

Section 702 of FISA: A “Foreign Intelligence” Law Turned Domestic Spying Tool

In 2008, Congress passed Section 702 of FISA to give the government greater powers to conduct warrantless surveillance of suspected foreign terrorists. The law allows the National Security Agency (NSA), when collecting information inside the United States or from U.S. companies, to target almost any foreigner abroad and acquire all their communications without an individualized court order. Congress explicitly prohibited the targeting of Americans, and it charged the FISA Court with approving the program and its procedures once a year.

Although purportedly targeted at foreigners, **Section 702 has become a rich source of warrantless government access to Americans’ phone calls, texts, and emails.** Since Section 702 was last reauthorized, a series of disclosures has revealed the extent of this problem. **In 2022 alone, the FBI conducted over 200,000 warrantless searches of Section 702 communications to find Americans’ information.**¹ This has turned Section 702 into something Congress never intended: a domestic spying tool.

Other equally serious problems have emerged. The secret and one-sided nature of FISA Court proceedings has undermined the court’s ability to conduct effective oversight, while Congress’s efforts to enable other means of judicial review have been thwarted. Gaps in the law are allowing the collection of Americans’ communications and other personal information outside of FISA, without *any* statutory limits or judicial oversight. And Section 702’s failure to establish any meaningful limits on the scope of surveillance is threatening U.S. companies’ ability to do business in Europe.

It’s high time for Congress to step in and enact reforms that will safeguard Americans’ rights and business interests. The well-documented problems with the law’s operation are described in more detail below, along with the solutions. **Congress should not reauthorize Section 702 without these critical reforms.**

Section 702: Problems and Solutions

1. Problem: Use of Section 702 to Spy on Americans. Surveillance under Section 702 inevitably sweeps in Americans’ communications, which ordinarily would require a warrant to obtain. Congress therefore required agencies to “minimize” the sharing, use, and retention of such “incidentally” collected information about Americans. Congress also required the government to certify to the FISA Court that it is not engaging in “reverse targeting” — i.e., using Section 702 to spy on Americans. **Over the past decade and a half, it has become clear that these critical protections for Americans’ constitutional rights have failed.**

Rather than “minimize” the sharing and retention of Americans’ data, the NSA routinely shares such data with the FBI, CIA, and National Counterterrorism Center, and all agencies retain it for at least five

¹ Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2022*, April 2023. https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf. In addition to the 204,090 query number, this report also includes a “de-duplicated query figure” of 119,383, which represents the number of unique identifiers used in the queries. The lower number, however, would exclude instances of the same U.S. person being subject to multiple queries— such as if a U.S. person’s communications are queried by different FBI personnel for independent reasons, or on multiple occasions over the course of an investigation to find any new communications—even though each query would represent a distinct privacy intrusion.

years. Worse, **all agencies have adopted rules allowing them to search through the data for Americans’ communications – even though the data is acquired without a warrant based on the government’s certification that it is targeting *only* foreigners overseas.** This practice is a bait and switch that guts Americans’ Fourth Amendment protections, and it occurred over 200,000 times last year.²

Congress and the FISA Court have tried to rein in backdoor searches by imposing certain limitations — but the FBI has consistently violated them. When Congress last reauthorized Section 702 in 2018, it added a provision requiring the FBI to obtain a warrant before accessing Americans’ communications in a very small subset of criminal investigations. This requirement has been triggered at least 100 times.³ But by the government’s own admission, **the FBI has never once adhered to the statutory warrant requirement.**⁴

For investigations that don’t fall within the statutory warrant requirement, the FISA Court allows backdoor searches *if* they are likely to yield foreign intelligence or evidence of a crime. But according to several recent FISA Court opinions and government reports, **the FBI has engaged in “widespread violations” of this minimal court-ordered privacy protection.**⁵ To name just a few examples, **FBI agents searched for the communications of:**⁶

