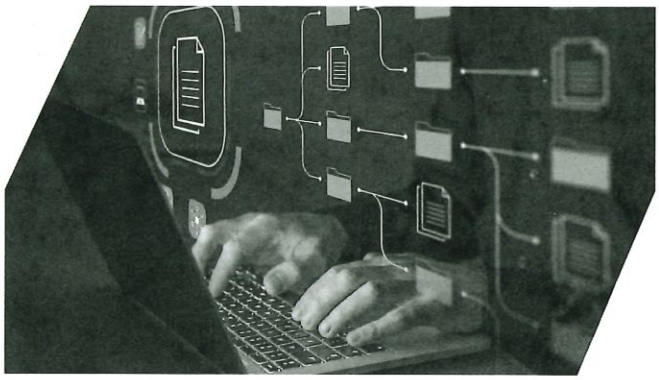
epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

EPIC, Coalition: New FBI Procedures under FISA Section 702 "Out of Touch" with Extent of Abuse and Gravity of Privacy Threat

June 13, 2023



EPIC joined a bipartisan coalition of civil liberties organizations in rejecting the FBI's newest attempt to preempt Congressional efforts to rein in the Bureau's warrantless querying of U.S. person information under FISA Section 702. Ahead of this morning's Senate Judiciary hearing on Section 702, the FBI announced internal procedural changes that are intended to increase accountability for violations of internal rules governing U.S. person queries. The changes include a "three strikes" policy for FBI agents who violate rules and provisions to incorporate FISA compliance into performance evaluations of leaders of FBI field offices. EPIC and its coalition partners emphasized that this response—coming after years of flagrant and persistent abuses—is "completely out of touch with both the level of abuse perpetrated by intelligence agencies and other serious threats to our privacy, like government agents tracking us through data brokers."

Ahead of the Senate Judiciary's hearing, EPIC submitted a letter to the committee, highlighting—among other things—the need to address the government's purchase of data as part of any reauthorization. EPIC emphasized that it is "vital that this conversation be informed by an understanding of the full scope of the government's collection and use of Americans' personal information." EPIC also joined a bipartisan coalition of civil liberties organizations to urge that Congress not reauthorize Section 702 without substantial reforms to the government surveillance ecosystem.

EPIC recently published several posts as part of a blog series focused on explaining Section 702 and the need to reform it. EPIC and its coalition partners have previously called for broad reform to Section 702 and related surveillance authorities.

epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

June 12, 2023

The Honorable Dick Durbin, Chair
The Honorable Lindsey Graham, Ranking Member
Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510

RE: Hearing on Section 702 of the Foreign Intelligence Surveillance Act and Related Surveillance Authorities

Dear Chairman Durbin and Ranking Member Graham:

We write to you regarding the hearing on "Section 702 of the Foreign Intelligence Surveillance Act" that will be held June 13, 2023.

EPIC has testified before Congress during previous FISA Section 702 reauthorization hearings. In 2012, we urged the House Committee on the Judiciary to adopt stronger public reporting requirements. We noted, prior to the disclosures of Edward Snowden, that the scope of surveillance by the Intelligence Community was likely far greater than was known to the public or even to the Congressional oversight committees.[1] In 2017, we wrote to the House Committee on the Judiciary, calling on Congress to establish new means of oversight measures and accountability as a counterbalance to the government's expansive surveillance powers.[2]

We write now to urge this Committee to address the ecosystem of warrantless surveillance authorities affecting Americans as part of any reauthorization of Section 702. To reauthorize the expansive provisions of Title VII of the FAA without these reforms would be a mistake.

The Need for a Warrant Requirement for U.S. Person Queries

Since its controversial inception, Section 702 has created a gap in the traditional FISA framework that allows the government to collect Americans' information without adequate judicial process, and this gap has grown more alarming as the government has increasingly leveraged the information collected on Americans.

---

[1] *See* Testimony of EPIC President Marc Rotenberg, *The FISA Amendments Act of 2008*, Hearing before the House Committee on the Judiciary, U.S. House of Representatives, May 31, 2012, https://epic.org/privacy/testimony/EPIC-FISA-Amd-Act-Testimony-HJC.pdf.

[2] *See* Letter from EPIC to U.S. House Committee on the Judiciary, *Hearing on Section 702 of the Foreign Intelligence Surveillance Act* (Mar. 1, 2017), https://archive.epic.org/testimony/congress/EPIC-HJC-Section702-Mar2017.pdf.

