

Section 702 – Essential Tool for National Security

Abraham Wagner

Surveillance against potential adversaries and terrorists has long been an essential part of the intelligence mission. As new communications technologies evolved and came into widespread use it was necessary for the Intelligence Community to develop both a responsive collection capability as well as an appropriate legal regime as well.

The 1978 Foreign Intelligence Surveillance Act (FISA) is a key element of this legal regime, establishing procedures for the collection of foreign intelligence on domestic soil and provides judicial and congressional oversight of U.S. surveillance of foreign entities and individuals in the United States, while maintaining the secrecy needed to protect national security.

FISA responded to revelations of widespread privacy violations by the Intelligence Community in the 1970s and requires law enforcement and intelligence agencies to obtain authorization for gathering "foreign intelligence information" between "foreign powers" and "agents of foreign powers" suspected of espionage or terrorism.

The initial Act was passed in an era of different technologies – a decade before the Internet and when cell phones hardly existed. Virtually all communications used 1930s technologies when phones and their numbers actually belonged to people and geography mattered. In today's world cell phones are the norm and in most of the world don't belong to anybody. Phone books no longer exist and data with respect to actual users must be compiled by intelligence or law enforcement agencies. For its part the Internet presents a similar and even more challenging set of problems where users, accounts and servers are across the planet. This is a world where geography no longer matters.

Meeting this evolving challenge FISA has been repeatedly amended since the 9/11 terrorist attacks, with several added provisions garnering political and public controversy due to privacy concerns. It now authorizes the government to conduct targeted surveillance of foreign persons located outside the United States, without a warrant, to acquire foreign intelligence information and enables the government to compel assistance from service providers to access the content of targeted electronic communications.

Such authorization comes from the Foreign Intelligence Surveillance Court (FISC) also established under the Act to grant surveillance warrants. Although FISA was initially limited to government use of electronic surveillance, subsequent amendments have broadened the law to regulate other intelligence-gathering methods and compelling the production of certain types of records to obtain the warrants.

The terrorist 9/11 terrorist attacks on the nation and the subsequent War on Terrorism caused the Intelligence Community to undertake a number of new programs responding to the terrorist threat including the President's Surveillance Program (PSP). This was a collection of secret intelligence activities where the information collected was protected within a security compartment codenamed STELLARWIND, which authorized warrantless wiretapping of international communications where one party to the communication was believed to be affiliated

with the *al-Qaeda* terrorist group as well as data mining of e-mail messages and telephone call detail records in the NSA call database.

Presidential authorization for the program expired in 2007, although some of the collection activities were continued under the FISA Amendments Act (FAA) of 2008. The FAA required all of the intelligence agencies involved in the program to "complete a comprehensive review" of their activities and concluded that the President's program involved "unprecedented collection activities" that went far beyond the scope of the Terrorist Surveillance Program. It also raised questions over the legal underpinnings of the authorizations, a lack of oversight. The report also concluded that the program was built on a "factually flawed" legal analysis.

In response to this report, Congress enacted Section 702 as a FISA provision Surveillance Act (FISA) that allows the collection and use communications of foreign targets located outside the U.S. for national security purposes. Section 702 was reauthorized by Congress for six years in January 2018, with some new privacy safeguards and reforms to address past abuses. The President's Intelligence Advisory Board also supported the reauthorization with a number of additional changes.

Since its enactment Section 702 has been subject to increasing criticism, largely from civil liberties organizations and privacy advocates. As currently enacted, Section 702 permits the Attorney General and the Director of National Intelligence to jointly authorize targeting of non-US persons reasonably believed to be located outside the United States.

By targeting it is meant that U.S. persons or persons located in the United States may not be the intended targets of the collection, but it does not mean the communications of U.S. persons cannot be collected, as they are subject to what is known as "incidental collection" such as when they communicate with non-US persons who are the targets of the collection. Here the targeting must have as its object the acquisition of foreign intelligence information as it is defined by FISA.

Under § 702(b) of the FISA Amendments Act, acquisitions are subject to several limitations an acquisition (1) may not intentionally target any person known at the time of acquisition to be located in the United States; (2) may not intentionally target a person reasonably believed to be located outside the U.S. if the target (a known person) is reasonably believed to be in the U.S.; (3) may not intentionally target a U.S. person reasonably believed to be located outside the U.S.; (4) may not intentionally acquire any communication where the sender and intended recipients are known to be in the U.S.; and, (5) must be conducted in a manner consistent with the Constitution.

