Primer: FISA's 702 Program Requires Major Reforms to Safeguard Americans

By: Jeffrey Bossert Clark

Summary

Title VII of the Foreign Intelligence Surveillance Act (FISA) will expire at the end of the year unless Congress reauthorizes it. FISA's Section 702 provides tools to the federal government ostensibly for targeting foreign individuals and entities located abroad that pose a threat to the national security of the United States.[1] However, the program has become known more for its infringements on the rights of American citizens and its abuses by federal law enforcement and intelligence agencies than for its stated security purpose.

In light of this reality—and the broader weaponization of government against the American people—it is imperative that Congress use this moment to force a realignment of the bureaucracy and reform FISA, along with the FBI itself.

Background

The Foreign Intelligence Surveillance Act was enacted in 1978 as part of an expansive effort to codify the surveillance and information-gathering activities of federal law enforcement and intelligence entities. The legislation sets out specific parameters for the collection of foreign intelligence information through physical and electronic surveillance techniques. Its existence is primarily due to the discovery of significant abuses in various agencies exposed by the Church Committee in 1975-76. The committee's findings uncovered disturbing operations by the Federal Bureau of Investigation (FBI) to both surveil and infiltrate multiple political and civil rights organizations, efforts by the Central Intelligence Agency (CIA) to drug and torture

[1] Tarinelli, R. (April 27, 2023). "Congress Starts Work on Renewal of Controversial Surveillance Law," *Roll Call*. https://rollcall.com/2023/04/27/congress-starts-work-on-renewal-of-controversial-surveillance-law/.

American citizens in order to experiment with mind-control techniques, and coordination between major telecommunication companies and the National Security Agency (NSA), exposing the existence of the NSA to the American public for the first time.[2]

The creation of the Senate Select Committee on Intelligence and FISA following the release of the Church Committee's findings initially served as prospective remedies for the illicit and disturbing abuses of power within federal intelligence and law enforcement agencies. In the intervening decades, however, FISA itself has become emblematic of a weaponized Washington at war with its own citizens.

FISA has undergone a number of reforms, revisions, and expansions since its inception. Among the most impactful were the:

- **Intelligence Authorization Act of 1995:** This legislation created Section 811 and the National Counterintelligence Policy Board to help settle intergovernmental agency disputes and develop the procedures for the President to oversee counterintelligence activities.
- **USA PATRIOT Amendments Act of 2006:** This legislation extended key provisions from the Patriot Act, including roving wiretaps under FISA, permission for the FBI to utilize FISA Court orders to seize any tangible item belonging to a target with minimal judicial review, and expanded year-long wiretap authority.
- **FISA Amendments Act of 2008:** Arguably the most profound expansion since the creation of FISA in 1978, this legislation added the current Section 702 and established a warrantless surveillance regime that threatened the rights of the American people.

When Congress created the now-infamous Section 702 under Title VII, it granted the NSA, FBI, and other entities unprecedented power to conduct surveillance operations against non-U.S. persons located outside the United States through the coerced cooperation of U.S.-based electronic communications providers. Specifically, Section 702 authorized the warrantless "collection, use, and dissemination of electronic communications content stored by U.S. internet service providers . . . or traveling across the internet's 'backbone.'"[3]

---

[2] Select Committee to Study Governmental Operations with Respect to Intelligence Activities (April 23, 1976). "Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities," U.S. Senate. https://www.rightsanddissent.org/resource/church-committee-final-report-book-iii-1976/.
[3] "Section 702: What Is It and How It Works," *Center for Democracy and Technology.* https://cdt.org/wp-content/uploads/2017/02/Section-702.pdf

The foreign intelligence benefit of Section 702 has always been dependent on the say-so of the U.S. intelligence community, who alone have the authority to declassify details of purported "success stories"—and lack the incentive to shine a light on failures and missteps. According to recent congressional testimony from representatives of five government agencies, "Section 702 helped foil an active plot to bomb the New York City subway" in 2009 and "played an important role in the strike against Al-Qa'ida's leader, Ayman al-Zawahiri" in 2022.[4]

Under Section 702 as it is currently being implemented, even the carefully curated "success stories" reflect a drift from the counterterrorism context in which the tool was originally developed and implemented. According to senior Biden administration officials, among the key reasons Section 702 should be reauthorized is its utility in calling out Russia, China, and an unnamed Middle Eastern country regarding human rights violations.[5]

