Written Statement
Jonathan Turley

Shapiro Professor of Public Interest Law
The George Washington University Law School

"*Fixing FISA, Part II*"

United States House of Representatives
Committee on the Judiciary
Subcommittee on Crime and Federal Government Surveillance

July 14, 2023

I. INTRODUCTION

Chairman Biggs, Ranking Member Lee, members of the Subcommittee, my name is Jonathan Turley, and I am a law professor at George Washington University, where I hold the J.B. and Maurice C. Shapiro Chair of Public Interest Law.[1] It is an honor to appear before you today to discuss the Foreign Intelligence Surveillance Act (FISA) and the reauthorization of Section 702. Given the limited time to prepare testimony for today's hearing, I would like to briefly outline a few areas where reforms are warranted before any reauthorization of Section 702.

As a threshold matter, Congress could clearly let Section 702 sunset and return the law to the position that existed before 2008. We are, once again, looking at a reauthorization after years of open defiance and violations by the government. Allowing the sunsetting of this provision would establish a clear deterrent for the agencies under an "abuse it, lose it" rationale. However, in the absence of such a decision, there are other areas worth exploring for needed reforms.

For background purposes, I come to this subject as a longtime critic of FISA. However, you will find considerable agreement among the witnesses today called by both parties. I have great respect for my co-panelists and I have benefited from speaking with them on this subject in the past. Despite the great political divisions today (and the rage of this age), this hearing is a rare opportunity for members of both parties to find common ground in the interest of the American people. Louis Brandeis famously described privacy as "the right to be let alone," an essential human component.[2] These warrantless searches discussed below threaten a host of rights including free speech, the free press, freedom of religion, and free association. Such surveillance creates a chilling effect on citizens exercising their rights, particularly free speech, when they are uncertain whether the government is collecting and storing their communications. In an upcoming book, I discuss how the federal government has historically used investigations to chill dissenting speech throughout our history.[3] We should not allow this history to repeat

---

[1] I appear today on my own behalf, and my views do not reflect those of my law school or the media organizations that feature my legal analysis.

[2] Olmstead v. United States, 277 U.S. 438, 478 (1928).

[3] JONATHAN TURLEY, THE INDISPENSABLE RIGHT: FREE SPEECH IN THE AGE OF RAGE (forthcoming 2024).

itself. If Congress is going to reauthorize Section 702, it should do so with substantive reforms in light of violations throughout the years by the FBI and other agencies.

II. FISA AND THE FALLACY OF GOVERNMENT SELF-REGULATION

My first encounter with FISA came during the Reagan Administration as a young law student working at the National Security Agency (NSA) as an intern. One particular memory stands out for me. After returning from my entry into the Foreign Intelligence Surveillance Court ("FISC"), I was asked what I thought of the court, and I said that it scared the daylights out of me due to the sweeping agency deference and minimal legal standards. My boss assured me that, while it can be unnerving, the key was that the NSA shared those concerns and showed great restraint in its duties. That was not an empty statement. What I saw at the NSA were professionals taking their duties to the Constitution seriously. However, we have always avoided relying on the good motivations or actions of government officials to protect our rights. Indeed, James Madison stressed in *Federalist 51* that good government could not be based on good intentions:

> "If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and, in the next place oblige it to control itself."[4]

FISA fulfills Madison's worst expectations, not only about the reliance on the good motivations of officials, but also the ability of the government to "control itself." The trust in the good intentions of officials has been repeatedly shown to be misplaced under FISA, including abuses by the CIA, NSA, and FBI. The use of FISA in the Carter Page investigation (which technically occurred under Title I of FISA) highlighted the lack of effective supervision and accountability in this process. The targeting of Page was based on flawed or false information. The FBI turned to FISA as an easy avenue for an investigation, so much that even FBI Director Christopher Wray admitted this week (in testimony before this Committee) that the investigation was driven by bias.

