committee in July 2023 describes several other concerns stemming from Section 702 and other warrantless surveillance practices, and identifies reforms that would address them. Because there have been relatively few developments in these areas since 2023, they are only briefly summarized here, with footnotes citing the relevant pages of my earlier testimony.

1. Protecting Americans' Privacy Under Section 702

Strengthen the reverse-targeting prohibition.[204] In its current form, the prohibition on reverse targeting applies only if "the purpose" of collection is to target a U.S. person. This language allows the government to target someone under Section 702 even when the *primary*

---

[199] *See* Emile Ayoub, "The Intelligence Community's Policy on Commercially Available Data Falls Short," Brennan Center for Justice, September 12, 2024, https://www.brennancenter.org/our-work/analysis-opinion/intelligence-communitys-policy-commercially-available-data-falls-short.
[200] *See id.*
[201] Fourth Amendment Is Not For Sale Act, H.R. 4639, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/house-bill/4639; Fourth Amendment Is Not For Sale Act, S. 2576, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/2576/text.
[202] *See* Ayoub and Goitein, "Closing the Data Broker Loophole," *supra* note 176; Elizabeth Goitein, "The Government Can't Seize Your Digital Data. Except by Buying It.," Washington Post, April 26, 2021, https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/.
[203] Government Surveillance Reform Act of 2023, S. 3234, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/senate-bill/3234/text; H.R. 6262, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/house-bill/6262.
[204] *See* Goitein, *Fixing FISA, Part II*, *supra* note 127, at 27.

purpose of the collection is to spy on a U.S. person with whom the target is communicating, as long as the government has any interest whatsoever in the foreign target. Congress should close this giant loophole by prohibiting the government from targeting someone if "a significant purpose" is to target a U.S. person.

Specify minimization requirements.[205] 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. Congress should specify that all information not subject to a litigation hold must be destroyed within three years unless it has been reviewed and determined to be foreign intelligence or evidence of a crime.

Narrow the scope of surveillance.[206] Section 702 authorizes surveillance of almost any non-U.S. person outside the United States, regardless of whether that person poses any threat to U.S. security or interests. The sprawling scope of permissible targets creates an enormous pool of Americans' communications that can be "incidentally" caught up in surveillance. It is also causing significant legal and economic problems for U.S. businesses, as European courts have twice blocked the transfer of data between EU and U.S. companies on the ground that U.S. companies cannot protect EU citizens' data against unjustified surveillance.[207] 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 impact on Americans' privacy and on U.S. businesses. It can do so by requiring the targets to be foreign powers or agents of a foreign power; by amending the definition of "foreign intelligence" information to remove overbroad catch-all language; by codifying certain limitations included in an executive order issued by President Biden; or through some combination of all three approaches.

---

[205] *Id.*

[206] *Id.* at 11–12, 28–29.

[207] *See* Case C-311/18, Data Protection Commissioner v. Schrems, ECLI:EU:C:2020:559 (July 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 (October 6, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en. President Biden issued an executive order to pave the way for a new data-transfer agreement, which took effect in July 2023. *See* Data Privacy Framework Program, "Data Privacy Framework (DPF) Program Overview," accessed November 18, 2025, https://www.dataprivacyframework.gov/Program-Overview. The General Court of the EU recently upheld the new agreement, *see* Case T-553/23, Latombe v. Commission, ECLI:EU:T:2025:831, (September 3, 2025), *available at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=303827&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=15593637, but its decision has been appealed to the CJEU, *see* Case C-703/25 P, Latombe v. Commission, *available at* https://curia.europa.eu/juris/liste.jsf?num=C-703/25&language=en, and observers doubt that the agreement includes sufficient constraints on surveillance to satisfy the higher court. *See* Iain Nash, "The European Commission's Rejection of Latombe," *Lawfare*, November 3, 2025, https://www.lawfaremedia.org/article/the-european-commission-s-rejection-of-latombe; Rachael Annear et al., "EU-US Data Privacy Framework Survives Its First Judicial Challenge – But More Are Expected," September 11, 2025, https://technologyquotient.freshfields.com/post/102l4m1/eu-us-data-privacy-framework-survives-its-first-judicial-challenge-but-more-are; "EU-US Data Transfers: First Reaction on 'Latombe' Case," *Noyb*, September 3, 2025, https://noyb.eu/en/eu-us-data-transfers-first-reaction-latombe-case.