Beyond the uncertainty of its national security benefits, the fundamental problem with Section 702 is that the U.S. intelligence community has *never* implemented the program to achieve such benefits while safeguarding the rights of Americans. Title VII includes explicit protections against targeted surveillance of U.S. persons. However, in reality, the incredibly powerful blunt instrument unleashed by well-meaning legislation inevitably vacuumed up the data, communications, and private information of American citizens who interacted intentionally, inadvertently, or even tangentially with those targeted by Section 702–all without the use of a warrant. According to recent reports, FBI conducted warrantless searches impermissibly targeting U.S. persons at least 278,000 times in 2020 and 2021 alone.[6]

While the statutory language expressly prohibits the targeting of Americans and instructs the FISA Court to engage in annual oversight of the activities within the program, the 702 program has remained one marred by endemic abuse, rampant corruption, constant ineptitude, and opaque accountability mechanisms. It is for these reasons that, in less than two decades of the program's existence the FISA Court has published five public rebukes to federal agencies for abusing their authority and violating the rights of Americans. Moreover, publicly available information about these abuses is often redacted, delayed, and incomplete.

---

[4] Fonzone, C. et al. (June 13, 2023). "Senate Judiciary Committee Joint Statement for the Record," U.S. *Department of Justice.* https://www.justice.gov/d9/2023-06/Section%20702%20of%20the%20Foreign%20Intelligence%20Surveillance%20Act.pdf

[5] *Ibid.*

[6] Siqqiqui, Z. (May 19, 2023). "FBI misused intelligence database in 278,000 searches, court says," Reuters. https://www.reuters.com/world/us/fbi-misused-intelligence-database-278000-searches-court-says-2023-05-19/

In the span of just 15 years, Section 702 has morphed into the premier domestic spying tool used by government security and intelligence agencies to collect the phone records, e-mails, and texts of American citizens. The Section 702 program is now arguably the metaphorical tip of the spear of a government weaponized against its own citizens.

A Brief Overview of Section 702

The process within 702 is relatively straightforward, though the decision-making on the front-end of that process and the impact on its back-end continue to remain murky and subjective despite the touted safeguards.

First, the Attorney General and Director of National Intelligence (DNI) submit FISA certifications to the FISA Court outlining the categories of foreign intelligence that the intelligence community intends to use Section 702 to collect. These certifications are required to include specifications on protections given to U.S. citizens so that their Fourth Amendment rights are not breached.

The FISA Court then reviews the certifications annually to ensure compliance and writes an opinion on whether or not the agencies have violated the provisions of the law or the constitutional rights of American citizens.

Once the FISA Court has approved of the proposed certifications, the Attorney General and DNI have the authority to compel electronic communication service providers to comply with the targeting of individuals or entities under the Section 702 surveillance program.

On a granular level, agency analysts then go after the e-mails, text messages, or other communiques of a target so long as the user is a non-U.S. person located outside the United States and their communications contain foreign intelligence of interest within the parameters of the certification. The NSA then engages in “upstream” data collection by acquiring target data from the communications as they go out with the assistance of service providers. The FBI, CIA, and other entities, like the National Counterterrorism Center (NCTC), then engage in “downstream” collection by acquiring the communications directly from the service provider.

Americans are supposedly protected by the statutory prohibitions against domestic surveillance, congressional oversight, annual FISA Court oversight, and the relevant

inspectors general. Unfortunately, such oversight remains toothless, and the ease with which the program can be and is abused has a long and increasingly alarming history.

FISA: A Long History of Abuses

Since its very inception in 1978, FISA teetered on the knife's edge as a tool conceived to provide protections for the American people against agency corruption versus a clandestine mechanism that could accelerate abuses in the name of national security. It is eminently clear that today's FISA resembles the latter far more than the former.

