FOREIGN AFFAIRS

JUNE 6, 2023

The Coming Fight Over American Surveillance

What's at Stake as Congress Considers FISA Reform

ELIZABETH GOITEIN

The Coming Fight Over American Surveillance

What's at Stake as Congress Considers FISA Reform

ELIZABETH GOITEIN

Americans are living in an era of unprecedented government surveillance, made possible by seismic changes in both technology and the law. Never have people generated such volumes of personal information—and never has the U.S. government possessed such powerful means to capture, store, and analyze it. At the same time, the 9/11 attacks prompted Congress to relax many of the legal constraints on surveillance.

For the better part of two decades, Americans acquiesced in these developments. In 2013, Edward Snowden, a National Security Agency contractor, disclosed that the NSA was secretly collecting Americans' phone records in bulk—a revelation that briefly rattled the public's trust and led to some legislative reforms in 2015. But Americans were soon occupied with matters that seemed more pressing than the abstract risk of surveillance abuse.

As with so many other things, that blithe status quo was dramatically upended by the presidency of Donald Trump. Many Republicans became

convinced that the FBI had abused the Foreign Intelligence Surveillance Act (FISA) to spy on Trump's campaign. Democrats, for their part, gained a new appreciation for the dangers of insufficiently constrained executive power. Their concerns were reinforced when it emerged that intelligence and law enforcement agencies had been spying on activists taking part in a newly reinvigorated racial justice movement.

The country is now headed for a reckoning over government surveillance, and the first testing ground will likely be a part of FISA known as Section 702. This authority, which permits the government to conduct warrantless surveillance of foreigners abroad, is scheduled to expire in December unless reauthorized by Congress. The government had little difficulty persuading lawmakers to renew the law in 2012 and 2018, despite growing evidence that it was being used to spy on Americans. But that evidence is now overwhelming, and the politics of surveillance have radically shifted. Section 702 is unlikely to be reauthorized this time without reforms.

What remains unclear is just how far Congress will go. The Biden administration and intelligence hawks in Congress will likely support minor tweaks at most, whereas other lawmakers will embrace far-reaching changes to the law. But Section 702 is just one part of a vast ecosystem of overlapping surveillance authorities, and addressing it in isolation would have limited effect. The government could evade any new restrictions by using other, more permissive authorities—or, in some cases, by simply purchasing the information from data brokers. If Congress intends to rein in warrantless spying on Americans, it will need to rethink surveillance more broadly.

A REASONABLE EXPECTATION OF PRIVACY

The framers of the U.S. Constitution understood that unjustified government intrusions into citizens' private lives threaten both individual liberty and the workings of democracy. The Fourth Amendment accordingly protects Americans from "unreasonable searches and seizures." Subject to limited exceptions, the Supreme Court has held that any government encroachment on a "reasonable expectation of privacy" is

inherently unreasonable under the Fourth Amendment unless the government has obtained a warrant from a court.

During the early decades of the Cold War, however, intelligence agencies frequently spied on social and racial justice activists, antiwar protesters, and political opponents in violation of their Fourth Amendment rights—abuses that came to light as a result of congressional inquiries in the 1970s. Moreover, the government believed, and some courts agreed, that warrants were not always required when the government eavesdropped on Americans' communications for the purpose of collecting "foreign intelligence": information about the intentions and activities of foreign entities.

Responding to these developments, Congress passed several laws to shore up Americans' constitutional rights and protect their privacy. One such law was FISA, which generally governs domestic collection of foreign intelligence. (Overseas collection of foreign intelligence usually relies on claims of inherent executive authority and is subject to far fewer constraints.) As enacted in 1978, FISA required the government to get a type of warrant known as a FISA Title I order to engage in domestic wiretapping of Americans' communications, including their communications with foreigners. To obtain such an order, the government had to show probable cause to the Foreign Intelligence Surveillance Court (or FISA Court), a special court created to oversee FISA surveillance, that the target of surveillance was a foreign power or agent of a foreign power.