In 1967, the Court handed down the historic decision in *Katz v. United States*, which held that the Fourth Amendment protects "people, not places."[5] It was a paradigm shift from the artificial protections of the trespass doctrine under the prior precedent of *Olmstead v. United States*.[6] In 1968, the Congress went further to codify the Supreme Court holdings on the necessity of warrants for electronic surveillance in Title III of the Omnibus Crime Control and the Safe Streets Act of 1968.[7] However, it also acknowledged that the law was directed at protecting U.S. persons, not foreign intelligence targets. As will be discussed, the expansion of FISA searches has implicated areas where U.S. persons clearly have the "reasonable expectation

---

[4] THE FEDERALIST No. 51, at 322 (James Madison) (Clinton Rossiter ed., 1961).
[5] Katz v. United States, 389 U.S. 347 (1967).
[6] Olmstead v. United States, 277 U.S. 438, 458-66 (1928).
[7] Pub. L. No. 90-351, tit. III, 82 Stat. 197 (codified as amended at 18 U.S.C. §§2510-2522 (2013)); see generally Jonathan Turley, *The Not-So-Noble Lie: The Nonincorporation of State Consensual Surveillance Standards in Federal Court,* 79 J. OF CRIM. L. AND CRIMINOLOGY 66-134 (1988); Jonathan Turley, United States v. McNulty: *Title III and the Admissibility in Federal Court of Illegally Gathered State Evidence,* 80 NW. U. L. REV. 1714-52 (1986).

of privacy" that *Katz* sought to protect. Indeed, the acquisition of data from sources like the cloud has once again allowed for intrusions based on location criteria.[8] Likewise, if a target is abroad, privacy rights can be lost due to the location of the surveillance.

Four years later, the Supreme Court recognized a national security exception in *United States v. U.S. District Court* (Keith).[9] The Court found that a warrantless national security wiretap conducted in the United States was unconstitutional. However, it then reserved the question of a national security exception, stating that it "expressed no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."[10] The then-current Nixon Administration continued to argue that national security rationales offered a sweeping exception to any warrant or statutory requirements, even with regard to domestic surveillance. Conversely, civil libertarians noted that the text of the Fourth Amendment offers no such exception.

In 1978, this long conflict between the legislative and executive branches came to a head with FISA, which created FISC and a process of judicial review that, while using the term probable cause, was not the same standard as the Fourth Amendment standard. However, Congress sought to maintain protections for U.S. persons in a myriad of ways. For example, Congress defined being an "agent of a foreign power" differently for U.S. persons than it did for foreigners to maintain privacy protections.[11] The government must establish a nexus between a U.S. person and criminal conduct, including espionage and terrorism. Yet, the blind spot was surveillance occurring outside of the country. "Electronic surveillance" is defined as surveillance of a communication "to or from a person in the United States." Thus, communications abroad are not subject to the limitations. As a result, a U.S. person could still be subject to surveillance through operations abroad.

Despite the ample authority given to the government, there was a demand for further powers after September 11th. The law still required that communications with a person in the United States were subject to the statutory warrant requirement. That became an issue in 2001 after the 9/11 attack when President George W. Bush authorized the Terrorist Surveillance Program (TSP) by executive order, permitting the NSA to intercept communications from al-Qaeda members to individuals within the United States.[12] That classified executive order was found unlawful by a district court in *ACLU v. NSA*,[13] which was later vacated on different grounds.[14]

Congress stepped in to remove the obstacle to the government involved in *ACLU v. NSA*. The FISA Amendment Act of 2008 (FAA) created Section 702, but still required compliance with the Fourth Amendment.[15] The FAA allowed for the interception of "persons reasonably believed to be located outside the United States" with virtually no limits. It does not require that

---

[8] United States House of Representatives, House Judiciary Committee, "*Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power*" June 30, 2021 (testimony of Professor Jonathan Turley).

[9] United States v. U.S. Dist. Court (Keith), 407 U.S. 297, 303-04 (1972).

[10] *Id*. at 321-22.

[11] 50 U.S.C. § 1801(b)(2).

[12] OFF. INSPECTORS GEN., DEP'T OF DEFENSE, DEP'T OF JUSTICE, CENTRAL INTELLIGENCE AGENCY, NAT'L SEC. AGENCY & OFF. DIR. NAT'L INTELLIGENCE, REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM (2009)

[13] ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006), vacated, 493 F.3d 644 (6th Cir. 2007).

[14] ACLU v. NSA, 493 F.3d 644, 688 (6th Cir. 2007).