In 2001, a Department of Justice Inspector General (IG) report found that the FBI had engaged in egregious errors in its FISA application methods—endangering the rights of American citizens in the process. In an effort to mitigate the damage such errors could inflict, former FBI attorney Michael Woods implemented numerous changes to ensure that FISA applications relied on "scrupulously accurate" information. Thus was born the Woods Procedures—the appropriately high standards of citation and corroboration that agents are supposed to meet to carry out a FISA application.[7]

Arguably, the most prominent abuse of the FISA process and Woods Procedures is that of Crossfire Hurricane, an operation launched by the FBI to investigate what the public now knows as fraudulent connections between the Trump campaign and Russia in the lead-up to the 2016 presidential election. The investigation relied on bogus opposition research generated by FusionGPS, a sub-contractor of Hillary Clinton's campaign and the Democratic National Committee that (ironically) relied on Russian-sourced gossip and innuendo.[8]

---

[7] Barrett, D. (September 30, 2021). "Inspector General Finds Widespread Problems in FBI's FISA Applications," *The Washington Post*. https://www.washingtonpost.com/national-security/fisa-woods-file-fbi-inspector-general/2021/09/30/2588e666-21ff-11ec-b3d6-8cdebe60d3e2_story.html

[8] Durham, J. (May 12, 2023). "Report on Matters Related to Intelligence Activities and Investigations Arising Out of the 2016 Presidential Campaigns," *U.S. Department of Justice.* This Durham Report accurately summarizes how the FISC proceeds when U.S. citizens are accused of being agents of a foreign power:

> The FISC may authorize electronic surveillance if there is probable cause to believe that the target of the surveillance is an agent of a foreign power. For a U.S. person, there are at least two additional related requirements. First, as the House Intelligence Committee's 1978 report on FISA explains, "[a]s a matter of principle ... no United States citizen ... should be targeted for electronic surveillance ... absent some showing that he at least may violate the laws of our society." Second, the person must be knowingly engaged in the specified conduct. Thus, a U.S. person may be an agent of a foreign power if the person is knowingly engaged in clandestine intelligence gathering activities on behalf of a foreign power, or knowingly helping another person in such activities, provided that the activities involve or may involve a violation of U.S. criminal law.

As the Durham Report confirmed, FusionGPS commissioned a document known as the Steele dossier alleging nefarious activities between then-candidate Donald Trump's business contracts and ventures in Russia. The information, however, was fabricated and stemmed from a confidential human source—a Russian national and onetime suspected spy named Igor Danchenko—who admitted the information was "rumor and speculation." The Durham Report stated that no one, including Danchenko, "was []able to provide any corroborating evidence to support the Steele allegations."[9]

Despite some of these red flags, the FBI submitted a FISA application targeting Carter Page, who had been affiliated with the Trump campaign as a foreign policy advisor at a time when much of the national security establishment was actively shunning Trump's candidacy. Among other claims, FBI told the FISA Court that it believed Page "currently is acting as an unregistered agent of the Russian Federation to undermine and influence the outcome of the 2016 U.S. presidential election in violation of U.S. criminal law." The FISA application relied in substantial part on the fabricated Steele dossier. The Bureau renewed the application to spy on Page three more times, despite knowing that the probability that Page was a Russian asset was "very low."[10] The IG later identified 17 "significant inaccuracies and omissions" associated with these applications,[11] and determined that at least the last two were legally deficient.[12] In effect, Crossfire Hurricane resulted in the FBI carrying out a political operation to spy on a presidential campaign–using dubious FISA applications—at the behest of a rival political campaign with information fabricated by a Russian national. Based on a lie, that investigation fueled rampant and ongoing discord among American citizens.

The revelations concerning the Carter Page FISA applications naturally generated questions about whether the associated abuses were isolated or systemic. An IG report from September 2021 revealed that the processes the FBI uses to seek FISA warrants are, unfortunately, riddled with widespread errors despite prior efforts at reform. The

---

[9] Durham Report at 13.

https://www.justice.gov/storage/durhamreport.pdf

[10] *Ibid.*

[11] Horowitz, M. (December 11, 2019). "Statement of Michael E. Horowitz, Inspector General, U.S. Department of Justice before the U.S. Senate Committee on the Judiciary concerning 'Examining the Inspector General's Report on Alleged Abuses of the Foreign Intelligence Surveillance Act'," Office of the Inspector General, U.S. Department of Justice.

https://oig.justice.gov/node/1100

[12] Shortell, D. and Perez, E. (January 23, 2020). "Two of four FISA warrants against Carter Page declared invalid," CNN.

https://www.cnn.com/2020/01/23/politics/fisa-carter-page-warrants/index.html.

