Cite as George W. Croner, 14 J. NAT'L SECURITY L. & POL'Y xx (forthcoming 2023)

FISA SECTION 702'S CHALLENGING PASSAGE TO REAUTHORIZATION IN 2023

George W. Croner*

Congressional authorization of section 702 (Section 702) of the Foreign Intelligence Surveillance Act (FISA) expires on December 31, 2023. [1] This particular section in Title VII of FISA, rather opaquely titled "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons," represents one of the most significant intelligence collection authorities available to the U.S. Intelligence community.[2] However, since its inception, the legal structure, scope, and intrusiveness of Section 702 have been perceived by critics as posing a serious threat to the privacy rights and civil liberties of both Americans and foreigners alike. This article examines the history, structure, and legal requirements of the Section 702 surveillance program, assesses those legal requirements in the context of the standards of the Fourth Amendment to the U.S. Constitution, and explores the legal, political, and practical issues making the 2023 reauthorization of Section 702 particularly challenging.

THE JUDICIAL AND LEGISLATIVE PRECURSORS LEADING TO FISA

The Fourth Amendment is neither verbose nor arcane. Totaling fifty-four words, its stated purpose is to keep "the people secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[3] Despite the Amendment's requirement that warrants issue only upon a finding of probable cause, the warrantless use of electronic surveillance in internal

* George W. Croner is a Senior Fellow in the Program on National Security at the Foreign Policy Research Institute and serves on the Advisory Council to the Center for Ethics and the Rule of Law (CERL) at the University of Pennsylvania. He is a former principal litigation counsel in the Office of General Counsel at the National Security Agency, a 1975 graduate (with distinction) of the U.S. Naval Academy, and a 1980 graduate (with honors) of the University of Pennsylvania Law School.

[1] 50 U.S.C. § 1881a (referred to throughout this article as "Section 702")."
[2] *See* George Croner, *The Clock is Ticking: Why Congress Needs to Renew America's Most Important Intelligence Collection Program*, 23 INTELLIGENCER: J. U.S. INTELL. STUD., no. 2, 2017, at 7, https://perma.cc/P6QJ-DVR9 (describing the operation of the Section 702 collection program and the value of the intelligence it produces).
[3] U.S. CONST. amend. IV.

security cases was "sanctioned more or less continuously by various Presidents and Attorneys General since July 1946"[4] predicated upon the president's "fundamental duty to preserve, protect and defend the Constitution of the United States" which implicitly included the duty "to protect the government against those who would subvert or overthrow it by unlawful means."[5]

The 1960s witnessed a significant evolution in the U.S. Supreme Court's Fourth Amendment jurisprudence as the Court grappled with rapid changes in developing communications technology and a corresponding expansion in the scope and intrusiveness of the government's use of electronic surveillance for law enforcement purposes. In two decisions issued in 1967, the Court required new procedural safeguards governing the government's use of electronic surveillance[6] while simultaneously abandoning the physical trespass to property that the Court had viewed as a Fourth Amendment prerequisite[7] in favor of a more expansive standard. The new paradigm shifted the Amendment's focus from physical trespass to whether the government had abridged or invaded a matter or area in which an individual had a "reasonable expectation of privacy"—including conversations intended to be private.[8]

Congress responded to the *Berger* and *Katz* decisions by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[9] Title III established procedural standards for the issuance of a warrant authorizing electronic surveillance and confined the use of such warrants to a specific limited group of crimes. Simultaneously, Title III disclaimed any congressional purpose directed to limiting the constitutional power of the president to protect national security, to obtain essential foreign intelligence information, and to take such measures

[4] United States v. U.S. District Court (*Keith*), 407 U.S. 297, 310 n.10 (1972).
[5] *Id.* at 310.
[6] Berger v. New York, 388 U.S. 41, 53-64 (1967).
[7] Olmstead v. United States, 277 U.S. 438, 464-85 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).
[8] Katz v. United States, 389 U.S. 347, 360-62 (1967) (Harlan, J., concurring).
[9] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801-02, 82 Stat. 197, 211-25 (1968).

as necessary to prevent the overthrow of the government by force or other means.[10] Title III also did not address a question reserved in the Court's *Katz* decision: whether safeguards other than prior judicial authorization would satisfy the Fourth Amendment in a situation involving the national security.[11]

In 1972, in *Keith,* the Supreme Court broached the question reserved in *Katz* in the context of Attorney General-authorized warrantless electronic surveillance of a U.S. citizen accused of bombing a Central Intelligence Agency (CIA) office building. [12] The Court concluded electronic surveillance in domestic security matters must comply with Title III standards requiring a warrant issued only after prior review by a neutral judicial officer, but the Court specifically declined to address the scope of the president's authority to authorize electronic surveillance in matters relating "to the issues which may be involved with respect to activities of foreign powers or their agents."[13] *Keith* represents the first judicially imposed limitation on executive discretion in the conduct of electronic surveillance arguably related to national security.

Following the *Keith* decision in 1972, subsequent congressional investigations in the 1970s into U.S. intelligence activities, conducted principally through the inquiries of the "Pike Committee" in the House of Representatives and the "Church Committee" in the Senate, led to further calls for controls over executive discretion in the conduct of intelligence activities.[14] Two collection programs conducted by the National Security Agency (NSA), Project Shamrock and Project Minaret, were revealed as involving the acquisition of the communications of U.S.

[10] *Keith*, 407 U.S. at 302-03.
[11] *Katz*, 389 U.S. at 358 n.23.
[12] *Keith*, 407 U.S. at 302-03.
[13] *Katz*, 389 U.S. at 322.
[14] *See* S. REP. NO. 94-755 (1976); H.R. Res. 591, 94th Cong. (1975).

persons without warrants or any judicial oversight. Largely in response to the exposure of the Shamrock and Minaret programs and other disclosed abuses of electronic surveillance ostensibly conducted for foreign intelligence or counterintelligence purposes, and with the *Keith* court's expressed view that judicial approval for domestic security surveillances might be "made in accordance with such reasonable standards as the Congress may prescribe,"[15] Congress passed FISA to provide a specific statutory framework incorporating judicial oversight for the conduct of electronic surveillance in the United States for foreign intelligence and counterintelligence purposes. FISA represents part of the "grand bargain" reached after the congressional hearings into intelligence activities in the 1970s whereby the intelligence community was allowed to continue to surveil domestically in the homeland but became subject to robust legal restrictions on the collection, analysis, and dissemination of intelligence information; strict reporting requirements to Congress; intra-executive monitoring by lawyers and inspectors general; and judicial oversight.[16]

Subject to certain prescribed statutory exceptions, FISA is "the exclusive means by which electronic surveillance and the interception of domestic wire, oral or electronic communications may be conducted."[17] Within FISA, "electronic surveillance" is a defined term requiring the acquisition of the contents of a wire or radio communication by the use of an electronic, mechanical, or other surveillance device.[18] As originally enacted in 1978, FISA's scope embraced the conduct of electronic surveillance for foreign intelligence purposes within the United States mandating that (with certain exceptions) such surveillance be conducted only

[15] *Katz*, 389 U.S. at 324.
[16] Jack Goldsmith, *The Dangers in the Trump-Brennan Confrontation*, LAWFARE (Aug. 20, 2018, 9:01 AM), https://perma.cc/23YC-3EU3.
[17] 50 U.S.C. § 1812.
[18] *Id.* § 1801(f).

pursuant to an order from the Foreign Intelligence Surveillance Court (FISC) issued only after findings by the FISC of probable cause to believe (1) that the target of the surveillance is a foreign power or an agent of a foreign power and (2) each of the facilities at which the surveillance is directed is being used or about to be used by a foreign power or an agent of a foreign power.[19] In terms of these substantive legal standards governing the conduct of electronic surveillance for foreign intelligence purposes in the United States, FISA remained largely unchanged until modifications implemented through the Patriot Act following the 9/11 attacks.

STELLAR WIND AND THE PATH TO THE FISA AMENDMENTS ACT OF 2008

Following the coordinated attacks directed at New York, the Pentagon, and Washington, D.C. on September 11, 2001, President George W. Bush declared a national emergency "by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States."[20] The "continuing and immediate threat of further attacks" prompted the President to direct the Secretary of Defense to use the capabilities of the Department of Defense and, more particularly, the signals intelligence capabilities of NSA to initiate an electronic surveillance program designed to counter the threat of further al Qaeda attacks in the United States.[21]

The codeword-level classified electronic surveillance program that grew from this presidential authorization was the component of the President's Surveillance Program (PSP) known as *Stellar Wind*[22] that provided the authority under which NSA began the warrantless

[19] *Id.* § 1805(a)(2).
[20] Proclamation No. 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001).
[21] U.S. DEP'T OF JUST. OFF. OF THE INSPECTOR GEN. OVERSIGHT & REV. DIV., A REVIEW OF THE DEPARTMENT OF JUSTICE'S INVOLVEMENT WITH THE PRESIDENT'S SURVEILLANCE PROGRAM (VOL. I) 7 (2009) [hereinafter DOJ Oversight I].
[22] *Id.* at 1 nn.1-2. *Stellar Wind* was the "cover term" given to NSA collection activities constituting part of the President's Surveillance Program. In Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008, the President's Surveillance Program is defined as "the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001 and ending on January 17, 2007,

targeted collection in the United States of international communications involving suspected terrorists.[23] From October 2001 through January 2007,[24] pursuant to 43 separate presidential authorizations issued under the PSP[25] but without a single order from the FISC, NSA conducted warrantless acquisition of (1) content from communications (including but not limited to a wire communication carried into or out of the United States by cable) where there was probable cause (as determined by the executive branch without any judicial involvement) to believe that a party to such a communication was a group engaged in international terrorism, and (2) metadata (header/router/addressing-type information, including telecommunications dialing-type data, but not the contents of the communication) with at least one party to such communication outside the United States or where no party to the communication was known to be a citizen of the United States. [26]

According to its advocates, *Stellar Wind* was needed to fill an "intelligence gap" created by the existing requirement to obtain a FISC order to collect international communications with a communicant in the United States. At that time, NSA's then-Director, General Michael Hayden, expressed the view that NSA could not address this intelligence gap using FISA because the process for obtaining FISC orders was "too slow" and required "extensive coordination" by multiple agencies.[27]

---

including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program)." *Id.* at 2 n.3.

[23] *Id.* at 8.

[24] U.S. DEP'T OF JUST. OFF. OF THE INSPECTOR GEN. OVERSIGHT & REV. DIV., A REVIEW OF THE DEPARTMENT OF JUSTICE'S INVOLVEMENT WITH THE PRESIDENT'S SURVEILLANCE PROGRAM (VOL. II) 73 (2009), [hereinafter DOJ Oversight II]; *see also* PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 5 (2014), https://perma.cc/8BJH-E7MY [hereinafter PCLOB Report] ("Section 702 has its roots in the President's Surveillance Program developed in the immediate aftermath of the September 11th attacks.").

[25] DOJ Oversight II, *supra* note 24, at 161.

[26] DOJ Oversight I, *supra* note 21, at 7-8.

[27] *Id.* at 6.

On December 16, 2005, *The New York Times* published the first public disclosures reporting on NSA's *Stellar Wind* surveillance activities,[28] and shortly thereafter, the government began efforts to secure approval of *Stellar Wind* collection from the FISC pursuant to the existing provisions of FISA. This effort proved cumbersome, and the Bush Administration continued to argue for legislation that would address the perceived "intelligence gap" and provide a more flexible statutory approach to the collection of international communications having at least one non-U.S. person communicant located outside the United States.[29]

The disclosures in *The New York Times* and the outcome of the 2006 election in which Democrats gained a majority in Congress brought considerable scrutiny to NSA's *Stellar Wind* surveillance activities. Continued concerns regarding the "intelligence gap" in a persisting high terrorist threat environment prompted Congress to pass the *Protect American Act* (PAA) in August 2007.[30] The PAA afforded those surveillance activities a patina of congressional approval by amending FISA to provide that nothing in the definition of "electronic surveillance"[31] contained in FISA "shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States" so long as a "significant purpose of the acquisition is to obtain foreign intelligence information."[32] As was evident from its 180-day "Sunset Date," the PAA was intended as a temporary fix while Congress and the Bush Administration continued to labor to produce a permanent statutory solution. [33]

[28] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://perma.cc/55UT-4N5W.
[29] *See* S. REP. NO. 110-209, at 5 (2007) (The Director of National Intelligence told the Senate Intelligence Committee that the actions of the FISC applying existing FISA standards had led "to degraded capabilities in the face of a heightened terrorist threat environment.").
[30] Protect America Act of 2007, Pub. L. 110-55, 121 Stat. 552 (2007) (codified as amended at 50 U.S.C. § 1801 et seq.).
[31] 50 U.S.C. § 1801(f).
[32] Protect America Act § 2.
[33] *Id.* § 6(c).

According to officials in the U.S. Intelligence community, the then-existing "intelligence gap" requiring redress was the product of significant changes that had transpired in communications technology since FISA was first enacted in 1978. At the time of FISA's passage, in addition to the essentially bipolar threat environment of known state actors that dominated U.S. security policy, the technological premises underlying FISA contemplated that most domestic communications would be transmitted by wire while most international communications would travel by radio wave.[34] By the early 2000s, however, intelligence officials argued the shift to undersea (predominantly fiber optic) cables for international communications and the vastly expanded domestic cellular network had essentially reversed the technological assumptions upon which FISA was premised, deleteriously impacting NSA's ability to conduct its signals intelligence mission[35] especially given the very different, multipolar, threat environment increasingly populated by non-state actors, operating either individually or collectively, that had evolved by the early 2000s as captured in its most horrid manifestation in the September 11, 2001 terror attacks.[36]

This growth in international wire communications occurred simultaneously with a corresponding explosion in the use of electronic communications such as electronic mail and text messaging. This explosion accompanied a rapid expansion of communications modalities that facilitated tremendous agility on the part of consumers in their choice and use of e-mail

[34] *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing before the S. Judiciary Comm.* 110th Cong. 3 (2007) [hereinafter PAA Hearing] (statement of J. Michael McConnell, Director of National Intelligence); *see* James Petrila, *A Brief History of Programmatic Collection Pre-Section 702*, LAWFARE (Apr. 12, 2023, 8:16 AM), https://perma.cc/AL33-QF3U ("[D]rafters of the original FISA wanted to ensure that the intelligence community continued to have access to a vast array of communications carried by commercial satellites where the target was a non-U.S. person located overseas even if that meant that a considerable amount of U.S.-person information would be incidentally collected in the process.").
[35] *Id.*; *but see* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 16.3 (3d ed. 2019) ("A review of telecommunications history … shows this claim to be exaggerated: the transition from satellite to cable was neither as dramatic, nor as unanticipated, as the government argued.").
[36] PAA Hearing, *supra* note 34, at 3 (statement of J. Michael McConnell, Director of National Intelligence).

addresses and/or telephone numbers ("selectors") across a growing number of services and devices. These commercial and technological developments introduced a significant challenge for intelligence services which, under then-existing FISA requirements, had to obtain explicit approval for each and every selector they wanted to target.