- More than 100 Black Lives Matter protesters
- a batch of 19,000 political donors who gave money to a congressional campaign
- a U.S. congressman
- a “local political party”
- “multiple current and former United States Government officials, journalists, and political commentators”
- two “Middle Eastern” men, flagged by a witness because they were loading boxes of cleaning supplies into a vehicle
- people who came to the FBI to perform repairs
- victims who approached the FBI to report crimes
- business, religious, and community leaders who applied to participate in the FBI’s “Citizens Academy”
- college students participating in a “Collegiate Academy”
- police officer candidates
- colleagues and relatives of the FBI agent performing the search

² Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2022*, April 2023. https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf.

³ Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2022*, April 2023. https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf.

⁴ Office of the Director of National Intelligence, *Statistical Transparency Report Regarding use of National Security Authorities Annual Statistics for Calendar Year 2021*, April 2022. https://www.dni.gov/files/CLPT/documents/2022_ASTR_for_CY2020_FINAL.pdf.

⁵ Memorandum Opinion and Order (FISA Ct. Dec. 6, 2019), available at <https://perma.cc/94E9-A6BE>.

⁶ Memorandum Opinion and Order (FISA Ct. Apr. 21, 2022), available at <https://perma.cc/26EN-YUHS>; Office of the Director of National Intelligence, 22nd Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (August 2021), <https://perma.cc/JB3J-NXWP>; Office of the Director of National Intelligence, 24th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (December 2021), <https://perma.cc/E76T-RKBG>; Memorandum Opinion and Order (FISA Ct. Nov. 18, 2020) available at <https://perma.cc/8U2N-5GYF>; Memorandum Opinion and Order (FISA Ct. Dec. 6, 2019), available at <https://perma.cc/94E9-A6BE>.

These represent just a small portion of the FBI's misuse of Section 702. Based on the 4 percent noncompliance rate reported in its most recent audit,⁷ which reflects compliance rates *after* the FBI implemented new training and oversight requirements and made changes to its data systems, **the FBI conducted over 8,000 U.S. person queries that violated rules in 2022 alone, an average of over 20 improper queries every day.**

Solution: Require a Warrant to Search for Americans' Communications. Lawmakers must put a stop to the government using Section 702 as an end-run around Americans' constitutional rights. **Congress should require agencies to obtain a warrant (in criminal investigations) or a FISA Title I order (in foreign intelligence investigations) before searching Section 702-acquired information for Americans' communications.** The House has twice passed legislation that would impose a warrant requirement for U.S. person queries.

2. Problem: Barriers to judicial review. The mechanisms Congress established for judicial review of surveillance are not working as intended. The FISA Court provides limited, general oversight of Section 702 surveillance, but it operates in secret and often hears only from the government.

Although Congress authorized the FISA Court to appoint amici to provide advice, amici don't have full access to the information they need, and they are left out of many important cases. In addition, FISA requires the government to give notice to criminal defendants when using evidence derived or obtained from Section 702, but the government has evaded this requirement through "parallel construction" (recreating the evidence using less controversial means). And a recent Supreme Court decision gutted a provision of FISA designed to enable judicial review of surveillance in civil cases.⁸

Solution: Bolster judicial review provisions. Congress should strengthen FISA's amici provisions by giving amici better access to relevant information and by encouraging appointment of amici in cases involving sensitive targets such as religious or political organizations, candidates for public office, and the media. **An amendment that would have implemented these measures, offered by Senators Leahy and Lee, passed the Senate by a vote of 77-19 in 2020.**⁹ Congress also should prohibit the government's use of "parallel construction"¹⁰ to avoid notice obligations. And it should correct the Supreme Court's misreading of FISA by clarifying that federal courts may review surveillance materials in civil cases.