Woods Procedures, implemented two decades prior, require the agency to include an attached file on a warrant application that justifies every assertion being made against a particular individual or entity. The IG report made clear even the Woods protocols were doing little to mitigate abuse.[13]

Specifically, the 2021 IG report revealed that among the 29 wiretap applications examined in the audit, the FBI failed to provide adequate documentation to support their claims a stunning 209 times.[14] That's an average of 10 times per application in this assessment. Further, the abuses were so profound that in four of the 29 cases, the FBI omitted relevant information that could have altered the FISA Court's decision to approve an application.[15]

These preliminary discoveries from the IG pushed the FBI to publish an expanded audit of nearly 7,000 FISA applications from January 2015 through March 2020. In 183 cases, roughly 2.6 percent of the total applications examined, the Woods Procedures files were destroyed, incomplete, or missing outright.[16]

Section 702: More Alarming Abuses

Following the 9/11 attacks, the Bush administration implemented a classified collection program known as Stellarwind that tasked the NSA not only with monitoring the phone calls of known or suspected Al-Qaeda operatives, but also the bulk phone metadata regarding all phone calls made in the United States.[17] This program served as the largest foray to date in warrantless surveillance and data collection and effectively circumvented FISA protocols while achieving FISA goals. The revelation to the American public of Stellarwind's existence in December 2005 created a political uproar

---

[13] Horowitz, M. (September 2021). "Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures For Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons," *Office of Inspector General, U.S. Department of Justice*.

https://oig.justice.gov/sites/default/files/reports/21-129.pdf

[14] *Ibid.*

[15] Editorial Board (October 5, 2021). "The FBI's Other Secret Warrant Abuses," *The Wall Street Journal*. https://www.wsj.com/articles/the-non-compliant-fbi-inspector-general-michael-horowitz-report-department-of-justice-fisa-surveillance-abuse-11633472138.

[16] Kennedy, B. (September 30, 2021). "DOJ Watchdog Uncovers 'Widespread' Issues with FBI's Handling of Surveillance Warrants," *The Week*. https://theweek.com/us/1005537/doj-watchdog-uncovers-widespread-issues-with-fbis-handling-of-surveillance-warrants

[17] Brenner, J. (October 2021), "Reflections on the IG's Role, Stellarwind, and the Information Sharing Fiasco," *Journal of National Security Law and Policy*. https://jnslp.com/wp-content/uploads/2021/10/Reflections-on-the-IGs-Role-Stellarwind-and-the-Information-Sharing-Fiasco_2.pdf

but also laid the predicate for the eventual statutory changes that emerged at the end of the Bush administration. These changes codified Section 702 and the procedural guidelines for widespread warrantless surveillance.

While the Patriot Act became the most well-known piece of legislation to supercharge domestic spying capabilities, it wasn't until the FISA reauthorization in 2008 that Section 702 was born and catalyzed the weaponization of federal agencies against American citizens through warrantless surveillance programs.

Just three years after Section 702 powers were implemented under the FISA Amendments Act of 2008, the FISA Court learned of mass violations of the Fourth Amendment due to so-called "about" collections from agencies utilizing Section 702's bulk data protocols. Specifically, federal agencies were acquiring communications that not only went to or from a specific target, but also information that *mentioned* a specific target. Tens of thousands of Americans had their private communications monitored and collected, unbeknownst to them, for simply mentioning individuals under active Section 702 applications.[18] The abuse of the Section 702 program hit new heights in the Obama administration, with bulk e-mail records of American citizens secretly collected by the NSA for more than two years.[19]

When the FISA Court demanded that the NSA implement a series of changes to its protocols for accessing "upstream" communications in 2012, the agency failed to comply. However, it was not until 2016 that the FISA Court formally rebuked the NSA for remaining in non-compliance with its data collection efforts. This eventually resulted in the NSA abandoning its "abouts" collection program in 2017 prior to congressional debate on reauthorizing FISA.[20] Yet, it took less than a year for federal agencies to implement a workaround to continue mass data collection, an inherent violation of the U.S. Constitution.