One of the most controversial aspects of Section 702 is the Federal Bureau of Investigation's (FBI) warrantless searching of communications acquired using Section 702 to pursue routine criminal investigation of U.S. persons—often referred to as "backdoor searches."[3] The National Security Agency (NSA), Central Intelligence Agency (CIA), National Counterterrorism Center (NCTC), and FBI may all "query" Section 702 databases, meaning searching the data using a specific term or terms to retrieve relevant contents or metadata. However, the frequency with which the FBI searches Section 702 databases dwarfs that of any other agency.[4] Further, the FBI's domestic law enforcement role raises concerns of foreign intelligence surveillance weaponization against Americans.

Since the last reauthorization of Section 702 in 2018, these concerns have been further substantiated with concrete examples of FBI misuse. According to recently declassified FISC opinions and government audits, **FBI agents have improperly searched Section 702 databases for racial justice activists,[5] donors to political campaigns,[6] sitting members of Congress,[7] local political parties,[8] as well as community and religious leaders.[9]**

It is clear the current structure of the Section 702 authority does not provide the protections necessary to prevent abuses and that warrantless backdoor searches are a run around the Fourth Amendment of the Constitution. Congress must eliminate the warrantless backdoor search and require a warrant for any search of Americans' information, whether by the FBI or any other agency—regardless of the claimed authority for the search.

Addressing the Ecosystem of Warrantless Surveillance of Americans

For all of Section 702's privacy issues, the reality is that surveillance programs conducted pursuant to Section 702 are only one part of a much broader, unchecked expansion of the national security surveillance apparatus. Government agencies—including elements of the Intelligence Community (IC)—have engaged in bulk collection under other authorities and have

---

[3] *See* Jeramie Scott, *Reforming 702: End Warrantless Backdoor Searches*, EPIC (Feb. 23, 2023), https://epic.org/reforming-702-end-warrantless-backdoor-searches/; Elizabeth Goitein, *The Year of Section 702 Reform, Part I: Backdoor Searches*, Just Sec. (Feb. 13, 2023), https://www.justsecurity.org/85068/the-year-of-section-702-reform-part-i-backdoor-searches/.

[4] *See* ODNI, Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2022 19-24 (Apr. 2023), https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf (reporting over 200,000 FBI U.S. person queries, compared to several thousand by the CIA, NSA, and NCTC combined).

[5] *See* In re *[REDACTED]*, Mem. Opinion & Order, No. [REDACTED] 27 (FISA Ct. Apr. 21, 2022), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf

[6] *Id.* at 29.

[7] ODNI & DOJ, Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 58 n. 92 (December 2021), https://www.intel.gov/assets/documents/702%20Documents/declassified/24th-Joint-Assessment-of-FISA-702-Compliance.pdf.

[8] *Id.* at 58.

[9] *See* In re *[REDACTED]*, Mem. Opinion & Order, No. [REDACTED] 39-40 (FISA Ct. Nov. 18, 2020), *available at* https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf.

purchased Americans' sensitive data to circumvent constitutional protections (to say nothing of the increasingly pervasive deployment—often without a warrant—of novel and intrusive surveillance tools like cell site simulators[10], spyware[11], and facial recognition[12]).

In addition to Section 702, the intelligence community relies heavily on Executive Order 12333 (EO 12333) to conduct foreign intelligence surveillance. The Privacy and Civil Liberties Oversight Board (PCLOB) has reviewed several intelligence activities pursuant to EO 12333 and has found that while agencies collect significant amounts of Americans' information, there are significant shortcomings in agency procedures governing how this information is collected, segregated, deleted, disseminated, or even used against Americans.[13]

Given the overlap between these surveillance activities, EPIC urges Congress to reform EO 12333 surveillance along with Section 702. Nearly a decade ago, the President's Review Group on Intelligence and Communications Technologies recommended that the government undertake parallel reforms of both Section 702 and EO 12333 surveillance.[14] The report recommended—in both the Section 702 and EO 12333 contexts—purging requirements, a prohibition on the use of evidence derived from this surveillance in criminal proceedings, and a prohibition on searching information in these surveillance databases without a warrant unless necessary to prevent death or bodily harm.[15] While the government incorporated some of these recommendations in the context of Section 702, it rejected the parallel EO 12333 recommendations, leaving Americans targeted through claimed executive authority even worse off than those subject to Section 702 surveillance.[16] And without accompanying EO 12333 reform, the reform (or sunset) of Section 702 may have the perverse effect of allowing the government to move its surveillance operations under its claimed executive authority.

