

April 9, 2026

Balancing Security and Liberty in the Reauthorization of Section 702 FISA

Since its passage in 2008, Section 702 of the Foreign Intelligence Surveillance Act (FISA) has allowed the United States government to collect, without a warrant, the communications of foreign targets abroad, even when those communications involve American citizens. Over the nearly two decades since its enactment, the law has become one of the most consequential tools in the American national security arsenal, credited with enabling the government to identify and disrupt some of the most serious foreign threats it faces. Yet despite explicit statutory prohibitions on targeting Americans, the authority has repeatedly been abused, with government agencies conducting unauthorized searches on citizens ranging from protesters to elected officials. Skeptics argue that the documented record of abuse makes reauthorization indefensible, and the long history of American surveillance overreach lends that concern real weight. Few questions in American national security law carry higher stakes: how Congress resolves the debate over reauthorization will determine not only whether the United States retains a critical intelligence capability, but whether Americans can trust their government to wield surveillance powers without turning them against the people those powers are meant to serve. This paper argues that Congress should reauthorize Section 702 because it is operationally indispensable, because the alternatives leave the United States dangerously exposed to foreign threats, and because reauthorization creates an opportunity to enact safeguards that prevent the cycle of surveillance abuse from repeating itself.

The most compelling case for reauthorizing Section 702 is that individual warrant requirements for foreign intelligence collection are not operationally feasible at modern scale, and the authority has since proven essential to protecting American national security. The original Foreign Intelligence Surveillance Act (FISA) was built on a geographic assumption that foreign communications would remain outside the United States, meaning only domestic surveillance required judicial oversight. However, “technological advances — the internet and fiber-optic lines — made foreigners’ messages available on domestic networks, where FISA’s warrant rule applied,” undermining this geographic logic (Savage 2024). This shift created a structural mismatch between the law and modern communications, forcing intelligence agencies to apply warrant requirements even when targeting foreigners abroad. Section 702 was designed to resolve this problem by allowing the government to “obtain from communication providers the calls and messages of large numbers of foreign targets — 246,073 in 2022 alone” without requiring a separate warrant for each case (Savage 2024). At that scale, individualized warrants are operationally unrealistic, particularly given that “getting a FISA court order is bureaucratically cumbersome and would slow down investigations — especially fast-moving cybercases” (Waxman and Klein 2024). Notably, time is a critical constraint in intelligence operations, and delays can prevent investigators from responding to emerging threats. The consequences of this constraint were already evident after September 11, when the Bush administration secretly ordered Stellarwind, a warrantless wiretapping program designed to detect and prevent terrorist activities, which directly “violated” FISA but was later incorporated into law as Congress “legalized a form of that program by carving out an exception” (Savage 2024). That retrospective approval is telling because it shows that even lawmakers concerned about executive overreach still recognized that the underlying limitation of the warrant

framework was real and that abandoning the capability was not a responsible option. Since then, Section 702 has delivered concrete results, supplying "extraordinary insight into foreign dangers, including military threats, theft of American trade secrets, terrorism, hacking and fentanyl trafficking," and in 2022 helping the government locate and kill al-Qaeda leader Ayman al-Zawahri, one of the architects of September 11 (Waxman and Klein 2024). Furthermore, the fact that Section 702 now contributes to "almost 60 percent of the articles in the president's daily intelligence briefing" suggests that eliminating or significantly narrowing the authority would not merely inconvenience American intelligence agencies but would critically degrade their ability to understand and respond to foreign threats (Waxman and Klein 2024). Ultimately, the operational case for reauthorization is not that oversight is unnecessary, but that requiring individual warrants for every foreign target whose communications pass through American infrastructure is not a workable standard in the modern intelligence environment.

Skeptics of reauthorization argue that the operational case for Section 702 cannot be separated from the risks it poses to Americans' Fourth Amendment protections. Although the law prohibits targeting U.S. persons, "when a foreign target communicates with an American, the government incidentally collects that American's messages to and from its target," often without a warrant (Savage 2024). Because global communication is routine, innocent domestic communications and their metadata, which can reveal networks, behavior, and relationships, are regularly swept into intelligence databases, creating a "loophole" that bypasses traditional constitutional standards. This concern is reinforced by documented misuse. In recent years, agents have conducted improper searches involving "protesters across the political spectrum; members of Congress; a congressional chief of staff; a state court judge; multiple U.S. government officials, journalists, and political commentators; and 19,000 donors to a political

campaign,” showing how easily these tools can be used to examine domestic actors (Brennan Center). Historical precedent deepens this concern. The weaponization of surveillance against Martin Luther King Jr., described as akin to “opposition research,” was not the result of a single rogue official but occurred within a broader system in which “the phalanx of informed government officials, from the president on down” were aware and complicit (Eig and Theoharis 2023). This history suggests that surveillance powers can be redirected toward political or dissenting figures, not just national security threats, especially when institutional checks fail. Ultimately, skeptics argue that even if Section 702 is designed for foreign intelligence, its structure, combining incidental collection, expansive data access, and limited safeguards, makes abuses not just possible but predictable.