[15] Pub. L. 110-261 (2008).

the government establish a nexus between the target and a foreign power, intelligence organization, or terrorist groups. This means that a person in the United States could be a party to interceptions or collections so long as they are not the intended target. The federal agencies poured into the opening left by the FAA. Such gathering can involve what is called "upstream collection" where the government taps into communications linked to foreign figures on the Internet coming into or going out of the country. It also involves so called PRISM collection where the government uses selectors like emails to secure information from service providers. The result is a massive gathering of communications which are then stored in databanks and made available to a variety of agencies.[16] Congress, however, foresaw the inherent dangers in such collection and required minimization of acquired material[17] and annual certification that there is no "reverse targeting" under Section 702 to surveil or intercept U.S. persons.[18]

The FAA protections were quickly rendered more aspirational than actual for U.S. persons subject to these operations. With the lower standard under FISA, prosecutors will follow the path of least resistance if they can use the secret court rather than a conventional court for surveillance. FISC has proven little more than a speed bump for these applications with few declinations in its history due to the low standard imposed on the government. Even concerning the controversial Section 702, FISC declared that "the Court is not required, in the course of this Section 702(i) review, to reach beyond the Government's procedures and conduct a facial review of the constitutionality of the statute."[19]

III. REFORMING FISA: RESTORING PRIVACY GUARDRAILS AND GUARDIANS IN NATIONAL SECURITY SURVEILLANCE

There remain serious questions over the constitutionality of FISA and its insular provisions. However, that may be a debate for another day. Likewise, those of us who would welcome the reconstruction of the wall in FISA are clearly in the minority and, absent a long overdue Supreme Court review, it is not likely to change. The courts have been clear that the Fourth Amendment does not apply to searches conducted abroad, even for U.S. citizens.[20] (However, Title VII does afford the protection of targeted citizens abroad).[21] Even accepting those positions, this reauthorization allows Congress the opportunity to make meaningful changes that we should all be able to agree on. Among the viable options is one that allows Section 702 to sunset at the end of this year in light of the gross and systemic violations by the government. However, no reauthorization should occur without real reforms based on the principle that U.S. persons should not be subject to surveillance without a warrant or judicial order. That principle then leads to equally obvious supporting protections, including prohibitions against backdoor searches or other circumventions. Finally, there must be a new and reliable system of mandatory disclosures on the number, means, and minimization of interceptions. It is my sincere hope that, while we may have disagreements on the overall constitutionality of FISA

[16] See generally PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 36-41 (2014).
[17] 50 U.S.C. § 1881a.
[18] 50 U.S.C. § 1881a(b)(2), (h)(2)(A)(iii).
[19] In re Proceedings Required by 702(i) of FISA Amendments Act of 2008, No. 08-01, 2008 WL 9487946, at 4-5 (FISA Ct. Aug. 27, 2008).
[20] United States v. Verdugo-Urquidez, 494 U.S. 259, 274 (1990).
[21] § 1881c(a)(2).

as it relates to domestic surveillance, there should be common ground in dealing with the much abused 702 provision.

Before 2008, FISA was criticized for its easily satisfied standards for surveillance. Yet, it still mandated applications for interceptions or collections. That changed in 2008 when Congress created Section 702 and eliminated that threshold requirement for surveillance ostensibly conducted outside of the country. Congress considered bills that year that would have mandated court orders, but members were assured that no such added protection was needed.[22] The problem is that the provision created a new and even greater avenue for acquiring material through "backdoor" or "reverse targeting" means. Government power operates like a gas in a closed space. If you expand the space, the gas will fill it and seek out any crack. Section 702 was not just a crack, but a virtual open door for government abuse. While Title I requires a FISC order to target a U.S. person domestically (or the government can secure a conventional warrant), the privacy of covered persons can be compromised on a huge scale through Section 702 investigations where their communications were "incidental" to searches on a foreign target. Moreover, despite minimization requirements, this material is widely shared among the agencies and kept for five years before deletion.

Title VII of FISA has other provisions under sections 703 and 704 that address surveillance of U.S. persons abroad. However, Section 702 has long been the greatest concern. It is the path of least resistance for officials. Since it focuses on non-U.S. persons, it has the least protections. Rather than face the necessity of an application to FISC based on probable cause showings for individual targets, Section 702 left targeting to the discretion of the Attorney General and Director of National Intelligence (DNI). It is based on the view that a foreign person abroad is not a person covered under the Fourth Amendment. In 2021 alone, almost a quarter of a million persons were targeted under Section 702. FISC reviews the procedures used by the government in what the Second Circuit described as "a form of programmatic pre-clearance."[23] Those procedures leave it to the very agency to review its own requests. Thus, for example, NSA queries are approved by the NSA General Counsel who simply signs off that the queries are "reasonably likely to retrieve foreign intelligence information."[24]

For civil libertarians, addressing FISA violations has been a virtual game of whack-a-mole, where getting Congress to address one abuse only leads to another popping up to achieve that same result. FISC has identified widespread interception of protected persons through "about" searches where an identifier (like an email address) is included in the communication.[25] Thousands of U.S. persons were intercepted in domestic communication through "about" searches. Nevertheless, FISC ruled that the law did not bar such operations since, while the NSA knew it was acquiring communications of U.S. persons, it did not know that origin of the information before the interception or collection. The NSA ultimately pledged to halt the practice and Congress statutorily banned the resumption of the practice.