In addition to these sweeping surveillance programs, the intelligence community (and law enforcement) has also sought to buy itself out of compliance with Americans' Fourth Amendment rights. Agencies have increasingly turned to the private sector, purchasing Americans' data and circumventing traditional legal processes, and without providing any transparency about the government agency procedures (or lack thereof) for protecting

---

[10] *See* DHS OIG, Secret Service and ICE Did Not Always Adhere to Statute and Policies Governing Use of Cell-Site Simulators (Feb. 23, 2023), https://www.oig.dhs.gov/sites/default/files/assets/2023-03/OIG-23-17-Feb23-Redacted.pdf.

[11] Mark Mazzetti & Ronen Bergman, *A Front Company and a Fake Identity: How the U.S. Came to Use Spyware It Was Trying to Kill.*, N.Y. Times (Apr. 2, 2023), https://www.nytimes.com/2023/04/02/us/politics/nso-contract-us-spy.html.

[12] Drew Harwell, *FBI, Pentagon helped research facial recognition for street cameras, drones*, Wash. Post (Mar. 7, 2023), https://www.washingtonpost.com/technology/2023/03/07/facial-recognition-fbi-dod-research-aclu/.

[13] *See* PCLOB, Report on CIA Financial Data Activities in Support of ISIL-Related Counterterrorism Efforts 62-68 (2017), https://documents.pclob.gov/prod/Documents/OversightReport/f01950e2-75ff-4fb4-9b2e-9e7d6937ae3a/PCLOB%20Report%20on%20CIA%20Activities%20-%20508,%20Mar%2022,%202022%201305.pdf.

[14] *See generally* Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies (Dec. 12, 2013), *available at* https://www.justsecurity.org/wp-content/uploads/2013/12/2013-12-12_rg_final_report.pdf.

[15] *See id.* at 28-30.

[16] *See* Charlie Savage, *Recommendation Not Taken Meant 'Significant Changes' for Executive Order 12333 Intercepts*, N.Y. Times (Aug. 13, 2014), https://www.nytimes.com/interactive/2014/08/14/us/14actiontracker.html.

Americans' privacy.[17] This end-run around the Fourth Amendments' protections has only grown more pervasive—and more severe—as private companies have stockpiled personal data, including sensitive data on Americans. Just to name a few recent examples:

- The Department of Defense (DOD), Defense Intelligence Agency, and FBI have both admitted to purchasing location information;[18]
- The DOD and FBI both bought netflow data, allowing the agencies to track internet traffic;[19]
- The Department of Homeland Security regularly buys commercial data, including location data;[20] and
- The Drug Enforcement Agency reportedly bought customer data from informants within airline, bus, and parcel companies in lieu of seeking a warrant.[21]

On Friday, in response to EPIC's FOIA request,[22] ODNI declassified a report on the IC's purchase of commercially available information (CAI).[23] The report revealed several alarming findings about the IC's purchase of data in bulk, including information about Americans. The report found that **the IC is collecting increasing amounts of CAI—including sensitive information like location data—but does not know how much CAI intelligence agencies are collecting, what types, or even what it is doing with that data**.[24] The report also found that, despite the Supreme Court's 2018 decision in *Carpenter v. United States*,[25] which requires a warrant for persistent location information and potentially other data,[26] **the IC has no formal,**

---

[17] *See* Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim, Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, Ctr. for Dem. & Tech. (Dec. 2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

[18] *See* Dell Cameron, *The FBI Just Admitted It Bought US Location Data*, Wired (Mar. 8, 2023), https://www.wired.com/story/fbi-purchase-location-data-wray-senate/; Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, N.Y. Times (Jan. 22, 201), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html; Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Motherboard (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

[19] Joseph Cox, *Revealed: US Military Bought Mass Monitoring Tool That Includes Internet Browsing, Email Data,* Motherboard (Sept. 21, 2022), https://www.vice.com/en/article/y3pnkw/us-military-bought-mass-monitoring-augury-team-cymru-browsing-email-data; Joseph Cox, *Here is the FBI's Contract to Buy Mass Internet Data*, Motherboard (Mar. 27, 2023), https://www.vice.com/en/article/dy3z9a/fbi-bought-netflow-data-team-cymru-contract.