The telecommunications infrastructure associated with this growth meant that internet communications by or even between foreign persons located outside the United States often transited communications infrastructure in the United States or were stored on servers located in the United States.[37] In passing FISA in 1978, Congress had explicitly exempted foreign-to-foreign wire communications from FISA's coverage based on the assumption that such communications would not come into contact with U.S. territory. However, less than a quarter century after FISA's passage, advancements in communications technology made it possible for a foreigner abroad to communicate with other foreigners abroad via email using an American internet service provider (ISP) and accessing that email stored on a server in the United States which arguably brought that email communication into FISA's ambit.[38] By the early twenty-first century, these advances in communications technology had evolved in a way where a sizeable percentage of the world's electronic communications passed through the United States, and foreign intelligence collection against persons physically located outside the United States was therefore increasingly conducted with the assistance of communication service providers inside the United States.[39] Absent revising FISA, this new communications paradigm would require the government to seek orders from the FISC to obtain authorization for electronic surveillance for

[37] Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L. & PUB. POL'Y 117, 147-48 (2015).
[38] *Id.*
[39] Gen. Paul M. Nakasone, Commander, U.S. Cyber Command; Dir., Nat'l Sec. Agency; Chief, Cent. Sec. Serv., Keynote Speech at the Privacy and Civil Liberties Oversight Board Public Forum on FISA Section 702 (Jan. 23, 2023), https://perma.cc/3WYE-XYLK.

foreign intelligence purposes even of individuals who were in fact outside the United States, a circumstance Congress had not anticipated at the time it enacted FISA in 1978 and which Congress had explicitly attempted to exclude from FISA's statutory coverage.[40]

Aside from adjusting FISA to address the technological changes impacting NSA's collection activities, another issue complicating the debate over FISA reform was that of immunity for those private electronic communication carriers that had cooperated by providing services essential to *Stellar Wind*'s collection activities. That cooperation had been secured by appeals to the patriotism of those carriers from senior government officials who warned of the grave risk of additional terrorist attacks while providing assurances that adequate protections would be used to ensure the privacy of the carriers' customers through targeting and analytic standards focusing only on al Qaeda-related individuals. By 2008, however, over 40 lawsuits had been commenced by customers claiming that their rights had been abridged by these communication carriers' participation in the warrantless seizure of their electronic communications.[41] To assure the future cooperation of electronic communication service providers in furnishing the assistance essential to Section 702 collection, the FISA reform legislation sought by the Bush Administration included (1) limited retroactive immunity for those providers that had provided assistance at the request and direction of the government in effectuating the PSP [42] and (2) prospective immunity for electronic communication providers

[40] PRESIDENT'S REV. GRP. ON INTEL. & COMMC'NS TECH., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 133 (2013), https://perma.cc/ZR5A-RFFW.
[41] S. REP. NO. 110-209, *supra* note 29, at 7; *see, e.g.*, Jewel v. NSA, 856 Fed. Appx. 640 (9th Cir. 2019), *cert. denied*, 142 S. Ct. 2812 (2022) (alleging constitutional and statutory claims arising from NSA's electronic surveillance activities).
[42] S. REP. NO. 110-209, *supra* note 29, at 22-24.

furnishing "any information, facilities, or assistance in accordance with a directive issued" pursuant to Section 702((i).[43]

THE STATUTORY REQUIREMENTS OF FISA SECTION 702

In July 2008, Congress passed the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 ("FISA Amendments Act of 2008") replacing the existing Title VII of FISA with a revised Title VII titled "Additional Procedures Regarding Certain Persons Outside the United States" and including a new Section 702.[44] The statutory scope of Section 702 can be synopsized as follows: Section 702 of FISA permits the Attorney General and the Director of National Intelligence (DNI) to jointly authorize the (1) targeting of persons who are not United States persons, (2) who are reasonably believed to be located outside the United States, (3) with the compelled assistance of an electronic communication service provider, (4) in order to acquire foreign intelligence information.

Section 702 opens by allowing the Attorney General and the DNI to authorize, for a period of up to one year, "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence."[45] This authorization is immediately followed in subsection (b) by a series of "Limitations" restricting the scope of a Section 702 authorization including: (1) no intentional targeting of any person known at the time of the acquisition to be located within the United States; (2) no person reasonably believed to be located outside the United States may be targeted if the purpose is to acquire the communications of a particular, known person reasonably believed to be in the United States; (3) no United States person reasonably believed to be located outside the United States may be intentionally targeted; (4) no

[43] 50 U.S.C. § 1881a(i).
[44] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (2008) (codified at 50 U.S.C. § 1881a et. seq.).
[45] 50 U.S.C. § 1881a(a).

communication may be intentionally acquired where, at the time of the acquisition, the sender and all intended recipients are known to be located in the United States; (5) no communication may be intentionally acquired that contains a reference to, but is not to or from, an authorized target of an acquisition; and (6) all acquisitions under Section 702 must be conducted in a manner consistent with the Fourth Amendment to the U.S. Constitution.[46]

To ensure compliance with these statutory Limitations, Section 702 requires that the Attorney General, in consultation with the DNI, adopt "Targeting Procedures,"[47] "Minimization Procedures,"[48] "Querying Procedures,"[49] and "Acquisition Guidelines."[50] The Targeting Procedures and Acquisition Guidelines are designed to ensure compliance with the above-described Limitations found in 50 U.S.C. § 1881a(b) by ensuring that targeting is (1) directed only at non-U.S. persons located outside the United States, (2) that there is no intentional acquisition of any radio communication where both the sender and all intended recipients are known to be located in the United States at the time of acquisition, (3) that all acquisitions are conducted only in accordance with a Section 702 certification approved by the FISC, and (4) that there is compliance with the Limitations set forth in Section 702. [51] The Minimization Procedures, like those required in connection with 'traditional' FISA surveillance,[52] are intended to minimize the acquisition, retention, use, and dissemination of nonpublic information

[46] *Id.* § 1881a(b).
[47] *Id.* § 1881a(d); *see also* William P. Barr, *NSA 2020 § 702 Targeting Procedures*, FOREIGN INTEL. SURVEILLANCE CT. (2020), https://perma.cc/66SY-U5BB.
[48] 50 U.S.C. § 1881a(e); *see also* William P. Barr, *NSA 2020 § 702 Minimization Procedures*, FOREIGN INTEL. SURVEILLANCE CT. (2020), https://perma.cc/74BU-VTLU [hereinafter 2020 NSA Minimization Procedures].
[49] 50 U.S.C. § 1881a(f); *see also* William P. Barr, *FBI 2020 § 702 Querying Procedures*, FOREIGN INTEL. SURVEILLANCE CT. (2020), https://perma.cc/8CJH-L8VV [hereinafter 2020 FBI Querying Procedures].
[50] 50 U.S.C. § 1881a(g).
[51] *Id.* § 1881a(b).
[52] *Id.* §§ 1801-12 (codifying Title I of FISA, also known as 'traditional' FISA surveillance).

concerning non-consenting U.S. persons (USP or USPs) consistent with the needs of the United States to obtain, produce and disseminate foreign intelligence information.[53]

These statutory limitations, procedures, and guidelines distinguish the programmatic electronic surveillance permitted by Section 702 from the bulk collection previously conducted, for example, under the authority of Section 215 of the Patriot Act. "Bulk" collection reflects the acquisition of information where a significant portion of the retained data pertains to identifiers that are not targets at the time of collection, for example, the metadata acquired in the Section 215 program where discriminants are applied to the data *after* collection.[54] As the Privacy and Civil Liberties Oversight Board (PCLOB) succinctly observed in its July 2014 report on Section 702, "The [Section 702] program does not operate by collecting communications in bulk."[55]

NSA retains the database of unminimized communications from acquisitions conducted under the authority of Section 702.[56] This unminimized collection represents a sort of primordial stew with no intelligence value until it is accessed by queries designed to extract its foreign intelligence content. Aside from NSA, the CIA, National Counterterrorism Center (NCTC), and Federal Bureau of Investigation (FBI) have access to all, or part, of the contents of the Section 702 database (Section 702 Database). The FBI, for example, has access only to the communications generated by the particular targets that the FBI has nominated for collection.[57] In Calendar Year (CY) 2022, this afforded the FBI access to only 3.2% of Section 702 targets —

[53] *Id*. § 1801(h)(1); *see also id.* § 1801(h)(2) (explaining minimization procedures also include "procedures that require that nonpublicly available information, that is not foreign intelligence information … shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance.").
[54] *See* NAT'L RSCH. COUNCIL, BULK COLLECTION OF SIGNALS INTELLIGENCE: TECHNICAL OPTIONS 37 (Nat'l Academies Press ed., 2015).
[55] PCLOB Report, *supra* note 24, at 103.
[56] *See id.* at 7.
[57] OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES 22 (2023), https://perma.cc/3T8C-D6N6 [hereinafter 2023 DNI Statistical Transparency Report]

or roughly 8,000 of the 246,073 non-USPs targeted.[58] Notably, the FBI nominates for collection only those targets associated with open, fully predicated national predicated national security investigations—the most serious class of investigation in the FBI's investigative hierarchy.[59]

The requirement that agencies with access[60] to the Database containing unminimized Section 702 communications develop procedures for querying that Database was added to Section 702 by the FISA Amendments Reauthorization Act of 2017 ("FISA Amendments Act of 2017") culminating in the reauthorization of Section 702 in January 2018.[61] The mandate for querying procedures was included, *inter alia*, to address critics' contentions that the FBI, in particular, routinely accesses the Section 702 Database using USP query terms to conduct "back door" searches in pursuit of its law enforcement, as opposed to foreign counterintelligence, investigations.[62] The Querying Procedures require that, aside from an exception available when there is a reasonable belief that access to the Section 702 Database will mitigate or eliminate a danger of death or serious bodily injury, where the FBI seeks to query that Database "in connection with a predicated criminal investigation opened by the [FBI] that does not relate to the national security of the United States," the FBI may not access the contents of any communications retrieved from the Database using a USP query term without first securing an order from the FISC demonstrating that probable cause exists to believe that the contents of the communications sought from the Section 702 Database will provide evidence of criminal activity, contraband, or property designed or intended for use in a crime.[63]

---

[58] *Id.* at 22-24.
[59] *See id.* at 22.
[60] *See id*. at 14-16.
[61] FISA Amendments Reauthorization Act of 2017, Pub. L. 115-118, § 101, 132 Stat. 3, 4-8 (2018) [hereinafter FISA Amendments Reauthorization Act].
[62] *See* Julian Sanchez, *Report Discloses Unlawful "Backdoor Searches" of FISA Database*, CATO AT LIBERTY BLOG (May 15, 2020, 3:59 PM), https://perma.cc/3D9T-S8EK.
[63] 50 U.S.C. § 1881a(f)(2).

Authority for a Section 702 acquisition is obtained in a manner that materially differs from a 'traditional' FISA surveillance. Title I of FISA requires an application to the FISC for an order which can issue only after an individualized determination by the FISC that there is probable cause to believe that the target is a foreign power or an agent of a foreign power, and that the target is using or about to use specified facilities.[64] Conversely, a Section 702 acquisition is initiated by a written "certification"[65] by the Attorney General and the DNI attesting that there are targeting procedures that have been submitted to the FISC (or will be submitted with the certification)[66] and guidelines[67] which, collectively, are reasonably designed to: (1) ensure that the proposed acquisition is limited to targeting persons reasonably believed to be outside the United States, (2) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States, (3) ensure compliance with the limitations in § 18881a(b), and (4) ensure that a certification is filed with the FISC. The certification must also include both minimization and querying procedures that comply with Section 702's requirements[68] and, in the case of the minimization procedures, meet the definition of minimization procedures prescribed in FISA.[69] Lastly, the certification must attest that "a significant purpose" of the acquisition is to obtain foreign intelligence information.[70]

However, in a clear departure from the requirements of a 'traditional' Title I FISA surveillance, a certification is not required to identify any particular target or to disclose the

[64] *Id.* §§ 1804-05.
[65] *See id.* § 1881a(h)(2)(C) (instructing the certification should be supported "as appropriate, by the affidavit of any appropriate official in the area of national security who is (i) appointed by the president with the advice and consent of the Senate, or (ii) the head of an element of the intelligence community.").
[66] *Id.* § 1881a(h)(2).
[67] *Id.* § 1881a(g)(2).
[68] *Id.* § 1881a(e), 1881a(f)(1).
[69] *Id.* § 1801(h) (defining "minimization procedures" in the context of electronic surveillance).
[70] *Id.* § 1881a(h)(2)(A)(v).

specific facilities, places, premises, or property at which an acquisition will be directed or conducted.[71] Clarifying that Section 702 acquisitions are not subject to the requirements of Title I of FISA, Congress specifically provided that "[n]othing in title I shall be construed to require an application under such title for an acquisition that is targeted in accordance with this section [702] at a person reasonably believed to be located outside the United States."[72]

Upon receipt of a certification and its accompanying targeting, minimization, and querying procedures, the statute specifies that the FISC has 30 days to conduct its "review" of that certification.[73] Under Section 702, the FISC conducts no probable cause inquiry and does not review the targeting of particular individuals;[74] instead, Section 702 specifies that the court determine whether a certification contains all the statutorily required elements and whether the targeting, minimization, and querying procedures applicable to the acquisition are consistent with Section 702's statutory requirements and with the Fourth Amendment to the Constitution.[75] If the FISC is satisfied that these statutory and constitutional standards have been met, it issues an order approving the certification.[76]

In its 2014 report on Section 702, the Privacy and Civil Liberties Oversight Board (PCLOB) observed that "[t]he FISC's review of the Section 702 certifications has been called 'limited' by scholars, privacy advocates, and in one instance, shortly after the FISA Amendments Act was passed, by the FISC itself."[77] Notably, however, while the statute circumscribes the

[71] *Id.* § 1881a(h)(4).
[72] *Id.* § 1881a(c)(4).
[73] *Id.* § 1881a(j)(1)(B).
[74] *See* OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES 13 (2022), https://perma.cc/872C-QW2D [hereinafter 2022 DNI Statistical Transparency Report] (detailing that although not reviewed by the FISC, the government must record, in every targeting decision, the specific rationale for targeting a specific person to obtain foreign intelligence information.).
[75] 50 U.S.C. §1881a(j)(2)-(3).
[76] *Id.*
[77] PCLOB Report, *supra* note 24, at 26-27.

matters subject to review (the Section 702 certification and the targeting procedures, minimization procedures, and querying procedures adopted in accordance with subsections (d), (e), and (f)(1) [of Section 702]), it imposes no strictures on the latitude afforded to the FISC in conducting its review. [78] The language used by Congress in Section 702 directs the FISC to satisfy itself that these targeting, minimization, and querying procedures[79] are "consistent with [Section 702] and with the fourth amendment to the Constitution of the United States."[80] The FISC is statutorily unfettered with regard to the process it pursues to reach its conclusion.