In 2018, the FISA Court once again found the federal government—specifically the FBI—in continued non-compliance due to a new workaround to collect downstream data. When Congress reauthorized FISA's Section 702 program in the same year and created new reporting requirements on counting individual queries of American citizens, the FBI "complied" by combining both queries of U.S. citizens and foreign targets

---

[18] Goitein, E. (October 15, 2019). "The FISA Court's 702 Opinions, Part I: A History of Non-Compliance Repeats Itself," *Just Security*. https://www.justsecurity.org/66595/the-fisa-courts-702-opinions-part-i-a-history-of-non-compliance-repeats-itself/

[19] Greenwald, G. and Ackerman, S. (June 27, 2013). "NSA Collected US Email Records in Bulk For More Than Two Years Under Obama," *The Guardian*. https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

[20] *Ibid*

without distinguishing between the two groups.[21] This decision sat poorly with the FISA Court, which determined that the statute was unambiguous and the U.S. government had violated the plain text of the reauthorizing language.[22]

Of course, concerns about the processes that go into FISA applications are both longstanding and in many respects bipartisan. Analysis by the liberal New America Foundation at the end of 2017 revealed that Section 702 compliance violations began to spike considerably in 2014.[23] The most common error was so-called "query violations" wherein analysts at the FBI or NSA conducted improper searches, reviewed private information that should not have been reviewed, or engaged in domestic surveillance activities that were unlikely to result in the gathering of foreign intelligence information.

Such query violations continue to be a significant issue.

In a 127-page opinion from April 2022, the FISA Court stated that the FBI engaged in "significant violations" of existing standards for accessing the data of private citizens, including many cases related to the January 6, 2021 protests at the U.S. Capitol.[24] Some of those violations included a breach into an individual's private emails, multiple "batch queries" collecting bulk data on individuals thought to have been at the U.S. Capitol that day, and one FBI agent in particular accused of running 13 improper queries and admitting to running "thousands of names through the FBI system" as part of her investigation into the January 6 protests.[25]

And yet, even after the FBI implemented changes to the manner in which it conducts these "backdoor searches," the agency's Office of Internal Auditing recently revealed an overall non-compliance rate that was roughly 4 percent.[26] Given the number of searches and queries carried out each year, this means thousands of FISA abuses occur every year—at a minimum.

---

[21] Boasberg, J. (October 18, 2018), "Memorandum Opinion and Order," *U.S. Foreign Intelligence Surveillance Court*. https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf.

[22] *Ibid.*

[23] Greene, R. (September 28, 2017). "A History of FISA Section 702 Compliance Violations," *New America Foundation*.
https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/.
[24] Dunleavy, J. (May 19, 2023). "FBI Abused Surveillance Tool Against Jan. 6 Suspects," *The Washington Examiner*. https://www.washingtonexaminer.com/news/justice/fisa-court-reveals-fisa-abuses-fbi-capitol-riot-investigation

[25] *Ibid.*

[26] Office of Internal Auditing (May 10, 2023). "FISA Query Audit May 2023," *Federal Bureau of Investigation, U.S. Department of Justice.*

https://www.fbi.gov/file-repository/fisa-query-audit-051023.pdf/view.

As background, the FBI conducted an astonishing 3.4 million warrantless searches of Americans in 2021 under the auspices of Section 702.[27] As frightening as the sheer volume of such queries should be, the error rate regarding basic competency underscores the danger even more. The FISA Court determined that approximately 278,000 of these searches were improper. On April 27, 2023, the House Judiciary Committee heard testimony from DOJ Inspector General Michael E. Horowitz who claimed his audit had instead ***found an error rate of nearly 30 percent in these 3.4 million FISA queries.***[28] If accurate, that would translate to some 1,020,000 queries against individuals or entities in a single year that contained errors of competence, judgment, substance, or some combination thereof.

The weaponization of the FISA program—increasingly for political purposes—could not be clearer. Its existence—particularly in its current form—poses a continued threat to both the God-given rights and safety of an increasing number of American citizens. If the FISA Court—one of the most staid, secretive, and pro-establishment institutions in the country—has repeatedly expressed exasperation with intelligence agencies' implementation of Section 702 and violation of Americans' civil liberties, one wonders how bad the abuses really must be. Given the corruption endemic within the FBI and that agency's public war against Americans who do not share the radical ideological proclivities of the Beltway elite, it is self-evident that the status quo cannot continue.

Recommendations on Potential Reform by Others

Many individuals and groups have weighed in on the contentious topic of Section 702 reform. James Baker is the former General Counsel of the FBI. He went on to serve as the Deputy General Counsel of Twitter (now X) but was fired last year by Elon Musk for trying to obstruct the revelations contained in the "Twitterfiles" controversy—especially for his role in the suppression by Twitter and other BigTech entities of the Hunter Biden laptop story.[29] Given his work on both ends of joint public-private censorship regimes, it

---

[27] Bovard, J. (May 21, 2023). "The FBI Just Got Caught in Yet More Massive, Outrageous FISA Abuses," *New York Post*.

https://nypost.com/2023/05/21/the-fbi-just-got-caught-in-yet-more-massive-outrageous-fisa-abuses/.