3. Problem: Gaps in FISA that allow surveillance of Americans outside of any statutory framework and without judicial oversight. Many of FISA's key definitions and distinctions are rooted in obsolete communications technologies. As technology has evolved, these anachronistic provisions have opened up gaps in the law's coverage, **allowing the government to collect vast amounts of Americans' communications and other personal data with no statutory limits, no effective congressional oversight, and no judicial oversight.** In particular, the government conducts sweeping surveillance overseas, and collects geolocation data and other sensitive information *inside the United States* (often purchasing it from data brokers), subject only to Executive Order (EO) 12333 and related agency

⁷ Federal Bureau of Investigations Office of Internal Auditing, "FISA Query Audit," May 10, 2023. <https://int.nyt.com/data/documenttools/fisa-query-audit-5-10/d9d8e20bafef27c8/full.pdf>.

⁸ See, *Clapper v. Amnesty International USA*; see also, *Jewel v. National Security Agency*.

⁹ Roll Call Vote 116th Congress - 2nd Session, Lee Amdt. No. 1584, May 13, 2020. <https://perma.cc/96XQ-D8BF>.

¹⁰ Human Rights Watch, *Dark Side Secret Origins of Evidence in US Criminal Cases*, January 9, 2018. <https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases>.

policies — which include even fewer protections for Americans’ rights than Section 702. We learned in 2022 that **the CIA has been exploiting these gaps in FISA’s reach for years to conduct a bulk collection program that pulls in Americans’ data.**¹¹

Solution: Establish legislative safeguards and judicial oversight for EO 12333 surveillance affecting Americans. Any surveillance that results in the collection of Americans’ communications and other sensitive data should take place pursuant to statute and with oversight by Congress and the courts. Accordingly, **Congress should legislate basic protections for any EO 12333 surveillance that impacts Americans.** These protections should include limits on bulk collection, which poses unique threats to Americans’ privacy; a warrant requirement for backdoor searches of EO 12333 data; and oversight by Congress and the FISA Court.

4. Problem: Economic and privacy impact of overbroad surveillance. Although the purpose of Section 702 is to prevent terrorism and head off other foreign threats, the law allows surveillance of an extremely broad class of foreigners abroad, including law-abiding private citizens. This jeopardizes the privacy of foreigners who pose no threat to the United States as well as the Americans with whom they communicate. For this reason — combined with the lack of sufficient mechanisms for redress when unlawful surveillance occurs — European courts, seeking to protect individuals’ privacy from overbroad surveillance, have struck down legal agreements that facilitate data transfers from EU companies to U.S. companies. **The overbroad scope of Section 702 thus undermines the ability of 5,000+ U.S. companies to do business overseas, and recently led to a \$1.3 billion EU fine for an American company based on risks of its data being subject to overbroad surveillance.**¹²

Solution: Codify reasonable limits on the scope of surveillance and remove barriers to judicial review. Congress should enact limits that will prevent the targeting of ordinary private citizens who are unlikely to be communicating information about foreign threats. Congress also should remove barriers to judicial review and establish limits on bulk collection, as described above. These measures would both protect Americans’ privacy and address the threat that Section 702 surveillance poses to U.S. businesses.

American Civil Liberties Union
Americans for Prosperity
Brennan Center for Justice
Center for Democracy & Technology
Defending Rights & Dissent
Demand Progress
Due Process Institute
Electronic Frontier Foundation
Electronic Privacy Information Center
Fight for the Future
Free Press Action
Freedom of the Press Foundation

Libertas Institute
National Association of Criminal Defense
Lawyers
Project for Privacy and Surveillance
Accountability
Project On Government Oversight
Restore The Fourth
Surveillance Technology Oversight
Project
TechFreedom
Wikimedia
X-Lab

¹¹ Charlie Savage, *New York Times*, “C.I.A. Is Collecting in Bulk Certain Data Affecting Americans, Senators Warn,” February 10, 2022. <https://www.nytimes.com/2022/02/10/us/politics/cia-data-privacy.html>

¹² Adam Satariano, *New York Times*, “Meta Fined \$1.3 Billion for Violating E.U. Data Privacy Rules,” May 22, 2023. <https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html>.