Consequently, the FISC does not limit its review to the statutory procedures as written, but extends that review to include an examination of how those procedures have been and will be implemented in practice.[81] Specifically, the FISC considers "every identified compliance incident reported by the government through notices and reports, other reports concerning implementation and compliance information such as the number of targets and other statistical information, the results of oversight reviews, and assessment of compliance trends."[82] And, to be clear, this Fourth Amendment review is not undertaken by administrative functionaries beholden to the executive branch or the Intelligence community: the FISC is populated by federal district judges who are appointed by the Chief Justice of the U.S. Supreme Court for seven-year terms.[83]

---

[78] 50 U.S.C. § 1881a(j)(2).
[79] Memorandum Opinion and Order [Caption Redacted], [Docket No. Redacted], at *14 (FISA Ct. Nov. 18, 2020) (Boasberg, J.), https://perma.cc/X7VY-P7BC [hereinafter *2020 Boasberg Opinion and Order*] (explaining that, like the FISC's concurrent review for practical reasons, "each agency's procedures make clear that the querying and minimization procedures are to be read and applied together").
[80] 50 U.S.C. § 1881a(j)(3)(A).
[81] *See* 2023 DNI Statistical Transparency Report, *supra* note 57, at 15; 2022 DNI Statistical Transparency Report, *supra* note 74, at 14; *see also 2020 Boasberg Opinion and Order, supra* note 79, at *35 ("FISC review of the sufficiency of Section 702 procedures is not limited to the procedures as written, but also encompasses how they are implemented.").
[82] *See* 2022 DNI Statistical Transparency Report, *supra* note 74, at 14; *see also* U.S. FOREIGN INTEL. SURVEILLANCE CT., RULES OF PROCEDURE 13(b) (2010), https://perma.cc/KU9E-CNTL (requiring disclosure of any instance where an authority or approval of the FISC has been implemented in a manner not complying with the court's authorization).
[83] 50 U.S.C. § 1803 (a)(1).

Once the FISC has entered an order approving a certification, the government conducts the acquisition by directing the assistance of an "electronic communication service provider."[84] Notwithstanding the foreign focus of the targets of Section 702 surveillance, Congress understood that the acquisition of the targeted communications would occur in the United States and the statute specifically provides that the Attorney General and the DNI, in conjunction with the authorization of an acquisition pursuant to Section 702, may direct an electronic communication service provider to immediately provide the government with all information, facilities, or technical assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition while producing minimum interference with the provider's service to the target.[85] Electronic communication service providers are compensated "at the prevailing rate" for all services provided to the government in connection with assisting an authorized Section 702 acquisition[86] and, reflecting the outcome of the extensive debate preceding the passage of the FISA Amendments Act of 2008 over the potential civil liability of those providers that had provided assistance to the *Stellar Wind* program, Section 702 assures that "no cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities or assistance in accordance with a directive issued pursuant to [Section 702]."[87]

As a further measure directed at securing the essential cooperation of electronic communication service providers, Congress also furnished those providers with the statutory

[84] *Id.* § 1881a(i). "Electronic communication service provider" is defined in Title VII and includes, by reference to other definitions found in the U.S. Code, a telecommunications carrier, a provider of electronic communication service, a provider of remote computing service, and "any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored." *Id.* § 1881(b)(4).
[85] *Id.* § 1881a(i)(1)(A).
[86] *Id.* § 1881a(i)(2).
[87] *Id.* § 1881a(i)(3).

right to challenge any directive by filing a petition requesting the FISC to modify or set aside any directive where the FISC concludes that the directive "does not meet the standards of [Section 702] or is otherwise unlawful."[88] The public record documenting instances in which electronic communication service providers have challenged a directive issued under Section 702 is sparse;[89] the best known instance catalogued is *In re Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Act*,[90] but the provision remains a statutory avenue by which an electronic communication service provider can challenge directives issued to facilitate the implementation of a Section 702 acquisition.

THE OPERATIONAL SCOPE AND INTELLIGENCE VALUE OF SECTION 702

Since first passed by Congress as part of the FISA Amendments Act of 2008, Section 702 has steadily grown to become arguably the most significant collection tool available to the U.S. Intelligence community. By 2014, it was estimated that more than a quarter (25%) of all foreign intelligence reports issued by NSA concerning counterterrorism included information based in whole or in part on Section 702 collection.[91] During the debate surrounding its reauthorization in 2017, Section 702 was described as "the most important electronic intelligence-gathering mechanism that the United States has to keep us safe"[92] and "as one of the most, if not the most, critical national security tool used by our intelligence community to obtain intelligence on

[88] *Id.* § 1881a(i)(4)(C).
[89] *See* PCLOB Report, *supra* note 24, at 32 n.112 (noting that no directive issued in conjunction with a Section 702 certification had been challenged).
[90] In re Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (*Directives*), 551 F.3d 1004 (FISA Ct. Rev. 2008). *Directives* was commenced by a petition initiated by an electronic communication service provider (Yahoo) under the provisions of the PAA. By the time the Foreign Intelligence Surveillance Court of Review decision was issued in August 2008, the PAA had expired and the provisions of the FISA Amendments Act of 2008 were in place. While the FISCR "assess[ed] the validity of the actions at issue here through the prism of the PAA," *id.* at 1004, the substantive provisions of the PAA regarding directives issued to providers do not materially differ from those found in the FISA Amendments Act of 2008.
[91] PCLOB Report, *supra* note 24, at 10.
[92] 164 CONG. REC. H147 (daily ed. Jan. 11, 2018) (remarks of Rep. Goodlatte).

foreign terrorists located overseas."[93] In connection with that same reauthorization debate, the DNI released a "Guide to Section 702 Value Examples" identifying multiple instances where information acquired through Section 702 surveillance had provided crucial information to U.S. policymakers.[94] Although similar calibrations of Section's 702 value remain classified, neither the volume of Section 702 collection nor its ubiquity in intelligence reporting seems likely to have diminished in the ensuing years.

Section 702 has been reauthorized by Congress twice since its enactment in 2008. During the 2012 reauthorization debate, the Attorney General and the DNI advised Congress that the reauthorization of Section 702 was the Intelligence Community's "top legislative priority."[95] Describing the collection program as "vital to keeping the nation safe," the letter advised that "[f]ailure to reauthorize Section 702 would result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities."[96] Subsequently, when Section 702 approached its sunset in 2017, the Attorney General and the DNI characterized its renewal as "the top legislative priority of the Department of Justice and the Intelligence Community" while noting that the PCLOB had publicly reported that "information collected under one particular section of FAA, Section 702, produces significant foreign intelligence that is vital to protect the nation against international terrorism and other threats."[97] In anticipation of the 2023 congressional debate concerning Section 702's

[93] *Id.* at H142 (remarks of Rep. Stewart).
[94] OFF. OF THE DIR. OF NAT'L INTEL., GUIDE TO SECTION 702 VALUE EXAMPLES (2017), https://perma.cc/6879-TDD8.
[95] Letter from Eric H. Holder Jr., Att'y Gen., and James R. Clapper, Dir. of Nat'l Intel., to the Honorable John Boehner, Speaker, U.S. House of Representatives, the Honorable Harry Reid, Majority Leader, U.S. Senate, the Honorable Nancy Pelosi, Democratic Leader, U.S. House of Representatives, and the Honorable Mitch McConnell, Republican Leader, U.S. Senate (Feb. 8, 2012), https://perma.cc/39W7-9VNF [hereinafter 2012 Letter].
[96] *Id.*
[97] Letter from Jefferson B. Sessions III, Att'y Gen., and Daniel R. Coats, Dir. of Nat'l Intel., to the Honorable Paul Ryan, Speaker, U.S. House of Representatives, the Honorable Mitch McConnell, Majority Leader, U.S. Senate, the

reauthorization, the Attorney General and the DNI have written to congressional leadership again characterizing the reauthorization of Section 702 as "a top legislative priority" [98] and, at a forum on Section 702 sponsored by the PCLOB, NSA's Director described Section 702 as "irreplaceable."[99] Recently, in anticipation of the current debate over reauthorization, it was reported that 59% of the intelligence reported in the President's Daily Brief "is gleaned at least in part from Section 702."[100]

Section 702 permits the FISC to approve the collection authority sought in a Section 702 certification for periods of up to one year. The FISC may issue a single order approving more than one certification to acquire foreign intelligence and, while the number of certifications submitted to the FISC by the government is classified, the number of FISC Section 702 orders is publicly available.[101] Indeed, since most details of the Section 702 collection program are highly classified, the information publicly available regarding the scope of Section 702 surveillance activity is limited. There are, however, some nuggets of insight. By 2011, three years after its passage, NSA was acquiring more than 250 million internet communications each year pursuant to Section 702.[102] In 2014, the DNI began publishing annual statistical reports that include the number of Section 702 targets in a calendar year.[103] As illustrated in the table below, the number

Honorable Nancy Pelosi, Minority Leader, U.S. House of Representatives, and the Honorable Charles E. Schumer, Minority Leader, U.S. Senate, (Sep. 7, 2017), https://perma.cc/8YYG-5HP4 [hereinafter 2017 Letter].

[98] Letter from Merrick B. Garland, Att'y Gen, and Avril D. Haines, Dir. of Nat'l Intel., to the Honorable Charles E. Schumer, Majority Leader, U.S. Senate, the Honorable Mitch McConnell, Minority Leader, U.S. Senate, the Honorable Kevin McCarthy, Speaker, U.S. House of Representatives, and the Honorable Hakeem S. Jeffries, Minority Leader, U.S. House of Representatives (Feb. 28, 2023), https://perma.cc/A2MN-DXZR [hereinafter 2023 Letter].

[99] Nakasone, *supra* note 39.

[100] Dustin Volz, *FBI Warrantless Searches of Americans' Communications Declined, Spy Agency Says*, WALL ST. J. (Apr. 28, 2023, 4:06 PM), https://perma.cc/6VD8-BQ6B.

[101] *See* 2023 DNI Statistical Transparency Report, *supra* note 57, at 18 (documenting one FISC Section 702 order issued in 2020, none issued in 2021, and one issued in 2022).

[102] Memorandum Opinion and Order, [Caption Redacted], [Docket No. Redacted], 2011 WL 10945618, at *9 (FISA Ct. October 3, 2011) (Bates, J.).

[103] *See, e.g.*, Press Release, Off. of the Dir. of Nat'l Intel., ODNI Releases Annual Intelligence Community Transparency Report (Apr. 29, 2022), https://perma.cc/46C6-6Z7N.

of Section 702 targets has generally increased each year and, presumably, the 89,138 targets reported in CY 2013 exceeded the number of targets that produced the 250 million+ communications referenced in the 2011 Bates Opinion. As of CY 2022, the number of Section 702 targets had grown from 89,138 in CY2013 to 246,073. Extrapolating from those target numbers produces the reasonable assumption that authorized Section 702 acquisitions are now collecting in the range of one billion internet communications annually.

FISA Section 702 Targets[104]

CY 2013	**CY 2014**	**CY 2015**	**CY 2016**	**CY 2017**	**CY 2018**	**CY 2019**	**CY 2020**	**CY 2021**	**CY 2022**
89,138	92,707	94,368	106,469	129,080	164,770	204,968	202,723	232,432	246,073

THE PERPETUAL DEBATE OVER THE LEGALITY OF SECTION 702

From its statutory construct to its practical application to its expansive compliance regimen, the Section 702 surveillance program represents a carefully configured national intelligence undertaking that is of apodictic value to the national security.[105] Yet, the legality of

[104] 2023 DNI Statistical Transparency Report, *supra* note 57, at 18; 2022 DNI Statistical Transparency Report, *supra* note 74, at 14; OFF. OF THE DIR. OF NAT'L INTEL., ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES 16 (2021), https://perma.cc/YGP7-W4EP; OFF. OF THE DIR. OF NAT'L INTEL., STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES 14 (2020), https://perma.cc/SU5Y-RDXD; OFF. OF THE DIR. OF NAT'L INTEL., STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES 13 (2019), https://perma.cc/D53U-AQN2; OFF. OF THE DIR. OF NAT'L INTEL., STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES 6 (2018), https://perma.cc/C78Y-8HNX; OFF. OF THE DIR. OF NAT'L INTEL., STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES 7 (2017), https://perma.cc/4R8Y-8URE; OFF. OF THE DIR. OF NAT'L INTEL., STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES 5 (2016), https://perma.cc/RPQ8-TYWC; OFF. OF THE DIR. OF NAT'L INTEL., STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES 1 (2015), https://perma.cc/DM5R-TVAK.