Although the documented pattern of abuse raises legitimate concerns, it ultimately warrants structural reform rather than elimination of the authority. The law already imposes four explicit limits: it may only be used to target foreign persons located abroad for foreign intelligence purposes, it may not be used to target Americans anywhere in the world, it may not be used to target anyone inside the United States regardless of nationality, and it prohibits reverse targeting of a foreign person when the true intent is to acquire an American's communications. The problem is not that these limits are inadequate on their face but that they have consistently failed in practice, because the current oversight system "relies almost entirely on executive branch self-policing to prevent, detect, and report abuses" (Goitein and James 2024). The backdoor search problem illustrates this failure most clearly. Although Section 702 is intended for foreign intelligence, agencies can later search that data for Americans' communications, effectively accessing domestic information without a warrant. Courts have now confirmed that this practice crosses a constitutional line, holding that “the Fourth Amendment’s warrant

requirement applies to backdoor searches” (Brennan Center 2024). The appropriate response, then, is not to abandon the authority, but to impose a judicial check at the point where Americans’ data is accessed. The SAFE Act does this by distinguishing between searching and reviewing communications: it allows intelligence agencies to query Section 702 data for Americans’ communications without a court order, but if that search returns results, which occurs in less than two percent of cases, agencies must obtain a warrant or FISA Title I order before accessing the content of those communications (Brennan Center 2024). This distinction is critical, as it preserves the government’s ability to quickly identify potential connections through filtering while ensuring that access to the substance of Americans’ communications is subject to constitutional protections. Concerns that such a requirement would harm national security or overwhelm the courts are overstated. The government has provided “little justification” for the value of the millions of backdoor searches conducted in recent years, suggesting that most are not essential to intelligence operations (Brennan Center 2024). Moreover, because the warrant requirement applies only when agents seek to access the content of Americans’ communications, initial queries can still be used to identify potential connections without delay, while access to the substance of those communications (the most sensitive layer of personal information) requires judicial approval. In practice, this change significantly narrows the number of cases that require judicial approval, ensuring that oversight is imposed precisely at the point where privacy interests are most directly implicated. Reauthorizing Section 702 with this reform would therefore address the core civil liberties concern while preserving a critical intelligence capability.

Regardless of these potential changes, the opposition often contends that no set of reforms can justify the continued use of Section 702 because the risks it poses are structural

rather than procedural. In this view, the problem is not simply that the authority has been misused, but that systems built to collect and store large volumes of data will inevitably expand and be repurposed over time. One example of this expansion is in technology used for current US immigration enforcement. Surveillance tools originally justified for identifying noncitizens are now used “not only to identify undocumented immigrants but also to track citizens who have protested,” demonstrating how quickly such capabilities extend beyond their initial scope (Frenkel & Krolik 2026). The integration of facial recognition, social media monitoring, and data aggregation has given the government “unprecedented abilities” to monitor individuals across contexts, blurring the line between foreign intelligence and domestic surveillance (Frenkel & Krolik 2026). Similarly, digital tracking systems in immigration enforcement have evolved into mechanisms of continuous monitoring, making those subject to surveillance effectively “easy pickings” once they are incorporated into the system (Mozur, Satariano & Krolik 2025). These examples reinforce a broader pattern in which surveillance powers, once granted, expand in scope and are used in ways that exceed their original legal and political justifications. From this perspective, Section 702 would be part of a larger surveillance infrastructure that is inherently difficult to constrain. Even with new legal requirements, internal compliance and self-regulation are unlikely to constrain agencies incentivized to expand the use of available data, ultimately suggesting that the risks may be inherent in the existence of the legislation.

The claim that Section 702 is fundamentally unfixable reflects a failure to distinguish between flaws in enforcement and flaws in design. Section 702 is uniquely reformable because its risks are concentrated within a legally bounded framework. The surveillance technologies often cited in comparison, particularly those used in immigration enforcement, operate with few clear or enforceable limits on how data can be collected, integrated, and repurposed, allowing

them to expand into broader forms of domestic monitoring. Section 702, by contrast, is not an open-ended data collection system but instead a statutory authority with explicit restrictions on who may be targeted and for what purpose. The problem is not the absence of these limits but the failure to consistently enforce them, particularly when agencies access Americans' communications after collection. Unlike more diffuse surveillance systems, this creates a clear and identifiable point where meaningful constraints can be applied. In this context, reform focuses on enforcing existing limits rather than attempting to contain an inherently expansive system, meaning the persistence of abuse reflects a failure of constraint, not an inherent flaw in the authority.

In conclusion, Section 702 should be reauthorized because it is operationally indispensable to modern intelligence, central to national security, and uniquely capable of being reformed in a way that meaningfully constrains its risks. The modern intelligence environment makes some form of large-scale foreign surveillance unavoidable, and eliminating this authority would leave the United States significantly less equipped to respond to evolving threats. At the same time, the documented record of misuse demonstrates that existing safeguards are insufficient and cannot be ignored. Reauthorization should therefore be paired not only with stronger limits on how Americans' communications are accessed, but also with broader reforms, including restrictions on the government's ability to purchase sensitive personal data from data brokers, which can otherwise function as a workaround to constitutional protections. As surveillance capabilities continue to expand alongside advances in artificial intelligence, the scale and speed of data analysis will only increase, making clear legal boundaries even more essential. The question is no longer whether the government will have access to powerful surveillance tools, but whether those tools will be governed by enforceable rules that protect the

rights of the people they are meant to serve. Reauthorizing Section 702 with meaningful reform ensures that intelligence capabilities keep pace with technological change while preserving the constitutional principles that define their legitimate use.