Congress must decide by April 19 whether to reauthorize Section 702 of the Foreign Intelligence Surveillance Act, also known as FISA. This controversial law was originally intended to make it easier for the government to monitor foreign terrorists, but the government has repeatedly abused it to illegally spy on Americans, violating individual rights on a wide scale. So far, four bills have been introduced in Congress that would reauthorize Section 702, but only two of them — the Protect Liberty and End Warrantless Surveillance Act (Protect Liberty Act) and the Government Surveillance Reform Act of 2023 — would help prevent future abuses.

Section 702 was enacted after 9/11 to give the government greater powers to monitor foreign terrorists. It authorizes the government to collect the communications of non-Americans located abroad without a warrant from a court. While this surveillance is supposed to target foreigners, it inevitably sweeps in Americans' private phone calls, emails, and text messages too. Once collected, federal agents can search through this information even when they are specifically looking for Americans' communications. Intelligence agencies conduct more than 200,000 of these warrantless "backdoor" searches for Americans' private communications every year.

By itself, that is an outrageous violation of Americans' privacy rights. But the problem is compounded by what one federal judge described as the FBI's "persistent and widespread" abuses of the minimal rules governing backdoor searches. Intelligence officials are only supposed to perform these searches if they reasonably believe they are likely to uncover foreign intelligence, or, in the case of the FBI, evidence of a crime. It's an extremely permissive rule, yet agencies have repeatedly violated it. Declassified documents have revealed that officials have performed baseless backdoor searches for the private communications of racial justice protesters, members of Congress, journalists, crime victims, and political donors, among many others.

These abuses have outraged lawmakers, with many vowing not to reauthorize the law without "significant reforms." But while there is bipartisan consensus in Congress that something must change, surveillance hawks who hold key positions are working hard to preserve the status quo.

What bills have been introduced to reauthorize Section 702? In addition to the Protect Liberty Act and the Government Surveillance Reform Act, the leadership of the House and Senate intelligence committees have introduced Section 702 [reauthorization bills](#) of their own. Though these are two different bills, they are both confusingly named the "FISA Reform and Reauthorization Act of 2023." Each of these four bills reauthorizes Section 702, but there are critical differences among them.

The Government Surveillance Reform Act includes the most comprehensive reforms. Among other changes, it would:

- require the government to obtain a warrant before performing backdoor searches of communications content, with exceptions for exigent circumstances, consent, certain cybersecurity-related queries
- provide similar protections for information acquired without a warrant under Executive Order 12333, which generally governs foreign intelligence surveillance conducted

outside of the United States and, like Section 702, results in the “incidental” collection of vast quantities of Americans’ information

- allow queries of communications metadata, such as to determine whether a particular U.S. person is in contact with a foreign target, without a warrant or court order
- close the data broker loophole that intelligence and law enforcement agencies are exploiting to buy their way around Fourth Amendment and statutory requirements by purchasing Americans’ sensitive information
- improve the workings of the Foreign Intelligence Surveillance Court (also known as the FISA court), the secretive body that reviews the government’s intelligence surveillance applications
- address privacy risks posed by modern surveillance techniques, such as the use of “stingray” cellphone trackers and the collection of data generated by automobiles.

While the bill does not include every reform privacy advocates want, it would be the most significant advancement to Americans’ privacy rights since FISA was enacted in 1978.

The Protect Liberty Act is a compromise bill that includes important surveillance reforms but omits some of the more far-reaching changes included in the Government Surveillance Reform Act. It requires a warrant for backdoor searches of communications content, with the same exceptions contained in the Government Surveillance Reform Act, closes the data broker loophole, and shores up oversight by the FISA court.

It does not, however, regulate surveillance performed under EO 12333, the use of stingrays, or the collection of car data. The bill’s composition reflects a careful balancing between protecting Americans’ privacy and the accommodations necessary to ensure ultimate passage. Indeed, each of the Protect Liberty Act’s three key reforms has already garnered majority support in at least one chamber of Congress.

The intelligence committee bills are a different matter altogether. Both claim to make meaningful improvements to Section 702, but the only real “reform” they contain is in their titles. Their marquee change is a prohibition on backdoor searches conducted solely for the purpose of uncovering evidence of a crime. Such queries constitute a vanishingly small proportion of the government’s total backdoor searches; in 2022, out of more than 200,000 searches, this ban would have prevented the government from accessing the contents of Americans’ communications in just two instances.

Had this prohibition been in place over the last few years, it would have done nothing to prevent the worst abuses of Section 702 — including the baseless searches for racial justice protesters, political donors, and members of Congress — as all of these searches were ostensibly intended to uncover foreign intelligence.

The bills’ other provisions relating to backdoor searches largely just codify policies and procedures that are already in place, including recent changes to the FBI’s internal rules. But we already know that these changes are insufficient. Since the changes were made, the government has continued to report violations of the FBI’s querying standard at a rate amounting

to several *thousand* violations per year. These recent violations, like the previous ones, include flagrant abuses — such as searches 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.