[105] *See* PCLOB Report, *supra* note 24, at 25, 103-04; *see also* 2012 Letter, *supra* note 95; 2017 Letter, *supra* note 99; 2023 Letter, *supra* note 100. The letters submitted by the Attorney General and the DNI in connection with the 2012, 2017 and 2023 reauthorizations of Section 702 attest to its value as a foreign intelligence tool.

Section 702 has been attacked from the day the FISA Amendments Act of 2008 became law.[106] That initial challenge was ultimately rejected by the Supreme Court on standing grounds and, in the decade that has passed since that decision, every federal appellate court to have considered a challenge to Section 702 surveillance—whether grounded in the Fourth Amendment, the First Amendment, or both—has affirmed its constitutionality.[107]

The Fourth Amendment challenge is the one most frequently addressed by the courts. The constitutionality of the Section 702 program poses some uniquely challenging questions precisely because, as the PCLOB recognized, it is a complex surveillance program—"one that entails many separate decisions to monitor large numbers of individuals, resulting in the annual collection of hundreds of millions of communications."[108] Moreover, the analysis is further snarled because the only constitutional interests at stake are not those actually targeted for surveillance—as non-U.S. persons located outside the United States, they lack any Fourth Amendment rights,[109] The constitutional issue arises for those USPs who, although not targeted, have their communications incidentally acquired as a result of communicating with foreign targets. Because it is large-scale programmatic surveillance, the operation of the Section 702 program captures telephone and internet communications of USPs in three ways;[110]

---

[106] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 407 (2013) ("*On the day when the FISA Amendments Act was enacted*, respondents filed this action seeking (1) a declaration that § 1881a, on its face, violates the Fourth Amendment, the First Amendment, Article III, and separation-of-powers principles, and (2) a permanent injunction against the use of § 1881a.") (emphasis added).

[107] United States v. Muhtorov, 20 F.4th 558 (10th Cir. 2021); United States v. Hasbajrami, 945 F.3d 641 (2d Cir. 2019); United States v. Mohamud, 843 F.3d 420 (9th Cir. 2016).

[108] PCLOB Report, *supra* note 24, at 86.

[109] *See* United States v Verdugo-Urquidez, 494 U.S. 259, 274-75 (1990) (The Supreme Court held the Fourth Amendment had "no application" to a search of a Mexican citizen and resident of Mexico who had no voluntary attachment to the United States … because "it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory."); *see also* Agency for Int'l Dev. v. Alliance for Open Soc'y Int'l, Inc., 140 S. Ct. 2082, 2086 (2020) ("[I]t is long settled as a matter of American constitutional law that foreign citizens outside U. S. territory do not possess rights under the U.S. Constitution.").

[110] PCLOB Report, *supra* note 24, at 87 (summarizing acquisition can occur as a result of: (1) a USP communicating by telephone or internet with a foreigner located abroad who has been targeted (i.e., "incidental" collection); (2) a

any Fourth Amendment analysis must take into account the cumulative impact of those privacy intrusions and, ultimately, balance those intrusions against the limitations and protections included in the Section 702 program to mitigate them.

The courts have explicated, repeatedly, the analysis confirming the constitutional foundation for Section 702. It begins with the Fourth Amendment itself which is grounded in the concept of "reasonableness." A search or seizure satisfies the Fourth Amendment if it is reasonable.[111] "Reasonableness" generally requires the obtaining of a warrant[112] but includes the flexibility to dispense with the warrant requirement in certain circumstances.[113] In the context of Section 702, that dispensation from the warrant requirement flows from the U.S. Supreme Court's decision in *Keith* where the Court observed that "the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection."[114] The *Keith* court went on to suggest that Congress might also judge that warrants in national security cases need not follow the requirements used in more traditional law enforcement settings (although, in *Keith*, the Supreme Court eschewed specifically recognizing a foreign intelligence exception to the Fourth Amendment warrant requirement) and might, instead, allege circumstances more appropriate to security cases, and, in sensitive cases, be addressed to "any member of a specially designated court."[115] Much of the construct of the FISA statute originally passed by Congress in 1978 reflects the *Keith* court's commentary on the flexibility of the warrant requirement with respect to foreign intelligence matters, the discretion

USP sending or receiving an internet communication that is embedded within the same transaction as a different communication that meets the criteria for collection (i.e., a Multiple Communication Transaction); or (3) a USP's communication being acquired by mistake due to an implementation error or technological malfunction (i.e., "inadvertent" collection)).

[111] *Muhtorov*, 20 F.4th at 591 (citing Riley v. California, 573 U.S. 373, 381-82 (2014)).

[112] Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).

[113] Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

[114] United States v. U.S. District Court (*Keith*), 389 U.S. 297, 323 (1972).

[115] *Id.*

of Congress in prescribing standards that satisfy the reasonableness standard of the Fourth Amendment, and the use of a "specially designed court" for electronic surveillance conducted for foreign intelligence purposes.[116]

The initial specific judicial recognition of the existence of a foreign intelligence exception to the warrant requirement in the context of a Section 702-like acquisition appears in the Foreign Intelligence Surveillance Court of Review's (FISCR's) decision in *Directives* where the FISCR surveyed the Supreme Court's holdings in so-called "special needs" cases excusing compliance with the warrant requirement "when the purpose behind the government's action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose."[117] Applying principles drawn from those special needs cases, the FISCR concluded that the type of foreign intelligence surveillance authorized by the PAA, and subsequently continued under the authority conferred in Section 702, "possesses characteristics that qualify it for such an exception," noting that "the purpose behind a [Section 702] surveillance … goes well beyond any garden variety law enforcement objective. It involves the acquisition from overseas foreign agents of foreign intelligence to help protect national security. Moreover, this is the sort of situation in which the government's interest is particularly intense."[118] Further, as the FISCR noted, "[c]ompulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government's ability to collect information in a timely manner."[119]

[116] *Id.* at 323-24.
[117] In re Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (*Directives*), 551 F.3d 1004, 1010 (FISA Ct. Rev. 2008).
[118] *Id.* at 1011.
[119] *Id.* at 1011-12.

Dispensing with the requirement of a warrant does not end the constitutional inquiry because the Fourth Amendment requires that every search "be reasonable in its scope and manner of execution"[120] and "even though the foreign intelligence exception applies in a given case, governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirements."[121] The absence of a warrant merely acknowledges that reasonableness be judged by examining the "totality of the circumstances" and balancing the degree of the intrusion upon an individual's privacy against the degree that intrusion is needed for the promotion of legitimate governmental interests.[122] In *Directives*, the FISCR recognized that the government interest at stake—the interest in national security—is of the highest order of magnitude and that the matrix of procedural mechanisms incorporated as part of every authorized Section 702 acquisition to protect the privacy interests of USPs struck a balance in favor of the intrusive surveillance being assessed as reasonable under the Fourth Amendment.[123]

Apart from the FISCR, three other federal appellate courts have now assessed the totality of circumstances surrounding an authorized Section 702 surveillance directed against a foreign target and each concluded that such surveillance does not violate the Fourth Amendment.[124]

For Section 702 critics, however, resolving the legality of surveillance as it pertains to the foreign target is the considerably less fraught inquiry when the other party to the acquired communication is a USP. A ubiquitous issue arising in every Section 702 reauthorization debate, and already resurfacing in 2023, is those critics' insistence that the incidental collection of USPs communicating with authorized Section 702 targets is unlawful. In *Directives*, the FISCR

[120] Maryland v. King, 569 U.S. 435, 448 (2013).
[121] *Directives*, 551 F.3d at 1012.
[122] PCLOB Report, *supra* note 24, at 91.
[123] *Directives*, 551 F.3d at 1013.
[124] United States v. Muhtorov, 20 F.4th 558 (10th Cir. 2021); United States v. Hasbajrami, 945 F.3d 641 (2d Cir. 2019); United States v. Mohamud, 843 F.3d 420 (9th Cir. 2016).

unequivocally stated: "It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."[125] The other federal appellate courts to address the issue in the context of Section 702 agree. *Muhtorov*, the Tenth Circuit decision that is the most recent to have considered Section 702, examined both the "incidental overhear" and "plain view" doctrines in concluding that "the initial intrusion [of the Section 702 acquisition] that brought the government into contact with Muhtorov's communications" was lawful, and "it was then reasonable for the government to collect Mr. Muhtorov's communications during the otherwise lawful Section 702 surveillance."[126] In the *Muhtorov* court's view, "once it was targeting the foreign national [with whom Muhtorov was communicating] under PRISM, the government was lawfully 'in' the two-way communications."[127] The court also pointed to the statutory restraints limiting Section 702 acquisitions to pursuing foreign intelligence – a circumstance where the government's need to collect time-sensitive information is "paramount" in the "reasonableness" balancing of interests – and the required use of targeting and minimization procedures designed to preclude targeting USPs while "minimiz[ing] the acquisition and retention … of nonpublicly available information concerning unconsenting United States persons" as limiting the intrusiveness of the acquisition and preventing its becoming an "unreasonable general exploratory" search.[128]

In the 15 years that have elapsed since the FISA Amendments Act of 2008 became law, critics of the Section 702 collection program have relentlessly insisted that its authorizing statute

[125] *Directives*, 551 F.3d at 1015.
[126] *Muhtorov*, 20 F.4th at 598.
[127] *Id.*
[128] *Id.* at 599-600; *see Mohamud*, 843 F.3d at 440-41 ("[T]he guiding principle behind [the Title III incidental overhear cases] applies with equal force here: when surveillance is lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons' communications with the targeted person is also lawful.").

is unconstitutional[129] even as the FISC, the PCLOB,[130] and every federal court of appeals to have considered the constitutionality of Section 702 have determined otherwise.[131] Nonetheless, challengers to Section 702 are already preparing their lists of the program's shortcomings in anticipation of the 2023 reauthorization debate. Principal among the deficiencies that will almost certainly be alleged are: (1) an insistence that, despite statutory changes to Section 702 enacted as part of the last reauthorization, the FBI's querying of the Section 702 Database in pursuit of its law enforcement responsibilities continues to constitute back door searches that violate the Fourth Amendment;[132] (2) that the "incidental" collection of millions of USP communications as an acknowledged element of the programmatic targeting of foreigners renders Section 702 unreasonable under any plausible reading of the Fourth Amendment; (3) that the absence of any statutory requirement for particularized identification of either the surveillance target or the communications collected represents precisely the sort of "general warrant" forbidden by the Fourth Amendment; and (4) that Congress must restore the "primary purpose" test to insure that Section 702 is used for its intended purpose of acquiring foreign intelligence and not suborned to prohibited law enforcement uses. There will be other protestations, too, concerning "abouts" collection by NSA and the privacy rights of foreigners, but this former group of alleged infringements is likely to dominate the coming debate and is deserving of examination in greater detail.

---

[129] *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 407 (2013) (noting that plaintiffs challenged the constitutionality of Section 702 "on the day when the FISA Amendments Act was enacted").
[130] PCLOB Report, *supra* note 24, at 93-97.
[131] *Muhtorov*, 20 F.4th at 558; United States v. Hasbajrami, 945 F.3d 641 (2d Cir. 2019); *Mohamud*, 843 F.3d at 420.
[132] *See, e.g.*, Elizabeth Goitein, *The Year of Section 702 Reform, Part I: Backdoor Searches*, JUST SEC. (Feb. 13, 2023), https://perma.cc/J7QD-XJ9E; Laura K. Donohue, *The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law*, COUNCIL ON FOREIGN REL. (June 26, 2017), https://perma.cc/NM5G-EEGX [hereinafter Donohue, *Case for Reform*] (arguing that Section 702 "violates citizens' rights, creates a situation ripe for abuse, and undermines the balance of power" and must be altered to prevent queries seeking information about criminal activity).

1. The FBI should not be permitted to conduct "back door" searches using USP queries to probe criminal activity without a warrant.[133]

From FISA's inception, Congress contemplated that information derived from FISA electronic surveillances could be retained and disseminated for law enforcement purposes. The definition of minimization procedures contained in FISA since it became law in 1978 provides authority to retain and disseminate information "that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminate for law enforcement purposes."[134] In the 45 years since, Congress has never excised this feature permitting the retention and dissemination of FISA-acquired information for law enforcement purposes consistent with the Fourth Amendment. Further, if one's view of querying is that only the initial Section 702 acquisition is a Fourth Amendment search or seizure, then any subsequent querying of those lawfully acquired communications requires no separate Fourth Amendment justification.[135]

Privacy advocates and some legal commentators, however, insist that the querying of the Section 702 Database using a USP query term is a Fourth Amendment search separate from the initial seizure of the communications contained within that Database and must satisfy the Fourth Amendment's warrant requirement if undertaken for law enforcement purposes.[136] Indeed, one critic has gone so far as to allege that Section 702 has become "a go-to domestic spying tool for the FBI."[137]

[133] Donohue, *Case for Reform*, *supra* note 132.
[134] 50 U.S.C. § 1801(h)(3).
[135] *See* United States v. Mohamud, No. 3:10-cr-475-KI-1, 2014 WL 2866749, at *26 (D. Or. June 24, 2014), *aff'd,* 843 F.3d 420 (9th Cir. 2016) ("[S]ubsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make a § 702 search unreasonable under the Fourth Amendment.").
[136] THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 104 (Jennifer Daskal & Stephen I. Vladeck, eds., 2017).
[137] Goitein, *supra* note 132.