[28] Subcommittee on Crime and Federal Government Surveillance (April 27, 2023). "Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them," *Committee on the Judiciary, U.S. House of Representatives*.
https://judiciary.house.gov/committee-activity/hearings/fixing-fisa-how-law-designed-protect-americans-has-been-weaponized.

[29] Victor Nava, "Elon Musk Fires Twitter Lawyer James Baker Over 'Suppression' of Documents on Hunter Biden Story," New York Post (Dec. 7, 2022).

may not be surprising that Baker advocates reauthorizing Section 702 without a new warrant requirement.

Baker concedes that Section 702 is a warrantless search requirement (therefore implicating special concerns under the Fourth Amendment) but he argues that "Section 702 is constitutional because the searches it authorizes are reasonable in light of the structure and purpose of the law."[30] This imagines that as long as it is reasonable to conduct searches as an overarching or "batch" matter, they can properly be authorized by the courts. But this framing ignores that the Fourth Amendment is plainly structured to require an individualized determination of whether a given search or seizure is reasonable or unreasonable, not a blanket trawling net that scoops up vast troves of information that then can be queried later at the discretion of FBI agents and other government actors.

In an argument contemptuous of the Constitution, Baker argues that at most an *ex post* warrant system from the FISA Court could be used.[31] But Fourth Amendment-compliant warrants obviously embody an *ex ante* warrant system where probable cause must be demonstrated before a warrant can be executed.

Baker's objections to any form of warrant requirement mostly boil down to workability objections. In other words, if a warrant requirement is imposed, the FBI may not be able to query the information scooped up from the telecom companies regarding domestic subjects as frequently as it can do now. But in light of the large number of abuses described above, one cannot assume that the benefits are worth the costs. Trying to drive abuse out of the system by creating Executive Branch protocols can hardly be expected to be successful. And they beg the question of Fourth Amendment compliance anyway. Or, as Chief Justice Roberts once put it, "The Government proposes that law enforcement agencies 'develop protocols to address' concerns raised by cloud computing. Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols."[32]

Around the same time as Baker's suggestions were penned, the Privacy and Civil Liberties Oversight Board (PCLOB) issued its 297-page Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, the first of its kind in attempting to provide an overview of the Section 702 program using unclassified information (though the Report does have a classified Annex). The overall bottom line of the PCLOB Report is:

---

[30] Jim Baker, "Reflections on Renewing and Reforming FISA Section 702," Just Security (Sept. 27, 2023).
[31] Baker, "Reflections."
[32] *Riley v. California*, 573 U.S. 373, 398 (2014).

> The Board concludes that although the Section 702 program presents serious risks to, and actual intrusions upon, the privacy and civil liberties of both Americans and non-Americans, the United States is safer with the Section 702 program than without it. The Board further finds that the most serious privacy and civil liberties risks result from U.S. person queries and batch queries, and the government has not demonstrated that such queries have nearly as significant value as the Section 702 program overall.[33]

PCLOB also includes 19 granular recommendations, one of which actually endorses Baker's view that *ex post* FISA Court review could improve matters.

It is notable that the PCLOB Report splits down party lines. Two of the five PCLOB members (Beth Williams and Richard DiZinno) refused to sign the Report. These Republican members stop short of recommending a warrant requirement and insist that Section 702 should not be allowed to expire. Also, two of their three policy suggestions are aimed at reforming the structure, culture, compliance, and auditing of the FBI as the main administrator of Section 702 rather than changing querying procedures or the like. Williams and DeZinno also argue that reforms are necessary so that nothing like the spying on the Trump campaign that occurred in the 2016 election cycle could occur in the future.[34]

The PCLOB is an ostensibly "independent agency" including representation of both parties. Unsurprisingly then, another board tied to the Biden Administration in a non-independent fashion is an even stronger supporter of Section 702.