The FBI has repeatedly pledged and reneged on pledges of compliance. For example, Congress correctly demanded that the FBI document the number of queries in 2018 that might show "backdoor" searches of U.S. persons. The FBI spent two years avoiding such reporting

---

[22] USA Rights Act, S. 1997, [11]5th Cong. § 2 (2017); USA Liberty Act of 2017, S. 2158, [11]5th Cong. § 101(a)(2) (2017).

[23] United States v. Hasbajrami, 945 F.3d 641, 652 (2d Cir. 2019).

[24] *NSA Querying Procedures* § IV.A; see generally Edward C. Liu, Reauthorization of Title VII of the Foreign Intelligence Surveillance Act, Mar. 17, 2023.

[25] Redacted, 2011 WL 10945618, at *15 (FISA Ct. Oct. 3, 2011).

through transparently bad faith arguments, and FISC had to intervene to order such reporting. It was not until four years later that the government revealed the massive number of queries involving U.S. persons.

The violations of the FBI are particularly chilling because the standard is so low. The government only has to show a reasonable basis to believe that a search will yield foreign intelligence or evidence of a crime. That practically reduces the barrier to highly intrusive searches to the fleeting burden of a *Terry* stop. None of this makes sense. Congress created Sections 703 and 704 to guarantee that queries targeting U.S. persons abroad would still be subject to a court order. It is important to keep in mind that both sections lower the already low standard of Title I for U.S. persons (which is lower than the standard of a warrant under the Fourth Amendment). Rather than simply require the same showing for any targeting of a U.S. person (as was the case under the original FISA system), these sections allow a step down in protections once a citizen steps across the border. Section 703 deals with electronic surveillance or the storage of such surveillance. Section 704 is a catchall provision for other sources of information. Yet, because Section 704 has the lowest standard, Congress stated that, when both apply, it wanted the more stringent Section 703 to be followed. That includes the minimization requirements of acquired material under Section 703. Neither of those sections require the showing under Title I that the target is linked to international terrorism or clandestine intelligence activities.

The government is now back in Congress, making the same assurances that it will follow not just the letter but also the spirit of this law. According to FISC, "the individuals whose identifiers were used as query terms included multiple current and former United States Government officials, journalists, and political commentators." Nothing could be more serious to a democracy than the circumvention of both the Fourth Amendment and federal law to conduct sweeping investigations or inquiries targeting reporters, political advocates, or members of Congress.

If Congress is moving toward reforms rather than the sunsetting of Section 702, there are a number of areas where legislation would be warranted to address the past abuses of the FBI and other agencies.

Closing Backdoor Searches. The long-standing failures under FISA have been due to the level of control afforded to the government, which has repeatedly shown itself incapable of self-policing. For example, intelligence agencies like the NSA now regularly share intercepted material with other agencies like the FBI. The government has allowed for a massive bulk collection bank of evidence acquired below the constitutional standard. In 2021, there were an estimated 3.4 million warrantless searches conducted under Second 702.[26] While that number has been contested due to possible overcounting or duplicative searches, the roughly quarter of million confirmed searches should be ample basis for congressional action. It is no longer plausible to deny the violations. FISC itself has found that the FBI systematically evaded statutory requirements and used FISA material as a casual option for searching the backgrounds of possible sources and even repair personnel.[27] Most queries are occurring as an "assessment" stage before a criminal predicate determination is made and an order must be sought.[28] Even with

[26] Statistical Transparency Report, CY2021, Office of the Director of National Intelligence at 21 (Fig. 9).
[27] Boasberg 2018 Opinion at 72-74.
[28] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 59 (2014)

recent changes, the FBI is still reporting roughly 200,000 U.S. person queries under Section 702.[29]

Section 702 currently bars its use for "the purpose" of surveillance of a U.S. person. To avoid further misconstruction of federal law, Congress should expressly state that it cannot be used for "a purpose" of targeting U.S. person even if it is one of multiple purposes behind a search. Otherwise, any interception is still purposeful and not incidental.