After 9/11, Congress raced to loosen the restrictions on government surveillance that it had put in place two decades earlier. The 9/11 Commission later determined that U.S. agencies had ample intelligence about the planned attacks; they simply failed to share and act on that intelligence. But in the attacks' immediate aftermath, Congress assumed otherwise. It passed the U.S.A. Patriot Act, a 341-page bill that amended more than a dozen major federal laws, one day after introduction—before most members even had time to read it.

The law's sweeping new surveillance powers did not satisfy the government, however. President George W. Bush authorized a set of secret programs, code-named Stellar Wind, to collect communications

and other personal data without congressional authorization. One of these programs involved the domestic warrantless collection of the content of communications between suspected foreign terrorists and Americans in the United States. This was a clear violation of FISA: although the Patriot Act expanded the purposes for which the government could seek a Title I order, it did not eliminate the requirement to obtain one.

OPENING THE FLOODGATES

After *The New York Times* exposed the spying program in 2005, the government attempted to obtain legal cover for it by securing the FISA Court's approval. When the court balked, the government turned to Congress. Bush administration officials argued that changes in communications technology had resulted in foreigners' communications being handled by U.S. service providers, triggering legal protections in FISA that were designed for Americans and impeding counterterrorism efforts. They asked Congress to "modernize" FISA by loosening its restrictions.

Congress responded by enacting Section 702 of FISA in 2008. The law authorizes the government to target almost any foreigner abroad and collect the content of all their communications, including those with Americans, without obtaining an individualized court order. The only substantive restriction is that a significant purpose of collection must be the acquisition of foreign intelligence. The FISA Court annually approves general procedures for how the government collects and handles the information, but it has no role in approving individual targets.

In 2011, the government informed the FISA Court that it had collected 250 million Internet communications under Section 702 the previous year. Given the growth in the program, the number today is likely closer to one billion. This inevitably includes large volumes of Americans' communications, for the simple reason that Americans communicate with foreigners. The government refers to the collection of Americans' communication as "incidental" to signify that Americans are not the intended targets of the surveillance.

Critically, if the government's intent were to eavesdrop on those Americans, the program would be unlawful. Purposefully spying on Americans would require either a regular warrant (in criminal investigations) or a FISA Title I order (in foreign intelligence investigations). To prevent the government from using Section 702 as an end-run around these constitutional and statutory requirements, Congress included two key provisions in the law. First, the government must "minimize" the collection, sharing, and retention of Americans' information. Second, the government must certify that it is not engaged in "reverse targeting," namely, using the surveillance to obtain the communications of particular, known Americans.

DOMESTIC SPYING

Fifteen years into the program, it is clear that these protections are not working. The government, with the FISA Court's backing, has adopted a remarkably maximal interpretation of minimization. After collecting the data, the NSA routinely shares portions of it—including Americans' communications—with the CIA, FBI, and National Counterterrorism Center. All agencies retain the data for at least five years, and in some cases, such as when the data is encrypted, much longer.

The most controversial aspect of the program, however, is the use of "backdoor searches" (or, as the government refers to them, "U.S. person queries"): the practice of electronically searching the Section 702–acquired data to find and retrieve Americans' phone calls, text messages, and emails. In other words, having obtained the data without a warrant by certifying that it is not seeking access to the communications of particular, known Americans, the government then intentionally searches that very data for the communications of particular, known Americans.

Information obtained through backdoor searches can be used against Americans in cases having nothing to do with the original surveillance. The FBI routinely performs these queries at the beginning, or what is known as the "assessment" stage, of its investigations—before it has sufficient facts to support a reasonable suspicion of criminal activity, let alone probable cause and a warrant.

This practice is a bait-and-switch that violates the spirit of the reverse-targeting prohibition, if not the letter. It might also violate the U.S. Constitution. The FISA Court has blessed backdoor searches, but the court, which operates in secret and often hears only from government lawyers, is notoriously deferential to the government. Among the handful of regular federal courts that have had the chance to address these searches, several judges have expressed constitutional concerns. As federal appellate judge Carlos Lucero stated: "U.S. persons do not lose their protected privacy interests when they communicate with foreigners abroad."

After years of resisting calls to disclose the information, the government recently began reporting the number of backdoor searches conducted by the FBI. In 2022 alone, the FBI conducted around 200,000 of these queries—upward of 500 warrantless searches for Americans' communications every day. The NSA and CIA also conduct thousands of backdoor searches each year, according to government reports. These staggering numbers leave little doubt that a surveillance authority meant to target only foreigners has become something else entirely: a powerful domestic spying tool.

