BRENNAN
CENTER
FOR JUSTICE

FISA Section 702: Close Backdoor Search Loophole by Requiring Warrant/FISA Title I Order for U.S. Person Queries

The Problem

Section 702 authorizes warrantless surveillance and therefore may only be used to target non-U.S. persons outside the United States. But this surveillance inevitably sweeps in enormous volumes of Americans' communications, because Americans communicate with foreigners. If the government's intent were to eavesdrop on these Americans, it would have to get a warrant (in a criminal investigation) or a FISA Title I order (in a foreign intelligence investigation). Accordingly, to prevent the government from using Section 702 as an end-run around the Fourth Amendment, Congress directed the government to "minimize" the retention and use of these "incidentally" collected communications of Americans.

Despite this directive, **the FBI, CIA, and NSA routinely search through Section 702 data for the express purpose of finding and reviewing the content of Americans' phone calls, emails, and text messages. The FBI conducted over 57,000 of these "backdoor searches" in 2023 alone, the last year for which the government might have provided complete data.** An authority to target foreigners has thus become a powerful domestic spying tool.

Both Congress and the FISA Court have attempted to limit this practice. **But the FBI has engaged in what the FISA Court called "persistent and widespread violations" of the rules governing backdoor searches.** Abuses in recent years have included searches for the communications of 141 Black Lives Matter protesters; 19,000 donors to a congressional campaign; members of Congress; multiple U.S. government officials, political commentators, and journalists; and tens of thousands of Americans engaged in "civil unrest."

The Solution

In 2024, bipartisan sponsors offered an amendment that would have required the government to obtain either a warrant or a FISA Title I order to search the content of Americans' communications obtained under Section 702. The proposal included several reasonable exceptions designed to accommodate legitimate security needs. **Under this proposal, no court order would be required (1) if there were exigent circumstances; (2) if the subject of the search provided consent (e.g., where the purpose of the search is to identify potential victims); or (3) for certain cybersecurity-related searches.**

In addition, **no court order would be required to search communications *metadata*.** The government could thus determine, without getting a court order, whether a particular U.S. person is in communication with a foreign target. In many cases, that information, combined with what the government already knows about the person, would be sufficient to show probable cause. This commonsense solution has had broad bipartisan support for years. It has been passed twice in the House and in 2024, it was defeated in the House by a single vote. **Polling shows that 76% of Americans support a warrant requirement for backdoor searches.**

New Reasons to Close the Backdoor Search Loophole

The reasons to close the backdoor search loophole have only intensified since Congress passed the Reforming Intelligence and Securing America Act (RISAA) in April 2024.

- **RISAA has failed to address the problem.** RISAA's leading "reform" was a prohibition on backdoor searches performed solely to find evidence of a crime — i.e., with no foreign intelligence purpose. However, the FBI almost never labels its searches "evidence-of-a-crime only." Of the 57,094 backdoor searches conducted by the FBI in 2023, this reform would have prohibited agents from accessing the results of only four. Most of RISAA's other reforms merely codified internal policy changes that the FBI had already made. But those changes proved to be insufficient. *After* the FBI implemented the majority of these changes, serious abuses continued — including improper backdoor searches for communications of a U.S. Senator, a state senator, and a state court judge.

- **A federal court has ruled that the Fourth Amendment's warrant requirement applies to backdoor searches.** In 2019, a unanimous Second Circuit panel held that backdoor searches are a separate Fourth Amendment event from Section 702 collection and sent the case back to the district court to evaluate the constitutionality of the backdoor searches in the case. In December 2024, the district court ruled that the Fourth Amendment's warrant requirement applies to backdoor searches, meaning such searches must be authorized by a warrant or qualify for an exception to the warrant requirement. The court found that the backdoor searches at issue failed both criteria and thus violated the Fourth Amendment, refuting the argument that the Fourth Amendment places no limits on searches of lawfully obtained data.
- **The expanded definition of "electronic communications service provider" has not been fixed.** RISAA included a provision that was intended to allow the government to compel the cooperation of one particular type of company when conducting 702 surveillance. But the type of company was (and remains) classified, so the provision was deliberately written in broad language to obscure the type of company at issue. The unintended consequence is that the provision gives the NSA access to the communications equipment of *almost every* U.S. business or organization, vastly expanding the universe of Americans' communications that can be "incidentally" collected and creating enormous potential for abuse. The then-chairman of the Senate Intelligence Committee promised to fix the provision in future legislation, but Congress has not voted on that fix, leaving the dangerously overbroad provision in effect.

What Opponents Will Say — and Why They're Wrong

- **"RISAA's reforms significantly reduced the number of U.S. person queries conducted by the FBI and improved compliance, making a warrant requirement unnecessary."** In 2024, the Department of Justice's National Security Division discovered that the FBI was using an "advanced filter function" to query Section 702 data, but was not complying with statutory and court-ordered requirements designed to prevent abuse, such as obtaining attorney approval and documenting the reasons for U.S. person queries. In addition, these queries were not tracked or audited as required by law. **Due to these violations, the total number of U.S. person queries and the overall compliance rate for 2024 remain *unknown*.**
    - Moreover, even if the FBI conducted only a handful of U.S. person queries and complied perfectly with its querying procedures, 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.
- **"A warrant requirement for backdoor searches would harm national security."** An 18-year track record says otherwise. The government has provided multiple examples in which *surveillance of foreign targets* provided key national security information. By contrast, according to the Privacy and Civil Liberties Oversight Board, "little justification [was] provided . . . on the relative value of the close to 5 million [U.S. person queries] conducted by the FBI from 2019 to 2022." The government has been able to cite only a handful of instances in which backdoor searches have been useful. In each case, it appears the government could have obtained a warrant or invoked a proposed exception — a point the Board Chair confirmed.
- **"A warrant requirement for backdoor searches would overwhelm the courts."** While the FBI currently conducts thousands of backdoor searches each year, DOJ has acknowledged that most of these are basically fishing expeditions, conducted at a point when the FBI has little to no information. Under the proposed warrant requirement, the FBI could run queries of communications *metadata* without a court order to determine whether the U.S. person is even in communication with a foreign target. According to the government's own statistics, this would narrow the pool of inquiry by 98%, leaving a very manageable number of cases in which the FBI might seek a warrant to access content.

For questions about Section 702, contact Liza Goitein at goiteine@brennan.law.nyu.edu or Hannah James at jamesh@brennan.law.nyu.edu.