If Section 702 is reauthorized, Congress can also close much of the backdoor searches by making the standards consistent for any searches of U.S. persons. Under Title I, an agency must show probable cause that the subject is an "agent of a foreign power," which is defined:

> **"(A)** knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
> **(B)** pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
> **(C)** knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
> **(D)** knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
> **(E)** knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C)."[30]

Given the virtual uniform approval of such applications by FISC with few rejections, it is not clear why such a showing would be burdensome for the agencies. More importantly, it would require officials to sign off on these representations to FISC. These queries are separate governmental acts that should meet their own showing of support and need. Requiring such orders would also address the artificial distinctions between information that is addressed as part of a domestic source as opposed to a foreign source when information is now stored or routed throughout the world by transnational corporations. All agencies should have to obtain a judicial order for U.S. person queries under Section 702 regardless of whether it is justified as part of a foreign intelligence operation or criminal investigation. Otherwise, we will see a repeat of the rationalization used in controversies like the investigation of protesters after the George Floyd murder as based on a "reasonable" belief that it could render "foreign intelligence."[31]

Finally, a direct bar on the search of such information of U.S. persons without a court order would counter the use of E.O. 12333. Indeed, it is still not clear how much surveillance is occurring outside of FISA. Congress needs to establish the scope of any searches conducted pursuant to the executive order and, if necessary, to curtail such searches outside of the Act. That

---

[29] OFF. DIR. NAT'L INTELLIGENCE, ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES: CALENDAR YEAR 2022 at 20 (Apr. 2023) .

[30] 50 U.S.C.A § 1801 (2020) (emphasis added).

[31] [Redacted], at 27 (FISA Ct. Apr. 21, 2022), *available* at https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opini on.pdf.

includes bars on the storage of such material generated by searches under E.O. 12333 or alternative means. Otherwise, closing off the backdoor searches under Section 702 will only result in the "gas" described earlier finding this alternative point of release.

Congress should also expressly bar "parallel construction," where the government is given access to evidence through FISA and then re-acquires the known evidence through a second investigation to hide its source. While FBI Director Wray denied knowing what parallel construction means in his testimony before this Committee this week, it has long been a complaint of civil libertarians and defense counsel. It avoids "poisonous tree" problems by replanting the seeds of the evidence to claim independent acquisition. It hides the true origins of evidence from courts and in some cases, Congress. While defendants are supposed to receive notice of Section 702 evidence, parallel construction can be used to evade that obligation. Indeed, there have been only five notices issued to counsel.[32] This practice needs to be statutorily barred and there needs to be a required certification of compliance.

Commercially Available Information. Congress should also address another circumvention used by the agencies in the purchase of information that it cannot gather directly without a warrant or court order. This includes purchases of commercially available information (CAI) by the Defense Department, FBI, DEA, and Homeland Security of locational information on citizens.[33] The use of CAI has long been a point of contention between the government and civil libertarians.

While *Katz* protects the reasonable expectation of privacy, the Court created a loophole for information shared with third parties in cases like *United States* v. *Miller*[34] (financial records held by a bank) and *Smith* v. *Maryland*[35] (telephone numbers conveyed to telephone company). However, five years ago, in *United States v. Carpenter,*[36] the Court held that obtaining cellphone locational information from carriers is a violation of the Fourth Amendment without a warrant. The Court not only found a reasonable expectation of privacy, but also noted that such retroactive productions allow for:

> "access to a category of information otherwise unknowable…the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone."[37]

We now know that the government avoided any need for a warrant by simply going to data brokers to buy the information. Notably, this information allows the same pattern information "otherwise unknowable" to the government, discussed in *Carpenter*. I previously discussed this problem by suggesting legislative solutions to the growing biometric industry, including data

---

[32] United States v. Muhtorov, No. 12-cr-00033 (D. Colo.); United States v. Mohamud, No. 10-cr-00475 (D. Or.); United States v. Hasbajrami, No. 11-cr-00623 (E.D.N.Y.); United States v. Khan, No. 12-cr-00659 (D. Or.); United States v. Mihalik, No. 11-cr-0833 (S.D. Cal.).