BREAKING THE RULES

Backdoor searches aside, Section 702 has been marked since its inception by repeated violations of the rules Congress and the FISA Court put in place to protect Americans' privacy. These violations are often revealed in FISA Court opinions that are declassified and made public in accordance with statutory requirements, as well as in government reports required by Congress.

One particularly serious violation dates back to the very beginning of the program. For several years, one of the NSA's collection methods resulted in the acquisition of tens of thousands of purely domestic communications. The NSA kept this information from the FISA Court until 2011. When the agency finally came clean, the court ruled that the agency's actions violated both Section 702 and the Fourth Amendment. It imposed a set of remedial measures designed to limit NSA's access to

Americans' communications. Five years later, the NSA reported that its agents had not been complying with these measures. It was not until 2017, after nine years of operating the program unconstitutionally, that the NSA stopped using this particular collection method.

Around the same time, Justice Department auditors began noticing and reporting violations of the FBI's requirements for U.S. person queries. The FISA Court had approved a rule that U.S. person queries must be reasonably likely to return foreign intelligence or evidence of a crime. That is a fairly low bar, compared with the probable cause showing required for a warrant. Nonetheless, beginning in 2018, the FISA Court issued a series of opinions finding that FBI agents had engaged in "widespread violations" of this standard.

The country is now headed for a reckoning over government surveillance.

Some of the reported breaches carry echoes of the politically and racially motivated surveillance abuses that occurred under J. Edgar Hoover's reign as the head of the FBI. In 2021, for instance, the FBI conducted 113 searches of Section 702–collected data for the communications of people who were arrested in connection with protests after the police killing of George Floyd. FBI agents reportedly wanted to find out whether the protesters had any foreign ties, but as the FISA Court found, they had no basis to suspect such connections. FBI agents also ran thousands of U.S. person queries in a baseless hunt for evidence of foreign involvement in the January 6, 2021, attack on the U.S. Capitol. That same year, the FBI searched for the communications of more than 19,000 donors to a congressional campaign. And between 2017 and 2020, the FBI searched for information about a member of the U.S. Congress; a local political party; multiple U.S. government officials, journalists, and political commentators; and two "Middle Eastern" men who were reported by a witness because they were loading boxes labeled "Drano" into a vehicle.

The FBI has also entirely ignored a separate limitation on U.S. person queries imposed by Congress. In 2018, Congress enacted a provision requiring FBI agents to obtain a warrant for a very small subset of queries

that take place in advanced-stage criminal investigations. According to a statistical report produced by the government, this requirement was triggered at least 100 times between 2018 and 2022. According to that same report, the FBI never once complied with it.

In response to these violations, the FBI implemented new training and oversight requirements. Officials promise that these changes will ensure compliance with the rules going forward. But the government has made similar claims on numerous occasions, and there has been little effect on the overall pattern of violations. As surveillance expert Julian Sanchez put it, the government has been engaged in a 15-year game of "compliance whack-a-mole."

Given this history of violations, one might well wonder why the FISA Court continues to approve Section 702 surveillance. At bottom, the FISA Court operates fundamentally differently from ordinary courts. In most cases, it hears arguments only from one party: the U.S. government. It must accept the facts that the government presents, as there is no discovery process to unearth additional or conflicting information. And the government attorneys who appear before the court are repeat players who engage in an ongoing dialogue with court staff, creating a kind of partnership dynamic. Reading the court's opinions, it is difficult to escape the conclusion that the court, even when expressing profound frustration over the government's conduct, sees its role as "getting to yes."

COLLECTING IT ALL

When Section 702 was enacted, government officials and lawmakers described its purpose as preventing terrorist attacks. As the threat of terrorism has become less salient, the government's description of Section 702's value has shifted. Officials now tout the law's usefulness in combating cybersecurity attacks, fentanyl trafficking, and espionage attempts by China and other major powers.