In a report issued by the President's Intelligence Advisory Board (PIAB), that board argued that "history may judge the lapse of Section 702 authorities as one of the worst intelligence failures of our time."[35] The PIAB opposes the imposition of a warrant requirement on FISA Section 702. Reflecting its lack of member balance, the PIAB reaches dubious conclusions, the worst of which is this: "Unfortunately, complacency, a lack of proper procedures, and the sheer volume of Section 702 activity led to FBI's inappropriate use of Section 702 authorities, specifically U.S. person queries. The

---

[33] PCLOB Report at 11.
[34] *Id.* at 18.
[35] President's Intelligence Advisory Board (PIAB) and Intelligence Oversight Board (IOB) Review of FISA Section 702 and Recommendations For Reauthorizationpresident's Intelligence Advisory Board (PIAB) and Intelligence Oversight Board (IOB) Review of Fisa Section 702 and Recommendations for Reauthorization at 2 (July 2023). Note that the PIAB claims a strange status; "The PIAB, and its component IOB, is an independent element comprised of volunteer citizens who operate within the Executive Office of the President. The PIAB has the authority to access all information it needs to perform its functions." Of course, any entity acting within and dependent on the Executive Office of the President is not an independent agency.

Board, however, found no evidence of willful misuse of these authorities by FBI for political purposes."[36]

The PIAB's assessment flies in the face of the alarming number of abuses known to have occurred through the use of these bulk data collection efforts. Further, the recent introduction of the Government Surveillance Reform Act[37] underscores that Section 702 reform is a bipartisan endeavor.

The bill, introduced by Sens. Ron Wyden (D-OR) and Mike Lee (R-UT) and Reps. Warren Davidson (R-OH) and Zoe Lofgren (D-CA), implements a number of reforms that include ending warrantless queries for U.S. citizens, limiting the use of Section 702 information, repealing the statutory authority for the "abouts" collection program, instituting a process for civil action against federal agencies that violate citizens' rights, and imposing accountability measures for federal agents and analysts that abuse the program.

If nothing else, the policies proposed in the Government Surveillance Reform Act reflect a healthy bipartisan understanding of the need to address Section 702 with urgency.

The Path Forward: Recommendations

The old idiom to avoid "throwing the baby out with the bathwater" is one that many prospective reformers of FISA often ascribe to their policy preferences. However, it is clear that the root of FISA's most recent abuses lies within the agencies tasked with carrying it out,the National Security Agency, the Federal Bureau of Investigation, and the Central Intelligence Agency. In particular, until the DOJ and FBI are sufficiently held accountable for their weaponized posture toward the American people—and there are numerous ways[38] in which such accountability can and should be pursued—Section 702 will remain a tool used to continually violate the rights of citizens notwithstanding whatever well-intentioned statutory restrictions that exist currently or be envisioned.

Therefore, policymakers should seek nothing less than to abolish Section 702, eliminate its secret courts, and disarm the weaponized surveillance state that the United States has created against its people. This must be the stated objective of Congress and all efforts should lead to this outcome.

---

[36] *Id.* at 1-2.

[37] Sabin, S. (November 7, 2023). "Lawmakers Unveil First Bill to Renew Controversial Surveillance Program," *Axios*. https://www.axios.com/2023/11/07/surveillance-fisa-section-702-renewal-legislation

[38] Clark, J. (May 17, 2023). "The U.S. Justice Department is Not Independent," *Center for Renewing America*. https://americarenewing.com/issues/the-u-s-justice-department-is-not-independent/.

Short of that worthy goal, policymakers should at least use the reauthorization opportunity to curtail FISA abuse, improve transparency and accountability, and lay the policy foundation for Section 702's eventual expiration through the following measures:

1. **Warrant Requirements:** Congress should require every agency that utilizes FISA to obtain a front-end warrant for criminal investigations or a FISA Court Title I order before accessing Section 702 data that implicates the private communications of U.S. persons.

2. **Prohibit Bulk Data Collection:** Congress should tie the hands of federal intelligence and law enforcement agencies so that they are unable to engage in bulk data collection against the American people through the Section 702 program, or any related program, authority, or effort.