Congress addressed the issue of back door searches in conjunction with its 2017 reauthorization of Section 702 by adding querying procedures to the panoply of requirements governing the conduct of Section 702 acquisitions.[138] Those procedures include the requirement that, in connection with a predicated criminal investigation opened by the FBI unrelated to the national security, the FBI may not access the content of communications in the Section 702 Database using a USP query term that is not designed to find and extract foreign intelligence information without first procuring an order from the FISC demonstrating probable cause that the USP query term will produce (1) evidence of criminal activity, (2) contraband or the fruits or instrumentalities of crime, or (3) property designed for use or intended for use in committing a crime.[139]

Simultaneously, however, Congress circumscribed this "F(2)" querying requirement by adding a "Rule of Construction" that permits the FBI (1) to review, without a court order, the results of any query that was "reasonably designed to find and extract foreign intelligence information, regardless of whether such foreign intelligence information could also be considered evidence of a crime," and (2) to "access the results of queries conducted when evaluating whether to open an assessment or predicated investigation relating to the national security."[140] Notably, in adding the F(2) querying requirement in 2017, Congress made clear that the new querying procedures represented a policy compromise and were not constitutionally required, as reflected in these comments made during the 2017 reauthorization debate:

[138] 50 U.S.C. § 1881a(f)(1)-(2).
[139] *Id.* § 1881a(f)(2) (the "F(2)" query requirement).
[140] *Id.* § 1881a(f)(2)(F)(ii)-(iii).

- "This [F(2)] order requirement does not reflect the [HPSCI] committee's belief or intent that law enforcement access to lawfully acquired information constitutes a separate search under the Fourth Amendment;"[141]
- "The Fourth Amendment, as interpreted by numerous federal courts, does not require the FBI to obtain a separate order from the FISC to review lawfully acquired 702 information;"[142]
- "Though not required by the Constitution, this compromise is meant to provide additional protections for U.S. person information that is incidentally collected under section 702."[143]

These new querying mandates added in 2017 have not allayed the objections of Section 702 critics and, given the broad "Rule of Construction" that Congress built into the querying standards, this is not particularly surprising.[144] In practice, since 2017, the FBI has yet to seek a single order under the F(2) querying requirement and, in April 2022, the DNI reported that there had been four "identified instances" in CY2021 where a FISC order "was required pursuant to Section 702(F)(2) but not obtained" prior to reviewing the results of a USP query.[145] Subsequently, in April 2023, the DNI reported that one additional incident of non-compliance with the F(2) querying requirement had occurred beyond the four incidents reported in CY 2021,

[141] 164 CONG. REC., *supra* note 92, at H142-43 (remarks of Rep. Stewart).
[142] *Id.*
[143] *Id.*
[144] 50 U.S.C. § 1881a(f)(2)(F)(ii)-(iii).
[145] 2022 DNI Statistical Transparency Report, *supra* note 74, at 22. *See also* Memorandum Opinion and Order [Caption Redacted], [Docket No. Redacted], at *42 (FISA Ct. Nov. 18, 2020) (Boasberg, J.), https://perma.cc/X7VY-P7BC ("[T]he government has reported numerous incidents involving U.S. person-queries that were designed to return evidence of a crime unrelated to foreign intelligence … [but] the government has never applied to the FISC for an order under Section 702(f)(2).").

and that an additional incident of non-compliance with the F(2) querying requirement had been reported in CY 2022.[146]

These revelations for CY 2021 and CY 2022 appeared simultaneously with the DNI's first public disclosures regarding the extent of the FBI 's use of USP queries to query the roughly 3.2%[147] of the Section 702 Database to which the FBI has access comprised of that part of the Database containing communications acquired from those targets that the FBI has nominated for collection.[148] Notably, the FBI nominates for collection only those targets associated with "full" predicated investigations – the most serious class of investigation in the FBI's investigative hierarchy and, accordingly, the U.S. person communications incidentally collected are those of Americans communicating with the foreigners targeted by virtue of being the subjects of those predicated investigations.[149] The tables that follow contain, first, the cumulative numerical use of USP query terms to search the Section 702 Database (both for contents and noncontents (*i.e.*, metadata)) by NSA, CIA and the NCTC since Section 702 was last reauthorized at the close of CY2017, including certain revised statistics as recalculated by NSA and included in the 2023 DNI Annual Statistical Transparency Report.[150] The second table is the 2023 DNI statistical disclosures regarding the FBI's use of USP query terms to query the contents and noncontents of that part of the unminimized Section 702 Database to which it has access "for foreign intelligence information and/or evidence of a crime" during the indicated time intervals.

Table 1

USP Query Terms Used to Query Section 702 Content and Noncontents By NSA, CIA, and NCTC since 2017 Section 702 Reauthorization[151]

[146] 2023 DNI Statistical Transparency Report, *supra* note 57, at 26.
[147] *Id.* at 22.
[148] Asha Rangappa, *Don't Fall for the Hype: How the FBI's Use of Section 702 Surveillance Data Really Works*, JUST SEC. (Nov. 29, 2017), https://perma.cc/7DNB-P558.
[149] *Id.*
[150] 2023 DNI Statistical Transparency Report, *supra* note 57, at 20-21.
[151] *Id.*

FISA Section 702	**CY 2018**	**CY 2019**	**CY 2020**	**CY 2021**	**CY 2022**
Estimated number of searches of Unminimized Content/Noncontents of Section 702 Database by NSA, CIA, and NCTC using USP query terms	13,892/ 14,307	9,222/ 16,545	7,282/ 9,051	8,406/ 3,958	4,684/ 3,656

Table 2

Number of USP Queries of Section 702 Combined Contents/Noncontents (FBI)[152]

Estimated No. of U.S. Person Queries of Unminimized Section 702-acquired Contents and Noncontents	**Duplicative Counting Method Used in CY 2021 Report**	**De-Duplicated Counting Method Used in CY 2022 Report**
December 2019–November 2020	1,324,057	852,894
December 2020–November 2021	3,394,053	2,964,643
December 2021–November 2022	204,090	119,383

While the methodology and parameters used to produce these FBI querying statistics are somewhat arcane—the 2022 DNI Statistical Transparency Report devotes four pages to explaining them, and the 2023 DNI Statistical Transparency Report follows by devoting another four pages to explaining why the FBI querying statistics disclosed for CY 2021 were not accurate[153]—it is apparent that, by any standard of measurement, the FBI's querying of unminimized Section 702 content dwarfs the cumulative querying totals of the NSA, CIA and

[152] 2023 DNI Statistical Transparency Report, *supra* note 57, at 24.
[153] *Id.* at 22-25; 2022 DNI Statistical Transparency Report, *supra* note 74, at 19-22.

NCTC.[154] This is a reflection, at least in part, of the FBI's unique role in both foreign counterintelligence and law enforcement,[155] but Section 702 critics have long condemned and continue to accuse the FBI of improperly accessing the content collected under Section 702 for law enforcement purposes using these so-called back door searches.[156]

Since Section 702's 2017 reauthorization, support for those back door search accusations can arguably be found in FISC opinions that, pursuant to congressional mandate,[157] have been redacted and released by the DNI and reflect the FISC's review of Section 702 certifications submitted by the government subsequent to the addition of the querying requirements.[158] A significant focus of repeated concern expressed in those FISC opinions is the querying practices of the FBI.[159] The FISC has stressed that querying the Section 702 Database when conducted to find evidence of crime at an early stage of a criminal investigation that is unrelated to national security likely implicates Fourth Amendment concerns, implying that there may be limits to

[154] *See* Memorandum Opinion and Order [Caption Redacted], [Docket No. Redacted], at *66 (FISA Ct. Oct. 18, 2018) (Boasberg, J.), https://perma.cc/8NR9-ZVVX [hereinafter *2018 Boasberg Opinion and Order*] ("In 2017, NCTC, the CIA, and NSA collectively used approximately 7500 terms associated with U.S. persons to query content information acquired under Section 702 while during the same year FBI personnel on a single system ran approximately 3.1 million queries against raw FISA-acquired information, including section 702-acquired information.").

[155] 2023 DNI Statistical Transparency Report, *supra* note 57, at 22.

[156] *See, e.g.*, Goitein, *supra* note 132.

[157] 50 U.S.C. § 1872(a).

[158] *See, e.g. 2020 Boasberg Opinion and Order, supra* note 79; Memorandum Opinion and Order [Caption Redacted], [Docket No. Redacted] (FISA Ct. Dec. 6, 2019) (Boasberg, J.), https://perma.cc/7JU5-CCFM [hereinafter *2019 Boasberg Opinion and Order*]; *2018 Boasberg Opinion and Order*, *supra* note 154.

[159] *See, e.g.*, *2020 Boasberg Opinion and Order*, *supra* note 79, at *39 ("[T]he FBI's failure to properly apply its querying standard when searching Section 702-acquired information was more pervasive than previously believed."), *42 ("[T]he government has reported numerous incidents involving U.S.-person queries that were designed to return evidence of crime unrelated to foreign intelligence … [but] the government has never applied to the FISC for an order under Section 702(f)(2)"); *2019 Boasberg Opinion and Order*, *supra* note 158, at *69 ("The government has never applied to the FISC for an order under Section 702(f)(2), but FBI personnel have violated Section 702(f)(2) by accessing Section 702-acquired contents returned by a query under circumstances in which they were required to first obtain such an order."); 2018 *Boasberg Opinion and Order*, *supra* note 154, at *72 ("Of serious concern, however, is the large number of queries evidencing a misunderstanding of the querying standard—or indifference toward it.").

judicial acceptance as "reasonable" of the large volume of incidental collection of USP communications that inevitably accompanies programmatic Section 702 collection.[160]

The FISC's consternation with the perpetual compliance problems surrounding the FBI's querying procedures represents an Achilles heel on which Section 702 critics, within and outside Congress, already are capitalizing to demand changes during the 2023 reauthorization debate.[161] The danger posed to Section 702's renewal in a form that perpetuates its irreplaceable value as an intelligence tool by these ongoing FBI compliance problems should be apparent—particularly their potential to undermine the Fourth Amendment "reasonableness" analysis that furnishes the essential predicate for the compliance architecture of the Section 702 program. Executive branch concern about the potential difficulties posed by these compliance issues is reflected in the expanded discussion found in the letter from the Attorney General and the DNI to congressional leadership urging reauthorization of Section 702 which emphasizes, at considerably greater length than in 2017, the "robust privacy and civil liberties safeguards" and "comprehensive oversight regimen" governing the operation of the Section 702 program.[162]

In 2017, these allegations of back door searches of the Section 702 Database by the FBI were largely a theoretical challenge mounted by privacy and civil liberties advocates with no documented scope of either the number of those back door searches or the manner in which those queries were conducted. Now, the back door search issue has resurfaced at precisely the time when a series of redacted FISC opinions have confirmed both the FBI's enduring Section 702 compliance problems and, according to critics, its continued evasion of the F(2) querying

[160] *2020 Boasberg Opinion and Order*, *supra* note 79, at *49; *2019 Boasberg Opinion and Order*, *supra* note 158, at *73.
[161] *See, e.g.*, Goitein, *supra* note 132.
[162] *Compare* 2023 Letter, *supra* note 100, *with* 2017 Letter, *supra* note 99 (The 2023 Garland/Haines letter affords considerably greater focus to addressing privacy protections and comprehensive oversight associated with the Section 702 program.).

requirement that Congress added to Section 702 in 2017 for the very purpose of addressing the back door search issue. Not surprisingly, despite the PCLOB's assessment that any evaluation of the Section 702 program "must consider the program *as a whole*," these opponents tend to isolate this back door search issue, extract it from the holistic "totality of the circumstances" analysis that courts and the PCLOB have relied upon in concluding Section 702 meets the Fourth Amendment touchstone of reasonableness, and characterize the FBI's failings as a constitutional deficiency requiring changes that prospectively pose a significant impediment to the continued effective functioning of the nation's most valuable foreign intelligence collection asset.[163]

The "Rule of Construction" included by Congress in the querying standards found in Section 702(f) affords considerable discretion to FBI querying practices, but even those who recognize Section 702's critical utility as a foreign intelligence tool and the importance of its reauthorization must acknowledge a level of discomfort in the FBI's compliance record as reflected in the series of publicly available FISC opinions. The FBI's Querying Procedures require that any query conducted using a USP query term that is not designed to find and extract foreign intelligence information (*i.e.*, a query of the Section 702 Database that is being initiated to find evidence of a crime) "follow the procedures in subsection 702(f)(2) of FISA before accessing the contents of communications retrieved by such queries in connection with a predicated criminal investigation that does not relate to the national security of the United States."[164] In practice, however, the undeniable problem is that the FBI repeatedly does not comply with either the statutory mandate found in Section 702(F)(2) or with its own Querying Procedures.[165]

[163] PCLOB Report, *supra* note 24, at 93 (emphasis in original).
[164] 2020 FBI Querying Procedures, *supra* note 49, § IV.A.2.
[165] *See generally Muhtorov*, 20 F.4th; Hasbajrami, 945 F.3d; *Mohamud*, 843 F.3d (recounting FBI compliance violations).

It is apparent that the FISC views those situations where the FBI is using USP query terms and reviewing the contents of the Section 702 Database extracted by those query terms for evidence of a crime as representing "the subset of queries that are particularly likely to result in significant intrusions into U.S. persons' privacy."[166] Indeed, the FISC separately requires that the FBI report on a quarterly basis the number of USP queries run by the FBI against the Section 702 Database in which the post-query documented justification for the query indicates "evidence of crime-only" purpose.[167] Consequently, it is perplexing that, in the face of the FBI's pervasive querying problems as documented in the redacted FISC opinions, unlike the NSA, CIA and NCTC, the FBI's Querying Procedures do not require its personnel to memorialize their reasons for believing that a USP query of the Section 702 Database is reasonably likely to return foreign intelligence information before actually initiating the query.[168] Instead, the FBI's Querying Procedures permit the analyst to run the USP query term, extract the responsive contents, and then "provide a written statement of facts showing that the query was reasonably likely to retrieve foreign intelligence or evidence of a crime."[169] Equally perplexing, unlike, for example, NSA which requires that the use of any USP query term be accompanied by a statement of facts that is approved by the NSA Office of General Counsel establishing that the identifier is reasonably likely to extract foreign intelligence information, there is no requirement in the FBI

[166] Memorandum Opinion and Order [Caption Redacted], [Docket No. Redacted], at *73 (FISA Ct. Dec. 6, 2019) (Boasberg, J.), https://perma.cc/7JU5-CCFM; 2018 *Boasberg Opinion and Order*, *supra* note 154 at *93.
[167] 2023 DNI Statistical Transparency Report, *supra* note 57, at 27.
[168] *2018 Boasberg Opinion and Order*, *supra* note 154, at *73-74; *compare* William P. Barr, *NSA 2020 § 702 Querying Procedures*, FOREIGN INTEL. SURVEILLANCE CT. § IV.A. (2020), https://perma.cc/82H8-7XDR [hereinafter 2020 NSA Querying Procedures], *with* 2020 FBI Querying Procedures, supra note 49, IV.A.2-3.
[169] 2020 FBI Querying Procedures, *supra* note 49, § IV.A.3.