The intelligence committees' bills not only fail to address Section 702 abuses, they would actually expand warrantless surveillance. Both bills require intelligence agencies to develop procedures for querying all non-Americans traveling to the United States, subjecting business people, students, and tourists to invasive searches even when the multiple vetting mechanisms already in place have uncovered no reason for concern. Moreover, the House bill includes a provision that fundamentally rewrites Section 702's definition of "electronic communication service provider."

This change would dramatically expand the universe of people and entities that can be required to assist the government in conducting surveillance. For instance, any U.S. business that provides WiFi to their customers — including hotels, coffee shops, or even libraries — could be forced to give the National Security Agency access to their routers. According to the American Civil Liberties Union, it "would be the largest expansion of domestic government surveillance since the Patriot Act."

Wasn't Section 702 set to expire last year? Section 702 was originally set to expire on December 31, 2023. In the weeks leading up to this deadline, House Speaker Mike Johnson elected to bring both the Protect Liberty Act and the House Intelligence Committee bill to the floor at the same time using an infrequently invoked procedure known as Queen of the Hill. Under this procedure, if both votes were to garner support from a majority of the members, the bill that got the most "yea" votes would be advanced to the Senate. But the Rules Committee refused to agree to this arrangement, and after a contentious [session](#) in which pro-reform lawmakers faced off against surveillance hawks, Johnson pulled both proposals from the floor.

Instead, congressional leadership — Johnson, Senate Majority Leader Chuck Schumer, Senate Minority Leader Mitch McConnell, and House Minority Leader Hakeem Jeffries — inserted an extension of Section 702 into the "must-pass" National Defense Authorization Act. The act, which passed Congress and was signed into law by President Biden late last year, included a provision extending Section 702 until April 19. However, the extension language did not include a key provision to prevent the Biden administration from unilaterally continuing surveillance into 2025.

Under Section 702, surveillance takes place pursuant to annual "certifications" approved by the FISA court. The law that established Section 702 includes a **provision** stating that any certifications in place at the time the law sunsets remain in effect until they expire. The extension of Section 702 in the defense authorization act did not include a prohibition on the government obtaining new certifications, meaning the intelligence agencies could go to the FISA court in early April and get a new certification — one that would allow the surveillance to continue until April 2025 even if Congress chose not to reauthorize the law.

Nonetheless, in pushing for an extension of Section 702 last December — even though the existing certification permits surveillance until April 11, 2024 — the administration argued

vehemently that it could lose valuable intelligence if the law expired, as companies might balk at turning over data with no statutory authorization in place. In addition, administration officials reportedly assured members that the government would not seek to continue surveillance under a new certification if Congress does not reauthorize Section 702 by April 19. For these reasons, April 19 should be treated as a hard deadline for Section 702 reauthorization and reform.

Congress has not been actively focused on Section 702 since reconvening after the holidays. Nevertheless, Schumer and McConnell have committed to negotiating a bipartisan bill that could be enacted “early” this year. Johnson has similarly indicated that he wants to achieve a “consensus” bill, something Rep. Darin LaHood (R-IL), a member of the House Intelligence Committee, says could happen by February.

It is clear that there is no bill that could satisfy both those who support substantial reform of Section 702 and those who oppose any meaningful reform. A negotiation designed to achieve a “consensus” bill is thus doomed to fail. Instead, Johnson should bring the Protect Liberty Act to the floor and allow members to offer amendments. The Protect Liberty Act is already a compromise bill, representing a middle ground between the Government Surveillance Reform Act (or, as some have advocated, letting Section 702 expire altogether) and the intelligence committees’ bills.

Moreover, it was approved by the House Judiciary Committee, which has primary jurisdiction over Section 702 and FISA in general. An amendment process would then give intelligence committee leaders a fair opportunity to make their case for allowing the government to have warrantless access to Americans’ emails and text messages.

One thing that should not be on the table is allowing Section 702 to continue in its current form after April, whether by enacting another temporary extension or by allowing the administration to obtain a new certification and continue surveillance under that certification after the April 19 deadline. As some Hill-watchers have noted, it might be tempting for congressional leaders to punt this contentious issue until after the 2024 election, leaving it to be taken up in the lame-duck session next winter or in 2025.

But that would be a dereliction of duty and a betrayal of Americans’ trust. Failing to act on Section 702 would allow the persistent abuses of Americans’ rights to continue unchecked. Congressional leaders must fulfill their responsibility to end these abuses by bringing reform legislation to the floor quickly and urging its rapid passage.