2. Bolstering Judicial Review

Congress provided two mechanisms by which courts other than the FISA Court may review electronic surveillance conducted under FISA. First, 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. Second, Congress expressly provided for civil lawsuits to challenge unlawful surveillance under FISA. Neither mechanism is working as Congress intended, and reforms are needed to shore them up.

End the practice of parallel construction.[208] The government has a statutory and constitutional obligation to notify criminal defendants when it uses evidence "obtained or derived from" Section 702 surveillance. But there is reason to believe that the government is avoiding its notification requirements by engaging in "parallel construction" — i.e., recreating the Section 702 evidence using less controversial means. 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.

Clarify application of standing and state secrets doctrines.[209] Congress expressly authorized civil suits against the government for FISA violations, and it included a provision carefully directing courts how to handle sensitive information in such cases. Yet civil lawsuits have consistently been derailed — either by stingy judicial interpretations of standing, or by courts allowing the government to evade FISA's rules for handling sensitive information through assertions of the "state secrets" privilege. Congress should remove these artificial barriers to civil litigation by (1) specifying that a person has standing to bring a civil lawsuit if they have a reasonable basis to believe their information has been (or will be) acquired, and if they have expended (or will expend) time or resources in an attempt to avoid acquisition; and (2) by clarifying that the statutory procedures for handling sensitive information in FISA cases govern how courts should resolve any claims of the state secrets privilege.

3. Closing Gaps in the Law to Prevent Warrantless Surveillance of Americans

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. 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 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

[208] *See* Goitein, *Fixing FISA, Part II*, supra note 127, at 31–32.
[209] *Id.* at 32–33.

surveillance of Americans and surveillance overseas generally meant surveillance of foreigners. By contrast, communications today 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.

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. In particular, purely domestic communications may be obtained under EO 12333 when the government conducts bulk surveillance. Moreover, even when EO 12333 surveillance is targeted at specific foreigners, it results in the "incidental" collection of Americans' communications, just as Section 702 does. Yet protections for Americans' data obtained under EO 12333 are left entirely to executive branch policies, with no judicial review to ensure that these policies comport with the Constitution — or that agencies' practices comport with the policies.

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. 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. Among other measures, Congress should prohibit the targeting of Americans under EO 12333; require the government to minimize the retention, sharing, and use of Americans' information that is "incidentally" acquired under EO 12333; 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; and require the government to inform criminal defendants when using evidence obtained or derived from EO 12333 surveillance.

Update the law to reflect the Supreme Court's decision in Carpenter v. United States.[210] For decades, the "third party doctrine" held that that people have no reasonable expectation of privacy — and therefore no Fourth Amendment protection — in any information that they voluntarily disclose to third parties. Whatever merit this doctrine might have had in the 1970s, when it was established, today it is virtually impossible to go 24 hours without disclosing highly

[210] *Id.* at 40–42.

sensitive information to the multitude of third parties (cell phone companies, internet service providers, mobile applications, etc.) that manage life in the digital world.[211]

In 2018, the Supreme Court began the long process of bringing the third-party doctrine in line with the realities of our modern era. In *Carpenter v. United States*,[212] the Court held that police officers need a warrant to compel cell phone companies to turn over historical cell-site information for a seven-day period, even though customers "share" such information with the companies. The Court reasoned that comprehensive geolocation information can reveal the most intimate details of a person's associations and activities — what the Court referred to as "the privacies of life."[213] In addition, 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. But 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. Congress should take 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. At a minimum, in addition to communications content and geolocation data, those categories should include communications metadata; internet search and web browsing records; biometric information; and health information.

Conclusion

Notwithstanding the government's terminology, Section 702's impact on Americans is anything but "incidental." Intelligence agencies have leveraged this authority on a systemic basis to gain warrantless access to Americans' communications and other personal information in ways that circumvent FISA, the Constitution, and orders of the FISA Court. At the same time, 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 next year, Congress has the opportunity — and the responsibility — to better align the law with Americans' constitutional rights and legitimate privacy expectations.

---

[211] *See generally Digital Dragnets: Examining the Government's Access to Your Personal Data, Hearing Before the H. Comm. on the Judiciary*, 117th Cong. 17–22, July 19, 2022 (testimony of Elizabeth Goitein, Senior Director, Liberty and National Security Program, Brennan Center for Justice), https://docs.house.gov/meetings/JU/JU00/20220719/115009/HHRG-117-JU00-Wstate-GoiteinE-20220719.pdf.

[212] Carpenter v. United States, 585 U.S. 296 (2018).

[213] *Id.* at 311 (quoting Riley v. California, 573 U.S. 373, 403 (2014) (internal quotation marks omitted)).