[20] *See* Dana Khabbaz, EPIC, DHS's Data Reservoir: ICE and CBP's Capture and Circulation of Location Information 9–20 (2022), https://epic.org/wp-content/uploads/2022/08/DHS-Data-ReservoirReport-Aug2022.pdf (detailing how DHS uses location data surveillance tools to enable its operations).

[21] Joseph Cox, *The DEA Bought Customer Data from Rogue Employees Instead of Getting a Warrant*, Motherboard (Mar. 29, 2023), https://www.vice.com/en/article/3akn8v/the-dea-bought-customer-data-airlines-parcel-bus-amtrak-no-warrant.

[22] EPIC, *EPIC Seeks ODNI-Led Report on Government Data Purchases* (Mar. 29, 2022), https://epic.org/epic-seeks-odni-led-report-on-government-data-purchases/.

[23] ODNI Senior Advisory Grp., Panel on Commercially Available Information, Report to the Director of Nat'l Intel. (Jan. 27, 2022), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf [hereinafter ODNI Data Purchases Report].

[24] *See id.* at 2.

[25] 138 S. Ct. 2206 (2018).

[26] *See id.* at 2221.

community-wide position on the issue, and IC elements continue to narrowly construe the decision to allow it to purchase otherwise protected information from data brokers without a warrant.[27]

It is vital that Congress address government data purchases as part of any reauthorization of Section 702.

Transparency and Oversight Needed to Make Informed Reauthorization Decision

EPIC has long urged for greater transparency and oversight of Section 702 to ensure that Congress and the American people can make an informed decision about whether to reauthorize this sweeping surveillance authority. However, fifteen years into the program, the government has continued to withhold key information from the public about the scope and nature of programs authorized under Section 702.

The Intelligence Community has yet to release statistics on the number of Americans whose communications are collected under 702 programs, despite prior commitments to do so.[28] A 2011 FISA Court opinion revealed that the NSA was collecting "more than two hundred fifty million Internet communications each year" under Section 702.[29] Since 2013, the number of targets of section 702 surveillance has increased at least threefold to 246,073 in 2022, suggesting that current collection far exceeds the FISC's 2011 estimate of 250,000,000 communications each year.[30] Given the sheer volume of communications collected by the NSA, the number of Americans' communications swept up in these programs is potentially quite high.[31]

Additionally, Congress and the American public deserve to know how the government interprets Section 702, and whether its interpretations comport with Congress's intent in passing Section 702. The newest FISA Court opinion discusses at length—in heavily-redacted passages—a "new—even expansive—application of [Section 702]."[32] It is incumbent upon Congress to ensure that the government does not rely on secret interpretations of the law that run counter to public understanding of its surveillance programs. This information is vital to ensuring that any decision on reauthorization of Section 702 is an informed decision.

---

[27] *See* ODNI Data Purchases Report, *supra* note 19, at 19.
[28] Dustin Volz, *NSA Backtracks on Sharing Number of Americans Caught in Warrant-less Spying*, Reuters (June 9, 2017), https://www.reuters.com/article/us-usa-intelligence/nsa-backtracks-on-sharing-number-of-americans-caught-in-warrant-less-spying-idUSKBN19031B.
[29] Mem. Op, *[Redacted]*, No. [redacted], at 29 (FISC Oct. 3, 2011), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.
[30] *See supra* note 4.
[31] *See* In re *[REDACTED]*, Mem. Opinion & Order, No. [REDACTED] 61 (FISA Ct. Apr. 21, 2022), *available at* https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf ("Notwithstanding this foreign-directed targeting, the extent to which Section 702 acquisitions involve U.S. persons should be understood to be substantial in the aggregate.").
[32] *Id.* at 93.

Conclusion

The Intelligence Community regularly emphasizes that it needs Section 702 to address a collection gap caused by technological development in the years after FISA's passage. The American people deserve a robust conversation about the privacy gap that has resulted from the evolution of government surveillance technology over the past two decades. It is also vital that this conversation be informed by an understanding of the full scope of the government's collection and use of Americans' personal information.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ Jeramie Scott
Jeramie Scott
EPIC Senior Counsel
Director, Project on
Surveillance Oversight

/s/ Chris Baumohl
Chris Baumohl
EPIC Law Fellow