[33] Elizabeth Goitein, *The Government Can't Seize Your Digital Data*, WASH. POST, Apr. 26, 2021, https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/.

[34] 425 U.S. 435 (1976).

[35] 442 U.S. 735 (1979).

[36] 138 S. Ct. 2206 (2018).

[37] *Id* at 2218.

banks.[38] This is an area that requires a comprehensive examination given the changes in technology in 1986 and the enactment of the Electronic Communications Privacy Act (ECPA). Digital data providers are largely unchecked and unmonitored in this work.

The use of purchased data creates other collateral problems. As lead defense counsel in espionage and terrorism cases, I have worked as the cleared lead attorney handling classified and FISA material. Mixing such material in FISA applications or classified material tends to create additional barriers for access in court proceedings. I have often found that redacted material available in SCIFs contain unclassified material previously withheld from counsel that was mixed in with classified material. Thus, if purchased data is used in later FISA applications, it can be insulated from conventional review in criminal cases or delayed in production. CAI clearly raises difficult issues, but Congress has to address the use of CAI to circumvent constitutional and statutory protections.

Minimization. The consistent failure of FISA to protect the privacy of U.S. persons has been due to the dependence on the good-faith actions of officials. The Act is riddled with ambiguous terms that have been routinely disregarded. For example, FISA mandates that the government "minimize" interception of citizens, but offers little real review of the performance of that obligation. Agencies are simply required to adopt minimization procedures "that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[39] There is also a specific allowance for the retention of possible criminal conduct.[40]

When these minimization procedures were subject to limited review by FISC, the government "materially misrepresented" the scope of its data and collection records.[41] The law is designed to stop "reverse targeting" of citizens, but clearly allows the practice to be used. The Act permits the government to seek the sharing of FISA information with criminal investigators with a simple motion to FISC. That access could have been sought in at least 100 cases, but has failed to do so.[42] Even that number of cases was artificially low because the 2018 requirement only requires a showing of probable cause and a court order in "predicated" cases involving U.S. persons. The FBI searches generally occur as "assessments" before the predication stage and thus evade the protection. However, even when there was a predicated basis, the FBI still appears to have ignored its statutory obligations. The agencies are maxing out the five-year period for retention of data, allowing for massive searches involving U.S. persons without an order. The five-year-period is itself illusory. It can be extended with the certification of a high-ranking official and does not apply to certain type of information like encrypted communications or material with linkage to criminal or foreign intelligence operations. Agencies like the NSA interpret that exception so broadly as to swallow the rule – allowing retention of information that could be valuable in future investigations.[43]

---

[38] Jonathan Turley, *Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics*, 100 B.U. L. REV. 2179 (2020).
[39] 50 U.S.C. § 1801(h)(1).
[40] 50 U.S.C. § 1801(h)(3).
[41] [REDACTED], FISA Ct. Sep. 25, 2012, at 2.
[42] [REDACTED], FISA Ct. Oct. 18, 2018, at 68-69 & 80
[43] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 62 (2014).

There should be a tightening of minimization procedures, including material gathered under Section 702, to require removal of incidental and overbroad collections impacting U.S. persons. Likewise, the broad interpretations of agencies like the NSA need to be statutorily curtailed to avoid hoarding of material that would otherwise be purged under minimization rules. The misconstruction of the minimization provisions undermines the constitutional status of FISA overall. As FSIC held in 2011, "the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."[44]

Special Advocates. FISA needs advocates for privacy rights. One of the oldest offices at the Vatican was the *advocatus diaboli* or Devil's Advocate. The official holding this office, created in 1587, had the responsibility to challenge calls for canonization of a possible saint to guarantee that all of the facts are considered before making a final decision. It was an unenviable position to argue against the a*dvocatus Dei*, or "God's advocate." However, that "promoter of faith" could make too great a leap of faith over countervailing facts. The same danger of blind faith has been evident in the FISA process where the FBI fails to properly investigate matters (as with Carter Page) or FISA judges sign off on abusive searches without the benefit of an opposing view. Notably, when controversies have forced a retroactive review, serious errors were found that were not identified under the current system (even with the allowance for amicus appointments). The Inspector General's review FISA 29 applications under Title I found that 25 of the 29 applications contained "apparent errors or inadequately supported facts."[45]

These violations have occurred because there is little danger of exposure or accountability. That is due in part to the lack of ability of possible targets to challenge surveillance in court due to narrow standing rulings in cases like *Clapper v. Amnesty International*.[46] Congress can explore avenues for improving the ability for litigants to meet those standing requirements. However, a special advocate can also serve to create this type of review with the FISA system.