Querying Procedures that the written statement prepared post-query by the FBI analyst be subjected to any legal review or approval mechanism before those contents are reviewed.[170]

The FBI has initiated a series of measures intended to improve its querying practices with respect to the use of USP query terms,[171] and the DNI's recently issued 2023 Annual Statistical Transparency Report arguably supports the view that the publicized remediation efforts directed at improving the FBI's Section 702 compliance record have produced measurable improvements.[172] As the Transparency Report explains, the bulk of the FBI's compliance-related changes were implemented in the second half of 2021, so CY 2022 represents the first year in which the full impact of those remediation efforts is reflected, and the statistics show a sizeable decrease in the FBI's use of U.S. person queries—119,383 USP queries in CY 2022 as compared to 2,964,643 in CY 2021 and 852,894 in CY 2020.[173]

Nonetheless, given the documented scope of the FBI's earlier querying problems, Congress will almost certainly consider, again, whether further action directed towards the FBI's querying of the Section 702 Database using USP query terms is needed. Should Congress move in this direction, prudence dictates that any legislative revisions of Section 702 should be directed exclusively towards the FBI and its use of USP query terms that are not designed to find and extract foreign intelligence information. By way of example, Congress might consider the following: (1) similarly to the crimes limitations for which electronic surveillance can be used for law enforcement purposes,[174] Congress could specifically limit the FBI's use of information

[170] *Compare* 2020 NSA Querying Procedures, *supra* note 168, § IV.A., *with* 2020 FBI Querying Procedures, *supra* note 49, § IV.A.3, IV.B.3 (The FBI requires only that written statements of fact be maintained "in a manner that will allow NSD and ODNI to conduct oversight and compliance in an effective manner.").
[171] 2023 DNI Statistical Transparency Report, *supra* note 57, at 23.
[172] *Id.* at 22-25.
[173] *Id.* at 23-24.
[174] 18 U.S.C. § 2516.

derived from Section 702 to "foreign intelligence crimes"[175] to ensure a tighter nexus between Section 702's foreign intelligence purpose and any prosecutions based, in whole or in part, on Section 702-derived information; (2) Congress might reexamine the "Rule of Construction" found in Section 702(f)(2)(F)[176] with a view towards allowing access to the Section 702 Database only in connection with predicated FBI investigations, but not with assessments; and/or (3) analogizing to the querying procedures used by NSA,[177] Congress could require that the employment of any USP query term used solely to find and extract evidence of crime receive prior review and approval by the FBI Office of General Counsel.

These measures, singularly or in concert, might be combined with statutory restrictions on Section 702's access within the FBI and increased reporting and compliance mandates to protect the privacy interests implicated by Section 702's admittedly significant incidental collection of USP communications. Critically, however, such reform efforts should be approached with a scalpel and tailored to ensure that the overridingly important foreign intelligence value of Section 702 is not compromised.

2. Congress should require NSA to delete communications that are exclusively between USPs and obtain a court order to retain conversations to which a USP is a party.[178]

As a purely legal matter, there is nothing that Congress must do during this particular reauthorization cycle to "make" Section 702 constitutional because the courts have repeatedly and uniformly concluded that Section 702 *is* constitutional. Nonetheless, the fluidity of the concept of reasonableness in the digital age that arguably has been reflected in some of the

[175] By way of example, criminal activity involving sabotage, international terrorism, clandestine intelligence gathering, and weapons proliferation represent crimes where foreign intelligence information would be particularly relevant.
[176] 50 U.S.C. § 1881a(f)(2)(F).
[177] 2020 NSA Querying Procedures, *supra* note 168, § IV.A.
[178] *See, e.g.*, Donohue, *Case for Reform*, *supra* note 132.

Supreme Court's more recent Fourth Amendment jurisprudence will surely elicit calls from opponents that the scope of incidental collection of USP communications that is an inevitable corollary of targeting foreigners abroad renders Section 702 collection an "unreasonable" search and seizure under the Fourth Amendment.[179]

Before embarking upon a more extensive discussion of the incidental collection issue, it bears noting as an initial matter that, since Section 702 prohibits both targeting any person inside the United States and targeting any USP located outside the United States,[180] any communication exclusively between USPs would not constitute an authorized acquisition and would not satisfy the standards for retention in NSA's minimization procedures.[181] Where information of or concerning USPs does not meet the retention standards under NSA's Minimization Procedures, those Procedures require that the communication be destroyed upon recognition.[182]

The broader issue of incidental collection has been raised in each of the prior debates over the reauthorization of Section 702 in 2012 and 2017 without Congress acting to restrict the scope of authorized acquisitions. However, two more recent Fourth Amendment decisions by the Supreme Court in the area of data privacy may energize civil libertarians and privacy advocates to argue that the Court is recognizing that technology and the expanding digital universe have made privacy intrusions more significant when government actors have access to digital information, and this increased access facilitated by digital technology must be balanced by an interpretation of the Fourth Amendment that affords greater protection to privacy interests.

In *Riley v. California*, the Court declined to extend the scope of a search incident to an arrest to include the authority of arresting officers to both physically secure an arrestee's cellular

[179] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206 (2018).
[180] 50 U.S.C. § 1881a(b)(1), 1881a(b)(3).
[181] *See* 2020 NSA Minimization Procedures, *supra* note 48, § 7(a).
[182] *Id.* § 4(b)(1).

telephone and search the data contained within that phone.[183] The Court specifically noted the material differences between physical records on cards or pieces of paper versus the trove of data available on even the most basic of cell phones, observing that there is "an element of pervasiveness that characterizes cell phones but not physical records."[184] Aside from the very different circumstances distinguishing a search incident to arrest from the lawful collection of communications acquired by targeting a foreigner pursuant to a FISC-approved Section 702 certification, in *Riley*, the government had possession of the cell phone but no way to access the communications contained in that phone other than by intruding into the cell phone itself. Conversely, in a Section 702 acquisition, the Section 702 Database contains the actual communications lawfully collected and now stored in that government-controlled depository. In other words, the government is retrieving the communications from its own Database—not from a device in which a possessory interest is held by another.

Subsequent to *Riley*, the Supreme Court considered the issue of whether the government's monitoring of cell site location information (CSLI) without a warrant violated the Fourth Amendment.[185] Acknowledging that "individuals have a reasonable expectation of privacy in the whole of their physical movements," the Court concluded that "the seismic shifts in digital technology that made possible the tracking of Carpenter's movements" dictated that the government's acquisition of the CSLI from Carpenter's cellular service provider constituted a Fourth Amendment search requiring a warrant supported by probable cause.[186] Significantly, in *Carpenter*, the Court emphasized that its decision was a "narrow one" while specifically disclaiming that it was intended to impact "other techniques involving foreign affairs or national

[183] Riley v. California, 573 U.S. 373, 393-95 (2014).
[184] *Id.*
[185] *Carpenter*, 138 S. Ct. at 2220.
[186] *Id.* at 2221.

security."[187] Without pretending to know precisely what "other techniques" the Court's disclaimer was intended to embrace, Section 702, as it happens, is a surveillance program using such "other techniques" involving the "national security."

In drafting Section 702, Congress clearly contemplated the incidental collection of communications between a USP and a non-USP located outside the United States, as well as communications of non-USPs outside the United States that may contain information about USPs.[188] Congress forbade the targeting of USPs, but not the incidental collection of USP communications acquired during a lawful Section 702 surveillance, and Congress has preserved that distinction through each of the prior Section 702 reauthorizations that preceded the sunset now scheduled for December 31, 2023.[189]

Instead, Congress predicated the statutory construct of Section 702 upon accepted doctrine that a reasonable search or seizure meets the requirements of the Fourth Amendment, and then created a statutory and compliance architecture satisfying that standard under which the Section 702 program operates with targeting, minimization, and querying procedures that afford USP communications privacy protections consistent with the government's need to obtain, produce, and disseminate foreign intelligence.[190] This architectural balance of Section 702 has been repeatedly confirmed as fulfilling the Fourth Amendment standard of reasonableness even in the context of the significant scope of incidental collection that Congress recognized to be a

[187] *Id.*
[188] PCLOB Report, *supra* note 24, at 82-83.
[189] *See id.* (citing S. REP. NO. 112-174, at 8 (2012)) (describing how the legislative history of Section 702 reflects the congressional understanding of the "inevitability" of incidental collection, and the legislative response in the form of "FISA court review and approval of procedures to minimize the acquisition, retention and dissemination of nonpublicly available information concerning unconsenting U.S. persons.").
[190] *Id.* at 83 (quoting the Senate Intelligence Committee's recognition that "it is simply not possible to collect intelligence on the communications of a party of interest without also collecting communications with whom, and about whom, that party communicates, including in some cases non-targeted U.S. persons").

feature of programmatic Section 702 collection.[191] Neither of the Supreme Court's recent law enforcement rulings should persuade Congress to abandon its consistent approach to the issue of incidental collection as practiced over 15 years and through two reauthorizations of Section 702.

Since Section 702 was enacted, there has been an enduring debate among courts and commentators over the scope of the Fourth Amendment's application to the acquisition and querying stages of the process by which Section 702 produces foreign intelligence where that process involves incidentally collected USP communications. Courts considering the issue in the context of Section 702 have consistently concluded that such incidental collection is lawful (or rather, constitutional) where the communication has been acquired through an authorized acquisition targeting a foreigner reasonably believed to be located outside of the United States.[192]

Concerns over the use of USP query terms to query the Section 702 Database of lawfully acquired communications, however, have led some commentators and one federal appeals court to call for a Fourth Amendment analysis of incidentally collected USP communications under Section 702 that examines both the initial acquisition of the communication, and any subsequent extraction of that communication from the Section 702 Database using a USP query term, as separate events—each of which must satisfy the Fourth Amendment.[193] Other courts and analyses have concluded that queries are not separate searches for Fourth Amendment

[191] *See, e.g.*, In re Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (*Directives*), 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008) (concluding the prophylactic protections incorporated into any Section 702 surveillance coupled with the vital nature of government's national security interest outweighs the intrusion upon individual privacy interests satisfying the Fourth Amendment's reasonableness standard).
[192] *See, e.g.*, United States v. Muhtorov, 20 F.4th 558, 599-600 (10th Cir. 2021) ("[W]hen surveillance is lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons' communications with the targeted person is also lawful."); *see also id.* at 1015 ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.").
[193] *See* Brittany Adams, Comments, *Striking a Balance: Privacy and National Security in Section 702 U.S. Person Queries*, 94 WASH. L. REV. 401 (2019); United States v. Hasbajrami, 945 F.3d 641, 669-73 (2d Cir. 2019).

purposes.[194] Most significantly, the FISC has rejected the position that the "querying of information lawfully acquired under Section 702 be considered a distinct Fourth Amendment event requiring a reasonableness determination independent of the other circumstances of acquisition."[195] Notably, one commentator, having opined that "queries are most accurately viewed as searches under the Fourth Amendment," proceeded to conclude "U.S. person queries are reasonable searches based on the minimization safeguards in place, the limited U.S. person information collected, and the foreign intelligence nexus of acquired data."[196]

In *U.S. v. Hasbajrami*, the Second Circuit, in dicta, embarked on a peripatetic inquiry culminating in the expressed view that querying should be considered "a separate Fourth Amendment event."[197] In attempting to elucidate the reasoning for its conclusion, the court acknowledged that "much would depend on who is querying the database" while admitting that it lacked the information necessary to make such a determination.[198] In the course of its analytic odyssey, the court included citations to the Supreme Court holdings in both the *Riley* and *Carpenter* decisions, notwithstanding that the first case, as noted earlier, was a criminal prosecution involving the search incident to arrest exception to the warrant requirement, and the second (*Carpenter*) is a decision specifically disclaiming any impact on "collection techniques involving foreign affairs or national security."[199] Significantly, since the Second Circuit decision

[194] *See* United States v. Mohamud, No. 3:10-cr-475-KI-1, 2014 WL 2866749, at *26 (D. Or. June 24, 2014), *aff'd,* 843 F.3d 420 (9th Cir. 2016) ("[S]ubsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make a § 702 search unreasonable under the Fourth Amendment."); *see also* Rachel G. Miller, *FISA Section 702: Does Querying Incidentally Collected Information Constitute a Search Under the Fourth Amendment?*, 95 NOTRE DAME L. REV. REFLECTION 139, 154 (2020) ("[Q]ueries are not separate searches for Fourth Amendment purposes.").
[195] Memorandum Opinion and Order [Caption Redacted], [Docket No. Redacted], at *86-87 (FISA Ct. Oct. 18, 2018) (Boasberg, J.), https://perma.cc/8NR9-ZVVX.
[196] Adams, *supra* note 193, at 437.
[197] *Hasbajrami*, 945 F.3d at 669-73.
[198] *Id.*
[199] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

in *Hasbajrami,* the FISC has twice considered whether the querying of the Section 702 Database using a USP query term represents a separate Fourth Amendment event and concluded, each time, that the protection of the privacy interests associated with the use of USP query terms is properly addressed by examining the reasonableness of the procedures governing any particular Section 702 surveillance "as a whole."[200]

Requiring the government to obtain a court order simply to retain any USP communication incidentally acquired during lawful Section 702 acquisitions would disruptively distort the congressional design of the Section 702 program that regulates the acquisition and handling of incidentally acquired USP communications. Under traditional FISA, a USP can be targeted for surveillance only if there is probable cause demonstrating that the USP is an agent of a foreign power, but any incidentally acquired communications of those USPs who are not targets of that surveillance are retained and disseminated in accordance with the minimization procedures approved by the FISC as part of that surveillance—no separate "retention" or "querying" court order is required. [201] The same approach governs the handling of incidentally acquired communications collected under an electronic surveillance executed under Title III – minimization is accomplished without the requirement of a separate court order. In structuring Section 702, Congress adopted this same approach with regard to the acquisition of USP communications incidentally acquired through collection directed at a Section 702 target – *i.e.*, privacy and civil liberties concerns are addressed through the use of court-approved targeting, minimization, and querying procedures without the need for a separate court order.