But no threat of any kind is required to conduct surveillance under Section 702. The law permits surveillance of any foreigner abroad, as long as a significant purpose of the surveillance is to acquire "foreign intelligence information." FISA defines this term extremely broadly to

include any "information related to . . . the conduct of U.S. foreign affairs." A conversation between friends about whether the United States should do more to support Ukraine would justify surveillance under this definition.

Spying on foreigners without a sufficient security-based justification would violate their privacy rights under international agreements, such as the International Covenant on Civil and Political Rights, to which the United States is a party. And the mere license to engage in such surveillance is already creating headaches for U.S. businesses. In 2015 and 2020, the Court of Justice for the European Union struck down U.S.-EU agreements governing the transfer of EU citizens' data from EU companies to U.S. companies—agreements that allowed more than 5,000 U.S. companies to do business overseas. The European court ruled that U.S. companies could not provide adequate protections for EU citizens' data, in part because Section 702 provides the U.S. government with such easy access.

The sprawling scope of Section 702 surveillance also has privacy implications for Americans. The larger the pool of permissible targets, the greater the amount of "incidental" collection that may occur. Moreover, if the government can target ordinary private citizens of other nations, that greatly increases the chances of obtaining wholly innocent conversations between Americans and their friends, colleagues, and relatives overseas.

POLITICS UPENDED

Since Section 702's enactment, progressives and libertarians in Congress have expressed concerns over the law and have worked together to try to reform it. But until recently, centrist Democrats and Republicans supported the law. Moreover, the congressional intelligence committees, like the FISA Court, have tended to act as intelligence agencies' partners rather than their overseers. These committees have exercised their clout to sideline reform efforts.

Over the course of the Trump administration, however, the politics of FISA radically shifted. The Department of Justice's inspector general issued a report in 2019 with sobering findings: the government's

applications to the FISA Court under Title I of FISA to surveil a Trump campaign aide, Carter Page, were riddled with errors and omissions. A follow-up report showed that similar flaws pervaded Title I surveillance applications in general, suggesting that slipshod submissions to the FISA Court are the norm. Nonetheless, Trump and his supporters in Congress concluded that the Obama administration (which initiated the Page surveillance) abused FISA for political purposes.

Since then, a large faction of Republicans has turned against FISA in all its forms. When a different provision of FISA came up for reauthorization in 2020, Trump fired off a storm of tweets opposing it, and the reauthorization failed. As for Democratic lawmakers, four years under Trump opened their eyes to the importance of meaningful checks on executive power. They also have been alarmed by recent revelations about the frequency of backdoor searches and the FBI's widespread violations of querying rules, including incidents of spying on racial justice protesters.

Democrats' concerns about Section 702 have been reinforced by recent abuses and misuses of other forms of warrantless data gathering. In 2019, U.S. Customs and Border Protection created a list of American reporters, lawyers, and activists who were subject to questioning and enhanced scrutiny at the border because of their role in assisting asylum seekers. During the summer of 2020, the Department of Homeland Security created dossiers on racial justice protesters and monitored their social media accounts. In late 2020, *Vice News* reported that the Department of Defense had purchased geolocation information generated by popular Muslim prayer and dating apps. And in 2022, DHS monitored social media for "reactions" and "reflections" related to the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*.

These incidents serve as stark reminders that warrants protect not only privacy but also the civil rights of marginalized communities. When government officials are not required to furnish evidence of wrongdoing, it is much easier for them to fall back on conscious or subconscious prejudices, whether racial, religious, or political.

GET A WARRANT

Given the newly reshaped political landscape, lawmakers are unlikely to reauthorize Section 702 this year without significant reforms. They should start by requiring government officials to obtain a warrant or a FISA Title I order before conducting U.S. person queries of communications obtained under Section 702. An amendment along these lines passed the House of Representatives in 2014 and 2015, and U.S. Vice President Kamala Harris cosponsored a similar amendment in 2018 when she was still a senator.

Government officials have countered that a warrant requirement would be unworkable. The courts lack the capacity, they argue, to absorb an additional 200,000 warrant applications each year; in any event, the government lacks probable cause in many of these cases. But of course, the massive number of queries and the absence of probable cause for those queries is exactly why advocates and lawmakers are pushing for a warrant requirement. The fact that warrants constrain government surveillance is a feature, not a bug.

