American University National Security Law Brief

Volume 7 | Issue 1 Article 1

2017

Strengthen Section 702: A Critical Intelligence Tool Vital to the Protection of Our Country

Deborah Samuel Sills

Follow this and additional works at: http://digitalcommons.wcl.american.edu/nslb

 Part of the National Security Law Commons

Recommended Citation

Sills, Deborah Samuel "Strengthen Section 702: A Critical Intelligence Tool Vital to the Protection of Our Country," American University National Security Law Brief, Vol. 7, No. 1 ().
Available at: http://digitalcommons.wcl.american.edu/nslb/vol7/iss1/1

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University National Security Law Brief by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.

STRENGTHEN SECTION 702: A CRITICAL INTELLIGENCE TOOL VITAL TO THE PROTECTION OF OUR COUNTRY

DEBORAH SAMUEL SILLS*

The rising globalization of terrorist organizations and their ever more sophisticated abilities to reach people throughout the world has deepened the threat of terrorist activities both in the United States and abroad. Recent events show that terrorist groups overseas have influenced homegrown terrorist acts in the United States.[1] Many of these same overseas terrorist

* Intelligence Community Fellow at Georgetown University Law Center, attorney with the Federal Bureau of Investigation, and former Counsel to the President's Intelligence Oversight Board. The views expressed in this article are my personal views and do not necessarily represent the views of any person or entity, including the United States Government. Nothing in the contents of this article should be construed as implying United States Government authentication of information. I especially would like to thank Professor David Koplow for his insightful guidance and encouragement throughout the drafting process. I would also like to thank Professor Laura Donohue, Judge James Baker, Professor James Zirkle, Professor William Buzbee, Tina Zimmerman, Robert Litt, my colleagues, particularly Karen Davis Miller, my husband, Jonathan Sills, and the members of the Georgetown Law Summer Workshop Group for their valuable and helpful comments. I am grateful to Professor Donohue and Susan Gibson for creating the fellowship program between Georgetown University Law Center and the United States Intelligence Community. I appreciate the dedication of the members of the editorial staff of the National Security Law Brief, American University Washington College of Law, particularly Ayat Mujais, for their meticulous review of this article.

[1] Sarah Frostenson, *Most Terrorist Attacks in the US are Committed by Americans – Not Foreigners*, VOX (Sept. 9, 2016) ("Homegrown terrorism commonly refers to terrorist acts committed by a government's own citizens."). *See* Marc Santora, William K. Rashbaum, Al Baker and Adam Goldman, *Ahmad Khan Rahami Is Arrested in Manhattan and New Jersey Bombings*, NEW YORK TIMES (Sept. 19, 2016), http://www.nytimes.com/2016/09/20/nyregion/nyc-nj-explosions-ahmad-khan-rahami.html; (reporting that on September 17, 2016, Ahmad Khan Rahami set off two bombs in New York City and Seaside Park, New Jersey, injuring 29 people); *see also* Marc Santora and Adam Goldman, *Ahmad Khan Rahami Was Inspired by Bin Laden, Charges Say*, NEW YORK TIMES (Sept. 20, 2016), http://www.nytimes.com/2016/09/21/nyregion/ahmad-khan-rahami-suspect.html (reporting that, according to a criminal complaint, Rahami was inspired by international terrorists and was charged with several criminal offenses including use of weapons of mass destruction and bombing a place of public use); *see also* Mitch Smith, *F.B.I. Treats Minnesota Mall Stabbing Attack as "Potential Act of Terrorism*," NEW YORK TIMES (Sept. 18, 2016), http://www.nytimes.com/2016/09/19/us/police-shoot-attacker-in-minnesota-mall-after-8-are-stabbed.html (noting that on September 17, 2016, ISIS claimed responsibility for a stabbing attack at a Minnesota shopping mall, in which nine people were injured); *see also* Asher Klein and Cathy Rainone, *Who is Omar Mateen, Gunman in America's Deadliest Mass Shooting?* NBC4 NEW YORK (June 12, 2016), http://www.nbcnewyork.com/news/local/Who-Omar-Mateen-Suspected-Florida-Nightclub-Gunman-382619981.html (describing that Omar Mateen,

organizations are recruiting thousands of new members from Western countries, including hundreds from the United States.[2] In light of these growing threats, the United States must ensure that our country has the necessary legal authorities to anticipate and counter them. One such vehicle for providing the United States with these critical legal tools is through strengthening Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA).