[200] Memorandum Opinion and Order [Caption Redacted], [Docket No. Redacted], at *66 (FISA Ct. Apr. 21, 2022) (Contreras, J.), https://perma.cc/72F3-RM9C; s*ee also* Memorandum Opinion and Order [Caption Redacted], [Docket No. Redacted], (FISA Ct. Apr. 11. 2023) (Contreras, J.), https://perma.cc/TS3Q-6LG2.
[201] *See* 50 U.S.C. § 1801(b)(2).

Moreover, the mechanics of Section 702 collection make any separate order mandate operationally problematic. The vast content of raw Section 702 traffic is labeled and stored in authorized repositories and is accessed in response to queries designed to produce foreign intelligence information.[202] Queries represent the trigger initiating retrieval of communications from that Section 702 Database, the first point at which a communication is identifiable as one of or concerning a USP, and no credible argument has been advanced that justifies requiring a court order simply to retain an incidentally required USP communication in the Section 702 Database.[203] Prior to this point in the analytic process, nothing in the unminimized Section 702 Database specifically identifies the existence of any particular communication as one to which a USP is a party. Consequently, requiring a court order as a prerequisite to retaining any particular "USP communication" before any query is initiated extracting such a USP communication from the Section 702 Database puts the cart before the proverbial horse, and renders the retention of those communications for foreign intelligence purposes unworkable.

Critics remain undeterred, however, insisting that queries of the Section 702 Database using USP query terms be viewed as separate Fourth Amendment events that can be undertaken only upon a showing of probable cause[204]—either the law enforcement warrant standard where the query is initiated to find evidence of a crime, or, as one commentator insists, the standard governing a FISA Title I surveillance order against a USP as an agent of a foreign power in those

[202] 2020 NSA Minimization Procedures, *supra* note 48, § 2(c).
[203] *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 548 (2005) ("In the context of digital searches, courts often consider the moment when data is 'exposed to human observation' to be the relevant point for determining whether a search occurred.").
[204] *See, e.g.,* PRIV.& C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE ACT A-2 (2023), https://documents.pclob.gov/prod/Documents/OversightReport/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf, [hereinafter PCLOB Report II] (PCLOB Chair calls for use of probable cause standard before the government is permitted to view the contents of USP communications retrieved from the Section 702 Database using a USP query term).

circumstances where the query is designed to find and extract foreign intelligence information.[205] Section 702's querying rules already establish the probable cause standard for USP queries that are not designed to find foreign intelligence information in predicated criminal investigations not related to the national security—that is the F(2) querying standard.[206] But even accepting the debatable premise that searching the Section 702 database of communications *already lawfully acquired* under the authority of a FISC-approved Section 702 certification constitutes yet another search, the Fourth Amendment's "reasonableness" standard simply does not require a FISA Title I order to use a USP query term to find and extract foreign intelligence information.

NSA, the focal point for Section 702 collection, is a foreign intelligence agency with no law enforcement mission. Significantly, in terms of the Fourth Amendment analysis, the NSA Querying Procedures approved by the FISC as meeting the requirements of the Fourth Amendment provide that the *only* purpose for which NSA analysts can query the Section 702 Database is to retrieve foreign intelligence information.[207] Courts have recognized that this foreign intelligence focus triggers an entirely different "reasonableness" assessment under the Fourth Amendment than that used either for law enforcement purposes or to assess whether a USP can be targeted as an "agent of a foreign power" under FISA Title I. This analysis recognizes both the existence of a foreign intelligence exception that exempts the query from the law enforcement-based warrant requirement, and that the application of court-approved minimization and querying procedures serves to make the query's intrusion into individual

[205] Goitein, *supra* note 132.
[206] 50 U.S.C. §1881a(f)(2).
[207] 2020 NSA Querying Procedures, *supra* note 168, § IV.A.

privacy interests "reasonable" when balanced against the government's interest in national security—an interest repeatedly recognized by the courts as being of the "highest order."[208]

Once identified and extracted from the unminimized Section 702 Database by use of such a query term, that USP communication will then be retained and disseminated only in accordance with the NSA Minimization Procedures that have been approved by the FISC as conforming with the Fourth Amendment both in form and in actual practice.

Separately, the significant adverse practical consequences that would accompany requiring a FISA Title I order before using a USP query term to find foreign intelligence information in the Section 702 Database cannot be overlooked. The Fourth Amendment reasonableness analysis that accepts the architecture of targeting, minimization, and querying procedures as the proxy for a warrant by furnishing acceptable privacy protections in connection with querying the Section 702 Database also recognizes as reasonable the government's need for "speed, stealth, and secrecy" in its pursuit of foreign intelligence to protect the national security.[209] The debilitating impact that would result from requiring a FISA Title I order whenever a USP query term is used to find and extract foreign intelligence from the Section 702 Database is starkly demonstrated by these numbers: in CY 2022, the FISC issued a total of 337 orders authorizing FISA Title I surveillances while NSA, CIA, and the NCTC conducted 8,340 queries of the Section 702 database using USP query terms designed to find and extract foreign intelligence.[210] Requiring the government to seek a FISA Title I court order for these 8,340

[208] In re Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (*Directives*), 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008).
[209] United States v. Muhtorov, 20 F.4th 558, 599-600 (10th Cir. 2021).
[210] 2023 DNI Statistical Transparency Report, *supra* note 57, at 12, 20-21.

queries would overwhelm the 11 members of the FISC and cripple the Intelligence community's ability to use Section 702 to provide crucial intelligence to policy makers on a timely basis.[211]

Assuming, hypothetically, that both the acquisition *and* querying of Section 702-acquired communications represent independent events triggering the Fourth Amendment, the proper analytic focus should examine the purpose of the query and the reasonable likelihood that the query will find and extract foreign intelligence information—and reject any interpretation that looks to impose a requirement for any court order where the query possesses this foreign intelligence nexus.

At this point, the extensive executive branch oversight of Section 702 deserves mention. Every feature of the Section 702 Program is subject to a plethora of oversight regimens and reporting requirements. By way of example, at NSA, which initiates all Section 702 collection,[212] that oversight begins internally where the Director of Compliance, the Director of Civil Liberties and Privacy, the Inspector General, the General Counsel, and embedded compliance elements within NSA's operational directorates join in an enterprise-wide compliance structure.[213] Any compliance incidents, whether in the form of inappropriate queries, database errors, detasking errors, or typographical mistakes, are reported to the National Security Division at the Department of Justice (DOJ/NSD) and the Office of the Director of National Intelligence (ODNI).[214] Additionally, as required by statute, NSA completes and delivers to the congressional intelligence and judiciary committees an annual review of the Section 702 program detailing: (1) an accounting of the number of intelligence reports containing reference to a USP identity; (2) an

[211] 50 U.S.C. § 1803(a).
[212] PCLOB Report, *supra* note 24, at 7.
[213] NAT'L SEC. AGENCY, DIR. OF C.L. & PRIV. OFF., NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702 9 (2014), https://perma.cc/53KV-YWH2.
[214] *Id.*

accounting of the number of USP identities subsequently disseminated in response to identity requests relating to intelligence reports where the identity was initially masked; (3) the number of targets that were later determined to be in the United States; and (4) a description of any procedure developed by NSA and approved by the DNI to assess, consistent with privacy rights and with national security and operational needs, the extent to which acquisitions authorized under the Section 702 Program acquire the communications of USPs.[215]

NSA is required to document on "tasking sheets" every targeting decision made under its targeting procedures, and DOJ/NSD conducts post-tasking review of every tasking sheet furnished by NSA.[216] Additionally, DOJ/NSD and ODNI conduct bimonthly reviews of NSA's application of its minimization procedures focusing particularly on dissemination and queries using USP identifiers.[217] The results of these targeting and minimization reviews are reported to Congress both in NSA's annual review[218] and in the *Joint Assessments* that also are furnished to the FISC.[219]

All of the foregoing represents an ongoing compliance structure documented in a recurring series of detailed reporting mandates. Aside from this oversight regimen, after its own independent, exhaustive and comprehensive review of Section 702, the PCLOB concluded that "the Board has seen no trace of any such illegitimate activity associated with the program, or any attempt to intentionally circumvent its limits."[220] By way of corroboration, the twenty-four separate semi-annual *Joint Assessments* have never reported an intentional violation

[215] 50 U.S.C. § 1881a(m)(3).
[216] PCLOB Report, *supra* note 24, at 70; U.S. DEP'T OF JUST. & OFF. OF THE DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 8 (2021), https://perma.cc/5XFK-3U8Z (covering the period December 1, 2019 – May 31, 2020).
[217] PCLOB Report, *supra* note 24, at 72.
[218] 50 U.S.C. § 1881a(m)(3).
[219] *Id.* § 1881a(m)(1)(A).
[220] PCLOB Report, *supra* note 24, at 11.

of the minimization or querying procedures approved by the FISC and employed in connection with every authorized Section 702 acquisition.

This entire operational and oversight process represents precisely the flexibility that the Supreme Court, in *Keith*, envisioned as being both consistent with the Fourth Amendment and responsive to the vital governmental interest in protecting the national security.[221] A new, ill-advised requirement that the government obtain a separate court order simply to retain any USP communication incidentally acquired during an authorized Section 702 acquisition, or a separate court order before initiating a query of the Section 702 Database using a USP query term, would materially impair the critical intelligence advantages that Congress intended the Section 702 program to supply to the nation's security.[222]

3. Section 702 operates as a "general warrant" prohibited by the Fourth Amendment.[223]

The Fourth Amendment handles the concern over the use of general warrants by requiring that warrants describe with particularity the place to be searched and the person or thing to be seized.[224] Section 702 operates without a warrant requirement but, focusing on "reasonableness" as the touchstone of Fourth Amendment analysis, Congress instead requires a matrix of procedural mechanisms—targeting procedures, minimization procedures, querying procedures, and guidelines—that collectively serve as a proxy for the particularity requirements of a warrant and which, themselves, must comply with the Fourth Amendment. The targeting procedures and guidelines limit targeting to foreigners reasonably believed to be located outside of the United States while assuring that no Section 702 acquisition is conducted without a

[221] United States v. U.S. District Court (*Keith*), 407 U.S. 297, 323-24 (1972).
[222] *But see* PCLOB Report II, *supra* note 204, *at* 205-208, A-3; *see also* PRESIDENT'S INTEL. ADVISORY BD. & INTEL. OVERSIGHT BD., REVIEW OF FISA SECTION 702 AND RECOMMENDATIONS FOR REAUTHORIZATION 35-37 (2023), https://perma.cc/H8LC-RXPV [hereinafter PIAB Report] (noting the absence of any constitutional requirement for a court order related to querying and recommending against such a mandate).
[223] *See, e.g.*, Donohue, *Case for Reform*, *supra* note 132.
[224] U.S. CONST. amend. IV.

certification reviewed by the FISC and that no communication is intentionally acquired where both the sender and all recipients are located in the United States.

The minimization and querying procedures ensure that queries of the Section 702 Database "must be reasonably likely to retrieve foreign intelligence information as defined in FISA."[225] Since only NSA may initiate Section 702 collection, attention is best focused on NSA's Minimization and Querying Procedures.[226] At NSA, every USP query term used to select Section 702-acquired content must be accompanied by a statement of facts, approved by the NSA Office of General Counsel, demonstrating that the query is reasonably likely to retrieve foreign intelligence information.[227] Other minimization restrictions require that information of or concerning USPs be destroyed at the earliest practicable point at which such information can be identified as clearly not relevant to the authorized purpose of a Section 702 acquisition.[228] Every communication that does not have at least one communicant outside the United States is considered a "domestic communication" and, subject to very narrow exceptions, is destroyed upon recognition.[229] Subject to limited exceptions requiring approval by the Director of NSA's Operations Directorate, foreign communications (those having at least one communicant outside the United States) of or concerning USPs must be destroyed within 5 years from the date of the certification providing the authority under which they were collected.[230] Additionally, where USP queries do produce analytically valuable foreign intelligence information, any subsequent dissemination of that foreign intelligence must use generic identifiers so that the information

[225] 2020 NSA Querying Procedures, *supra* note 168, § IV.A.
[226] PCLOB Report, *supra* note 24, at 42 n.164.
[227] 2020 NSA Querying Procedures, *supra* note 168, § IV.A.
[228] 2020 NSA Minimization Procedures, *supra* note 48, § 4(b)(1).
[229] *Id.* § 6.
[230] *Id.* § 7(a)(1).

cannot reasonably be connected with any identifiable USP (termed "masking") unless that identity is necessary to understand the intelligence or assess its importance.[231]

Finally, there is the role of the FISC itself. The FISC is tasked with ensuring that the targeting, minimization, and querying procedures employed with any Section 702 surveillance are consistent with the Fourth Amendment.[232] It does so by examining these procedures both in the form they are presented to the FISC and as they are actually applied in executing the Section 702 acquisition.[233] Consequently, the FISC's approval of a Section 702 certification and its continued oversight of the application of the associated procedures reflect its determination that, as utilized in the acquisitions falling within the parameters of the approved certification, the surveillance satisfies the Fourth Amendment and is not functioning as a general warrant.

All of these elements operate to ensure that Section 702 acquisitions are conducted with a degree of focus and particularity bearing no resemblance to the untrammeled rummaging of a general warrant.