Officials also assert that warrantless U.S. person queries are necessary to identify potential U.S. victims of foreign cyberattacks, spy recruitment efforts, and foreign influence campaigns. The argument has superficial appeal. But the need to protect victims is hardly unique to foreign intelligence cases. Law enforcement agencies are routinely faced with this task, and they manage to keep the public safe using investigative techniques that comport with the Fourth Amendment—including obtaining the consent and cooperation of potential victims themselves. There is no "victim" exception to the Fourth Amendment.

There is good reason for that. Regardless of the purpose of a search, the result is to expose an American's private information to review by a government agent, with all the potential for abuse such access entails. Indeed, the line between "victim" and "suspect" can be quite malleable—particularly when the activity being investigated is alleged foreign influence. Under J. Edgar Hoover, the FBI justified spying on antiwar protesters and civil rights activists by claiming that foreign communist groups were attempting to influence or infiltrate them.

In addition to closing the backdoor search loophole, Congress should narrow the pool of permissible targets to people or groups who are likely

to have information about a threat to the United States or its interests, rather than allowing the surveillance of almost any foreigner overseas. This would better protect the privacy of innocent foreign nationals and the Americans with whom they communicate, and it would ensure that U.S. companies can continue doing business with their counterparts in the European Union.

A BORDERLESS WORLD

If Congress stops at Section 702, however, its reforms will have limited impact. For one thing, the majority of the government's foreign intelligence surveillance activities do not take place under FISA at all.

Generally speaking, and regardless of whether the target is a foreigner or an American, FISA applies when the government collects information inside the United States or from U.S.-based companies. When the government conducts surveillance abroad, it typically relies on a claim of inherent presidential authority, as regulated by Executive Order 12333, a 1981 directive issued by President Ronald Reagan. This executive order has far fewer protections for Americans' privacy than FISA, and surveillance under it involves no judicial oversight whatsoever.

In 1978, when FISA was enacted, there was arguably some logic to the geographical distinction it incorporated. Domestic surveillance usually meant surveillance of Americans; overseas surveillance usually meant surveillance of foreigners. Today, however, communications are routinely routed and stored all over the world, regardless of where they originate or terminate. Indeed, the fact that purely foreign communications were being routed and stored inside the United States, thus triggering FISA's requirement of a probable-cause order, is one reason the government sought to "modernize" FISA in 2008 through the enactment of Section 702.

But Section 702 addressed only half of the problem. Just as foreigners' communications can travel through or reside in the United States, purely domestic communications frequently travel through or reside in other countries. An email between a mother in Akron, Ohio, and her daughter in Spokane, Washington, could transit over fiberoptic cables in France or

sit on a Google server in Ireland. In some cases, this digital wandering can remove domestic communications from FISA's protections and expose them to surveillance under the Reagan-era executive order. Congress and the executive branch have imposed limits on the targeting of Americans under this order, but these limits have little effect when the government engages in "bulk collection," a type of dragnet collection in which there are no specific targets. Bulk collection is prohibited under Section 702, but it is permitted under Executive Order 12333.

No threat of any kind is required to conduct surveillance under Section 702.

Moreover, even when targeted at specific foreigners rather than conducted in bulk, surveillance under Executive Order 12333 results in the "incidental" collection of Americans' communications, just as Section 702 surveillance does. Yet privacy protections for this information are left almost entirely to executive branch policies, with no court review to ensure that the policies comply with the Constitution—or that agencies comply with the policies. Agencies can and do perform backdoor searches of data obtained under the executive order.

In 2022, *The New York Times* reported that the CIA is conducting a set of bulk collection activities under Executive Order 12333 that pull in Americans' data, which CIA agents may retrieve through U.S. person queries. One group of programs collects information about financial transactions. Another program remains so heavily classified that the type of data being collected remains unknown, although the CIA's scant public statements suggest that the information pertains to communications.

Americans' constitutional rights should not depend on the accident of where their digital data happens to travel. To complete the modernization of FISA that began with Section 702, Congress should extend FISA's protections—including new protections resulting from Section 702 reforms—to any surveillance that acquires Americans' constitutionally protected information, regardless of where that surveillance takes place. Without this step, the government could undermine the impact of Section 702 reforms by shifting at least some domestic surveillance overseas.