Congress has long recognized the need for some opposing counsel or analysis in this process. To that end, in 2015, Congress amended FISA to allow the appointment of five individuals to serve as amici curiae as part of the USA FREEDOM ACT. That Act allows the use of amici appointments to help courts address any "novel or significant interpretation of the law." The authority to appoint amici was an important advance under FISA where courts had no independent or adversarial input into applications. However, the appointment was still discretionary and less than three dozen appointments have been made. No such appointments are known to have been made on individual applications. What is needed are special advocates who can regularly review applications and have the authority to raise an appeal to the Foreign Intelligence Surveillance Court of Review (FISCR). Similarly, there should be a mandatory review system for stored data and queries made under Section 702, if it is reauthorized. If we are to maintain a secret court in this country, the public should be assured that there are advocates not just for their security but their privacy under FISA.

---

[44] [Redacted], 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011); see also United States v. Hasbajrami, 945 F.3d 641, 669-73 (2d Cir. 2019)

[45] *See* OFF. INSPECTOR GEN., DEP'T OF JUSTICE, MANAGEMENT ADVISORY MEMORANDUM FOR THE DIRECTOR OF THE FBI REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FISC RELATING TO U.S. PERSONS 3 (Mar. 2020)

[46] 568 U.S. 398 (2013).

IV. CONCLUSION

Congress has an opportunity in these hearings to show that people of good faith can put aside political differences and have a civil and substantive discussions to protect our shared values. The witnesses today demonstrate that broad coalition to rein in the federal agencies after years of open defiance of both the law and Congress. This can be done without any loss to our national security.

Once again, thank you for the honor of appearing before you to discuss these important issues. I am happy to answer any questions from the Committee.[47]

Jonathan Turley
J.B. & Maurice C. Shapiro Chair of Public Interest Law
George Washington University

[47] I have been asked to supply a biographical statement. For three decades, I have litigated FISA and surveillance cases in the national security area, including espionage and terrorism cases. This includes the *Al-Arian* and *Al-Timimi* terrorism cases as well as the *King* espionage case. I have also testified on FISA and surveillance issues, including before the House and Senate Intelligence Committee.[47] United States Senate, Committee on the Judiciary, **"***Examining the 'Metastasizing' Domestic Terrorism Threat After the Buffalo Attack,"* June 7, 2022 (testimony of Professor Jonathan Turley); United States House of Representatives, House Judiciary Committee (Democratic members), United States House of Representatives, House Judiciary Committee, "*Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power*" June 30, 2021 (testimony of Professor Jonathan Turley); United States House of Representatives, House Committee on Science, Space, and Technology, "*Affirming Congress' Constitutional Oversight Responsibilities: Subpoena Authority and Recourse for Failure to Comply with Lawfully Issued Subpoenas*," September 14, 2016 (testimony of Professor Jonathan Turley); United States House of Representatives, Permanent Select Committee on Intelligence, The Media and The Publication of Classified Information, May 26, 2006 (Professor Jonathan Turley); "The Constitutionality of NSA Domestic Surveillance Operation," January 20, 2006 (testimony of Professor Jonathan Turley); United States Senate, Senate Judiciary Committee, Subcommittee on Terrorism, Technology, and Homeland Security, September 13, 2004. (Testimony of Professor Jonathan Turley); United States Senate, Select Committee on Intelligence (closed classified hearing), "The Prosecution and Investigation of the King Espionage Case," April 3, 2001 (testimony of Professor Jonathan Turley). I have also taught constitutional law, constitutional criminal procedure and written both in both the academic and popular press on related privacy, national security, FISA, and surveillance issues. See generally, Jonathan Turley, Anonymity, Obscurity, and Technology: Reconsidering Privacy in the Age of Biometrics 100 Boston University Law Review 2179 (2020); Jonathan Turley, The Not-So-Noble Lie: The Nonincorporation of State Consensual Surveillance Standards in Federal Court, 79 Journal of Criminal Law and Criminology 66-134 (1988); Jonathan Turley, *United States v. McNulty: Title III and the Admissibility in Federal Court of Illegally Gathered State Evidence,* 80 Northwestern University Law Review 1714-52 (1986).