Information collected pursuant to the FAA Section 702 provides foreign intelligence information that is critical to the protection of the United States against terrorist threats.[3] Members of the Intelligence Community believe

---

a 29-year-old New York-born American citizen and Florida resident, killed 49 people in an Orlando nightclub and wounded 53 others. During the attacks, Mateen pledged allegiance to ISIS); *see also* Faith Karimi, Jason Hanna and Yousuf Basil, *San Bernardino Shooters "Supporters" of ISIS, Terror Group Says*, CNN (Dec. 5, 2015), http://www.cnn.com/2015/12/05/us/san-bernardino-shooting/ (stating that on December 2, 2015, Syed Rizwan Farook, an American citizen born in the United States, and his wife Tashfeen Malik, killed 14 people and wounded 21 in a shooting at a holiday party in San Bernardino, California. Malik posted a pledge of allegiance to an ISIS leader to Facebook).

[2] *See, e.g.*, *Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy and Civil Liberties, Hearing before the Senate Committee on the Judiciary Oversight*, 114th Cong. 5 (2016) (statement of Matthew G. Olsen, Former Director of the National Counterterrorism Center), https://www.brennancenter.org/sites/default/files/analysis/Goitein_Written_Testimony_SJC.pdf [hereinafter Stmt. of Olsen] ("More than 6,000 Europeans – including many French, German, British, and Belgian nationals – have travelled to Syria to join the fight. This is part of the total of approximately 40,000 foreign fighters in the region. Among the Europeans who have left for Syria, several hundred fighters have returned to their home countries, typically battle-hardened, trained, and further radicalized. The number of Americans who have travelled to Syria or Iraq, or have tried to, exceeds 250."); TASK FORCE ON COMBATING TERRORIST AND FOREIGN FIGHTER TRAVEL, U.S. HOUSE OF REPRESENTATIVES, FINAL REPORT OF THE TASK FORCE ON COMBATING TERRORIST AND FOREIGN FIGHTER TRAVEL 6 (2015), https://homeland.house.gov/wp-content/uploads/2015/09/FINAL_2pager1.pdf [hereinafter HOMELAND SECURITY COMMITTEE REPORT]; ANTI-DEFAMATION LEAGUE, AL-SHABAAB'S AMERICAN RECRUITS 1 (2015), http://archive.adl.org/main_terrorism/al_shabaab_american_recruits.html -.V_qDmTuTWV4.

[3] *See* DAVID SHEDD, PAUL ROSENZWEIG, AND CHARLES "CULLY" STIMSON, MAINTAINING AMERICA'S ABILITY TO COLLECT FOREIGN INTELLIGENCE: THE SECTION 702 PROGRAM 1 (Heritage Foundation) (2016) [hereinafter THE SECTION 702 PROGRAM] ("Over the past several years, this surveillance of the online activities of foreigners has been an invaluable source of information for American intelligence professionals and officials."); *see also FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary,* 114th Cong. 8–9 (2016) Jt. Unclass. Stmt., Litt, Evans, Steinbach, Darby, https://web.archive.org/web/20160907202002/https://judiciary.house.gov/wp-content/uploads/2016/02/joint-sfr-for-doj-fbi-odni-and-nsa-updated.pdf; Permanent Select Comm. on Intelligence, U.S. House of Representatives, FISA Amendments Act

that Section 702 collection offers valuable insights into the plans, objectives, and operations of terrorist organizations.[4] For example, the NSA considers information acquired under Section 702 as the "most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."[5] Likewise, the former director of the National Counterterrorism Center (NCTC), Mathew G. Olsen, testified that "Section 702 collection was instrumental to our efforts to discern the intentions and capabilities of our terrorist adversaries, contributing both to our strategic judgments and tactical insights."[6] Congress also recognizes that the intelligence obtained under Section 702 is essential to our national security,[7] observing that this information is "often unique, unavailable from any other source, and regularly provides critically important insights and operationally actionable intelligence on terrorists and foreign intelligence targets around the world."[8]