FOURTH AMENDMENT RIGHTS FOR SALE

In cases where overseas collection proves impracticable, the government has another avenue for obtaining Fourth Amendment–protected data without a warrant: buying it.

In 2021, a series of investigative reports revealed that federal agencies—including the FBI, the Drug Enforcement Administration, Immigration and Customs Enforcement, Customs and Border Protection, the Secret Service, and the Department of Defense—were paying data brokers to obtain access to Americans' cell phone location information, sometimes in massive amounts. Even the Internal Revenue Service, according to *The Wall Street Journal,* "attempted to identify and track potential criminal suspects by purchasing access to a commercial database that records the locations of millions of American cellphones."

This practice would seem to violate *Carpenter v. United States,* a 2018 case in which the Supreme Court held that police needed a warrant to acquire a week's worth of geolocation information from a cell phone company. The decision broke new ground: courts had previously ruled that people have no Fourth Amendment rights when it comes to information they voluntarily disclose to third parties, such as phone companies. But the Court reasoned that detailed geolocation data can reveal the most intimate details of people's lives, including their associations, habits, and even beliefs. And there is nothing truly voluntary about disclosing it, as owning a cell phone is necessary to participate in modern life.

A large faction of Republicans has turned against FISA in all its forms.

Government lawyers, however, have found a way around the case law. They have construed *Carpenter* to apply only when the government compels companies to produce the data. When the government merely provides a cash incentive for such production, they argue, the warrant requirement disappears. Questionable as this analysis may be, it could take years for the courts to resolve the issue.

There are privacy laws that limit these types of purchases, but they include gaping loopholes. The Electronic Communications Privacy Act,

for instance, prohibits telephone and Internet companies from voluntarily disclosing customer records to government agencies. But the prohibition does not extend to digital data brokers—unsurprisingly, as these entities barely existed in 1986, when the law was passed. This gap creates an easy end-run around the law's protections: companies that are barred from selling data to the government directly can effectively launder it through data brokers.

Congress should expressly prohibit the government from evading FISA's requirements through the use of data brokers. But Congress should not stop there. Most of the laws that protect Americans' privacy do not come with sunset provisions (which cause the legislation to expire unless Congress extends it). The political stars rarely align to prompt reforms to such laws, or even basic updates to ensure that they keep up with technology. Lawmakers should use the leverage provided by the expiration of Section 702 to close the data broker loophole for all investigations, not just those involving foreign intelligence. Specifically, Congress should bar the government from purchasing information if the compelled production of that information would require a warrant, court order, or subpoena under U.S. law.

WINDOW OF OPPORTUNITY

Indeed, lawmakers who care about civil liberties would be wise to seize the rare political moment presented by this year's reauthorization of Section 702 to address surveillance practices more broadly.

In the past two decades, Congress and the executive branch have dramatically weakened many of the legal restrictions on surveillance that were put in place to safeguard Americans' constitutional rights. These legal changes have coincided with advances in technology that have had the effect of putting surveillance on steroids. With the arrival of smart devices, Americans generate mind-boggling amounts of information, often without even being aware of it, and almost all the data is stored by third parties. The Supreme Court has only just begun to extend Fourth Amendment protections to such information. On the "demand" side of the equation, the government's technological ability to capture and store

these rich streams of data, and to apply sophisticated algorithms to tease out highly personal information, is nearly limitless.

This state of affairs is a recipe for abuse, as we are beginning to see. Under Section 702 and other authorities that allow warrantless collection of sensitive data, law enforcement and intelligence are gaining access to sensitive information about social justice activists, journalists, and politicians. Without fundamental changes to the law, there will surely be more of these abuses—and perhaps worse ones—in the future.

In short, the United States is long overdue for a rightsizing of government surveillance. The reauthorization of Section 702 provides the best opportunity Congress has had since 9/11, and perhaps will have for a long time, for that undertaking. Lawmakers will almost certainly enact reforms to Section 702. At a minimum, they will place restrictions on backdoor searches. But unless Congress is willing to attack the other heads of the Hydra, it will have done little to rein in warrantless surveillance of Americans.