3. **Civil Right of Action:** Congress should create an explicit civil right of action—against both the federal government and cooperative tech companies—for U.S. persons whose Fourth Amendment rights (or other constitutional or statutory rights) are violated through the improper use of Section 702 and similar surveillance authorities. The process should require the FISA Court to flag clear violations, force agencies to notify U.S. citizens that their rights were potentially violated, and provide an opportunity to file suit for damages against the offending agencies and/or tech companies. Additionally, because quantifying damages in many instances could be difficult, Congress should consider also providing, in connection with any new private right of action, that a) some defined civil penalty be paid out of the violating agency's budget into the U.S. Treasury (e.g., $10,000 per violation); and b) if liability is demonstrated, that damages be set at some minimum figure (e.g., $250,000 per violation). Congress should also consider providing a new private right of action that if an individual federal employee or officer engages in willing misconduct that creates or contributes to a FISA violation, such an employee shall pay to any American citizen who experiences harm as a result of such violation actual damages of at least $10,000 per violation.

4. **Internal Consequences:** Congress should mandate that agency heads implement new metrics that punish agents and analysts who frequently carry out non-compliant queries, even if they are unintended. These disciplinary actions should be reported to the relevant committees on at least an annual basis to help ensure a heightened level of professionalism and competence within the agencies.

5. **Criminal Penalties:** Congress should enact new criminal penalties (including the possibility of significant prison time) for agents and analysts who unlawfully use information collected pursuant to Section 702, as well as for any DOJ or FBI officials who make inaccurate certifications to the FISA Court.

6. **Annual Report and Audit:** Congress should require agencies that utilize Section 702 and similar authorities to, following the FISA Court's annual assessment, make public an annual, plain English report that includes the number of Americans targeted by FISA, the number of U.S. citizens suspected of having their rights violated by each agency, and the accountability imposed on the personnel involved.

7. **Enhanced FISA Court Transparency and Protections:** Congress should require that the FISA Court keep transcripts of all hearings (which shall be available for *in-camera* inspection by the House and Senate intelligence and judiciary committees) and appropriately document all substantive interactions between executive branch employees and the court. Congress should further direct the DOJ OIG to conduct regular audits of compliance with the Woods Procedures, and beef up the FISA Court's friend-of-the-court provisions through expanded access to information and guaranteed appointment of *amici* in cases targeting American citizens (or otherwise posing a heightened risk of privacy violations).

8. **Automatic Sunset:** Congress should craft a statutory trigger that requires all of FISA—not just Section VII—to be reauthorized every five years. This will increase the frequency and urgency of oversight.

Furthermore, the debate over Section 702's reauthorization provides a timely opportunity for Congress to fundamentally reform a weaponized FBI. Legislative, budgetary, and oversight priorities in furtherance of that objective should include—but are certainly not limited to—nixing the $4 billion proposed new FBI headquarters in the Beltway,[39] impeaching FBI Director Christopher Wray,[40] and slashing the agency's overall budget with targeted spending reductions in the Intelligence and Counterintelligence branches.[41]

---

[39] Carney, J. (May 25, 2023). "House GOP Floats Blocking FBI's New HQ," *Politico*. https://www.politico.com/news/2023/05/25/house-gop-fbi-funding-hq-00098863

[40] Gateway Pundit (October 2022). "Kash Patel Calls for Chris Wray's Immediate Impeachment Following Tuesday's Shocking News," Rumble.

https://rumble.com/v1nnjhe-kash-patel-calls-for-chris-wrays-immediate-impeachment-over-tuesdays-shocki.html

[41] " CRA Budget in Focus: Ending the Weaponization of the FBI," *Center for Renewing America*. https://americarenewing.com/issues/ending-the-weaponization-of-the-fbi-cra-budget-in-focus/

Accountability is critical for restoring the trust of the American people in federal law enforcement and intelligence agencies. The very last thing Congress should do is reward the weaponized bureaucracy with new taxpayer-funded benefits when such entities continue to wage war on the very people from whom their legitimacy derives.

Conclusion

As Congress considers the reauthorization of Title VII the Foreign Intelligence Surveillance Act, it is clear that the status quo will continue to threaten both the rights of American citizens and the domestic tranquility necessary for our republic to survive. Weaponized government poses an existential threat to our way of life and strikes at the very heart of the American idea that all men are created equal and endowed by their Creator with certain unalienable rights.

Congress must use this opportunity—at a minimum—to defang the security bureaucracy's hostilities toward the American people. For the moment, the people's elected representatives remain the first and best line of defense. In the event that strong policy reforms to Title VII, FISA, and the FBI cannot be properly effectuated to guarantee the protection of the American people and remain insufficient in the long run for securing the rights guaranteed under the U.S. Constitution, Section 702 should be scrapped altogether.