4. Congress should reinstate the "primary purpose" test for FISA surveillance.[234]

As an initial matter, it is important to understand that Congress never established the "primary purpose" test for a FISA surveillance. Courts fashioned the primary purpose test to evaluate when information derived from a FISA surveillance could be used in a criminal prosecution. As applied, the use of FISA-derived information in a criminal case was permitted provided that the primary purpose of the FISA surveillance or search was to collect foreign intelligence information rather than to conduct a criminal investigation or prosecution. The test

[231] *Id.* § 7(b)(2).
[232] 50 U.S.C. § 1881a(j)(3)(A).
[233] *See* Memorandum Opinion and Order [Caption Redacted], [Docket No. Redacted], at *35 (FISA Ct. Nov. 18, 2020) (Boasberg, J.), https://perma.cc/X7VY-P7BC ("FISC review of the sufficiency of Section 702 procedures is not limited to the procedures as written, but also encompasses how they are implemented.").
[234] Donohue, *Case for Reform*, supra note 132.

comes from *U.S. v. Truong Dinh Hung* where the Fourth Circuit, in a pre-FISA decision, concluded that a warrantless surveillance predicated on the President's executive power must have the primary purpose of acquiring foreign intelligence rather than pursuing law enforcement objectives.[235]

Notwithstanding its judicial, as opposed to legislative, origins, certain groups have insisted that FISA is unconstitutional unless construed to prohibit the government from pursuing approval of a FISA application that has criminal prosecution as its quote "primary purpose."[236] As part of the Patriot Act, however, Congress revised FISA to reflect that the acquisition of foreign intelligence must be a "significant purpose" of the surveillance and, in its decision in *In re Sealed Case*, the FISCR confirmed that the significant purpose test satisfied the reasonableness standard of the Fourth Amendment.[237] Elaborating, the FISCR found the primary purpose standard rested on a false premise that, as the government investigation moved to criminal prosecution, its foreign intelligence concerns receded—a supposition that, in the FISCR's view, rested on an "inherently unstable, unrealistic and confusing" demarcation between foreign intelligence and criminal investigative purposes.[238] Indeed, FISA defines key terms like "agent of a foreign power," "sabotage," and "international terrorism" in terms of conduct that violate criminal statutes, and the definition of "foreign intelligence information," the acquisition of which is the *sine qua non* for a FISA application, incorporates these terms predicated upon criminal conduct.[239]

[235] United States v. Truong Dinh Hung, 629 F.2d 908, 915-16 (4th Cir. 1980).
[236] In re Sealed Case, 310 F.3d 717, 722 (FISA Ct. Rev. 2002).
[237] *Id.*
[238] *Id.* at 743.
[239] 50 U.S.C. § 1801(b)-(e).

In its broadest sense, the foreign intelligence function involves the collection, analysis, and subsequent dissemination of information on matters of interest to policy makers. Those matters of interest are identified and prioritized to guide the intelligence collection process while a separate regulatory framework governs the acquisition, retention, and dissemination of the acquired information.

Conversely, intelligence pursued for law enforcement purposes is driven by the objective of prosecuting violations of the criminal laws. Its collection and use are governed by a variety of constitutional, statutory, and regulatory mandates that reflect the compelling public interest in assuring that evidence acquired through law enforcement investigative activities is collected, used, and, where required, disclosed consistently with legal requirements.

Although foreign intelligence collection and law enforcement reflect different disciplines, the pursuit of foreign intelligence information and the prospect that such information will include data that is relevant both to intelligence needs and to the exposure of criminal activity is likely. An increase in the law enforcement value of particular information acquired after an electronic surveillance is initiated for intelligence or counterintelligence purposes does not necessarily reflect a corresponding diminution in intelligence value such that the surveillance inevitably morphs from intelligence collection predominantly to the assembling of prosecutorial evidence. While the objectives of these two disciplines may proceed in parallel, they often arc towards an intersection, particularly where foreign intelligence crimes are involved. The congressional use of "significant purpose" reflects an appropriate measure of the quantum of foreign intelligence purpose needed to have an electronic surveillance measured under the standards currently prescribed in FISA (and Section 702) rather than those prescribed for the distinctly different purposes of law enforcement.

5. Congress must eliminate "abouts" collection.[240]

"Abouts" collection is a feature of NSA's "Upstream" Section 702 surveillance that has persistently offended civil liberties and privacy activists. Only NSA conducts upstream collection, and NSA ended abouts collection in 2017.[241] Congress codified that cessation in the FISA Amendments Act of 2017, and the Limitations in subsection (b) of Section 702 now require that an acquisition "may not intentionally acquire communications that contain a reference to, but are not to or from, a target" of an authorized acquisition; in other words, an acquisition may not acquire abouts communications.[242]

However, while the FISA Amendments Act of 2017 codified NSA's cessation of abouts collection, it did not permanently curtail it. Instead, § 103(b) of the FISA Amendments Act of 2017 provides that, should the Attorney General and the DNI decide to "implement the authorization of the intentional acquisition of abouts communications," they must first provide "written notice" to Congress which sets in motion a 30-day period during which abouts collection may not be initiated while Congress considers and reviews information needed to "fully review the written notice" (including a copy of any certification submitted to the FISC or order issued by the FISC relating to the authorization to initiate such abouts collection).[243]

The 2017 FISA amendments offer little elucidation as to what happens after Congress receives the mandated written notice, and the Attorney General and the DNI have taken no action since Section 702 was last reauthorized to trigger the restrictions on abouts collection. Consequently, the permanent statutory ban on abouts collection demanded by Section 702

[240] *See, e.g.*, Donohue, *Case for Reform*, *supra* note 132.
[241] *See* Press Release, Nat'l Sec. Agency/Cent. Sec. Serv., NSA Stops Certain Section 702 "Upstream" Activities (Apr. 28, 2017), https://perma.cc/HUV5-QUP6 [hereinafter *NSA Stops Certain Section 702 "Upstream" Activities*]. The cessation of "abouts" collection is codified in § 103(b) of the FISA Amendments Act of 2017.
[242] 18 U.S.C. § 1881a(b)(5).
[243] FISA Amendments Reauthorization Act, *supra* note 61, § 103(b).

opponents seems superfluous and myopic. When NSA ceased abouts collection in 2017, it cited "mission needs, current technological constraints, United States person privacy interests, and certain difficulties in implementation" as the reasons for its decision.[244] It is certainly plausible that technological developments potentially resolve both the U.S. person privacy and implementation concerns such that abouts collection might be resumed in a manner that adequately protects those U.S. person privacy interests. Should events coalesce to produce such a circumstance and Congress receives notice of the intention to resume abouts collection, it can then "fully examine the written notice" and determine whether the technological improvements provide the necessary circumstances in which such collection could be resumed consistent with the protection of U.S person privacy interests.

Given the impact on collection capabilities produced by the constant evolution in technology, permanently banning a collection activity of demonstrated intelligence value when that capability might one day be employed in a manner consistent with both intelligence needs and U.S. person privacy interests is imprudent.

6. Section 702 must be amended to provide protections for non-USP privacy interests.

The issue of privacy protections for foreigners who are either targets of, or incidentally collected by, authorized Section 702 surveillance is principally dictated by foreign policy considerations since foreigners do not receive the constitutional protection of the Fourth Amendment. Consequently, these matters, whether considered in the context of international trade and data exchange or as a matter of equitably accommodating the privacy interests of foreigners, are best addressed by the president who is the nation's principal spokesperson in foreign affairs. This is not to suggest that Congress lacks a voice or role to play in the conduct of

[244] *NSA Stops Certain Section 702 "Upstream" Activities*, *supra* note 241.

the nation's foreign policy, but the debate over the reauthorization of the nation's most important intelligence collection program is a vehicle ill-suited to advancing congressional foreign policy objectives.

A comprehensive assessment of national security risks certainly includes not only those threats directed at the nation's defenses but also those risks posed to U.S. relationships with other nations and risks to trade and international commerce. Recognition of these other elements of national security risk does not, however, warrant addressing those risks through FISA with its *raison d'être* of providing the legal framework for electronic surveillance conducted for foreign intelligence purposes.

Multinational efforts to address data privacy issues are reflected in a number of international agreements addressing data access by both private and governmental actors. By way of example, in December 2022, the United States and the other thirty-seven members of the Organization for Economic Cooperation and Development (OECD) finalized a "Declaration on Government Access to Personal Data Held by Private Sector Entities" setting forth agreed upon "Principles" aiming to document the range of protections member governments already have in place for individuals' data they access.[245] The adoption of the Declaration followed the regulatory implementation in March 2022 of the Trans-Atlantic Data Privacy Framework which, in turn, was a direct response to the decision of the European Court of Justice in *Schrems II*.[246]

Notably, in conjunction with the agreement on this new Data Privacy Framework, the United States issued Executive Order 14086 titled "Enhancing Safeguards for U.S. Signals Intelligence Activities."[247] The Executive Order separates signals intelligence activities (which

[245] SEC'Y GEN. OF THE ORG. FOR ECON. COOP. & DEV., DECLARATION ON GOVERNMENT ACCESS TO PERSONAL DATA HELD BY PRIVATE SECTOR ENTITIES 6-8 (2023), https://perma.cc/KV8J-2UE6.
[246] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (*Schrems II*), ECLI:EU:C:2020:559 (July 16, 2020).
[247] Exec. Order No. 14086, 87 Fed. Reg. 62283 (Oct. 7, 2022).

include Section 702 and other electronic surveillance activities conducted under the authority of FISA) into twelve "legitimate objectives"[248] for targeted collection and six for bulk collection,[249] identifies five "prohibited objectives,"[250] and mandates that all U.S. signals intelligence activities be conducted in a manner that is both proportionate and necessary to the validated intelligence priority for which they have been authorized. The Executive Order also establishes minimization procedures for the retention and dissemination of information collected through signals intelligence activities that puts non-U.S. person information on a footing largely compatible with the procedures required for retaining and disseminating USP information. The provisions within E.O. 14086 have furnished sufficient reassurance regarding the handling of non-U.S. person information and data that the European Union published a draft decision finding that transfers made pursuant to the new Data Privacy Framework "adequate" for purposes of EU data protection law.

This framework of international agreements with E.O. 14086 supplying functional implementation that addresses foreign privacy interests within the broader regulation of U.S. signals intelligence activities represents the more coherent approach to addressing foreign data privacy issues. Difficult questions remain requiring resolution in the area of foreign data privacy, but those issues are better addressed through the foreign policy expertise of the executive branch than the likely contentious debate over the reauthorization of Section 702.

THE POLITICAL HEADWINDS FACING SECTION 702 REAUTHORIZATION

[248] *Id.* § 2(b)(1)(A).
[249] *Id.* § 2(c)(ii)(B).
[250] *See id.* § 2(b)(ii) (The prohibited purposes for which signals intelligence activities cannot be conducted are (1) suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press; (2) suppressing or restricting legitimate privacy interests; (3) suppressing or restricting a right to legal counsel; (4) disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation or religion; and (5) collecting foreign private commercial information or trade secrets to afford competitive advantages to U.S. companies.).

As two commentators shrewdly observed when Section 702 last faced renewal in 2017, "start with panicky civil libertarians, sprinkle in some right-wing conspiracy theories about 'unmasking' intelligence, and polish it off with a healthy dose of congressional dysfunction" and the result is "bad surveillance policy in the name of reform."[251] If anything, the current environment for surveillance reform makes 2017 look like the archetype of a prudent legislative process.

In the political climate that now prevails in Congress, Section 702's propensity for attracting a curious opposition coalition populated by privacy advocates, right-wing libertarians, and conspiracy theorists is exacerbated by those in the House of Representatives who are on record as holding the viewpoint that federal law enforcement and national security services have been "weaponized" against them.[252] In early January 2023, a divided House of Representatives voted to authorize a "wide-ranging investigation into federal law enforcement and national security agencies."[253] For those most vigorously advocating this inquiry, the FBI is the ultimate bête noire of those federal agencies, the avatar of the proverbial "Deep State," stemming from a distrust tracing to its involvement in both the investigation into Russian interference in the 2016 election and, more recently, its participation in executing the search warrant at Mar-a-Lago. The level of antipathy among the most strident of these firebrands has even led to calls to dismantle the FBI.[254]

Very little legislation escapes the political tempest that dominates Congress today, and the reauthorization of Section 702, facing opposition from that enduring consortium of privacy

[251] Susan Hennessey and Benjamin Wittes, *Congress Wants to Tie the Intelligence Community's Hands for No Reason*, FOREIGN POL'Y (Oct. 13, 2017, 11:50 AM), https://perma.cc/8FXJ-KBWM.
[252] Luke Broadwater and Catie Edmondson, *Divided House Approves Inquiry into 'Weaponization' of Government*, N.Y. TIMES, Jan. 11, 2023, at A1.
[253] *Id.*
[254] Gregory Svirnovskly, *Gosar, GOP Allies Call for Abolishing the FBI in Response to Mar-a-Lago Search*, ARIZ. REPUBLIC (Aug. 9, 2022, 5:17 PM), https://perma.cc/4R9H-NMTW.

and civil liberties critics, was always going to be a bumpy ride. Certain aspects of the handling of Section 702-acquired information may warrant revisiting but, with the privacy and civil liberties lobby that has historically opposed Section 702 now complemented by a conservative political faction that views the FBI as the principal instrument of a "weaponized" national security and justice system, the challenge for proponents of Section 702 is ensuring that the fundamentally sound Section 702 program is not dismembered. It will take all the persuasive powers of the executive branch, and perhaps then some, to preserve Section 702. Through its performance in the Carter Page FISA application fiasco and given the FISC's criticism of its challenging Section 702 compliance record, the FBI has made itself an irresistible target. [255] It remains for those inside and outside of Congress who recognize the value of Section 702 as an "irreplaceable" intelligence asset to ensure that "reform" efforts do not neuter its indispensable intelligence value.[256] Failure to reauthorize Section 702 in a form that retains that intelligence value will, in the words of the President's Intelligence Advisory Board, represent "one of the worst intelligence failures of our time."[257]

[255] *See, e.g.*, Jordain Carney, *House GOP warns FBI to Stay Out of Controversial Surveillance Talks*, POLITICO (Apr. 25, 2023, 8:39 AM), https://perma.cc/9T5D-7BV6 (According to House Intelligence Committee Chair Mike Turner: "The FBI is absolutely the problem child in FISA and Section 702. The abuses are abhorrent.").
[256] Nakasone, *supra* note 39.
[257] PIAB Report, *supra* note 222, at 2.