Information acquired from Section 702 has aided the government's efforts in preventing potential terrorist attacks. For example, in September 2009, information acquired pursuant to Section 702 was instrumental in

---

Reauthorization Act of 2012, H.R. Rep. No. 112-645 Part 2, at 2 (2012), https://www.congress.gov/congressional-report/112th-congress/house-report/645/2; *see also* NAT'L SEC. AGENCY, NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHT AND PARTNERSHIPS 5 (2013), https://www.nsa.gov/news-features/press-room/statements/2013-08-09-the-nsa-story.shtml (cited to in CHRIS INGLIS & JEFF KOSSEFF, IN DEFENSE OF FAA SECTION 702 20 (Hoover Inst., Stan. U.) (2016), http://www.hoover.org/research/defense-faa-section-702; *see also* Stmt. of Olsen*, supra* note 2, at 4.

[4] *See FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary, supra* note 3, at 8–9.

[5] NAT'L SEC. AGENCY, *supra* note 3, at 5 (citing INGLIS, *supra* note 3, at 1).

[6] Stmt. of Olsen*, supra* note 2, at 4.

[7] *See* THE SECTION 702 PROGRAM, *supra* note 3, at 1 ("Over the past several years, this surveillance of the online activities of foreigners has been an invaluable source of information for American intelligence professionals and officials."); *see also FISA Amendments Act Reauthorization Act of 2012*, H.R. Rep. No. 112–645, at 3 (2012), https://www.congress.gov/congressional-report/112th-congress/house-report/645/2.

[8] *See* H.R. Rep. No. 112–645, *supra* note 7, at 3 (stating that information gathered under Section 702 is "often unique, unavailable from any other source, and regularly provides critically important insights and operationally actionable intelligence on terrorists and foreign intelligence targets around the world").

disrupting a terrorist attack on the New York City subway system.[9] Using this information, the FBI identified and ultimately arrested Najibullah Zazi, a United States citizen living in the United States, for his role in an al-Qaeda plot to carry out suicide attacks on the New York City subway system.[10] As another example, in 2008, information collected under Section 702 was used to uncover an al-Qaeda cell in Kansas City, Missouri that was in the initial stages of planning an attack on the New York Stock Exchange.[11] Further, information obtained under Section 702 supported the arrest of David Coleman Headley, who had plotted to attack a Danish newspaper that had printed cartoons of the Prophet Muhammad and who had helped plan the 2008 Mumbai terrorist attacks.[12]

Importantly, comprehensive safeguards are built into the FAA, particularly into Section 702, that protect the privacy interests of United States persons.[13] Equally significant, the executive branch has established a

---

[9] *See* 9/11 REVIEW COMMISSION, FED. BUREAU OF INVESTIGATION, THE FBI: PROTECTING THE HOMELAND IN THE 21ST CENTURY 39 (2015).

[10] *See id.*

[11] *See* Aaron Katersky, James Gordon Meek, Josh Margolin, and Brian Ross, *Al Qaeda's Abandoned NY Stock Exchange Plot Revealed,* ABN NEWS (June 18, 2013), http://abcnews.go.com/Blotter/al-qaedas-abandoned-ny-stock-exchange-plot-revealed/story?id=19431509 (quoting FBI Assistant Director Sean Joyce's testimony before the House Permanent Select Committee on Intelligence); *see also* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 108 (2014), https://www.pclob.gov/library/702-Report.pdf [hereinafter PCLOB SECTION 702 REPORT]; *see also* Gia Vang, *Kansas City Man Suspected in New York Terror Plot*, FOX4KC.COM (June 18, 2013), http://fox4kc.com/2013/06/18/kansas-city-man-suspected-in-new-york-terror-plot/.

[12] *See Four Declassified Examples from the NSA*, U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMMITTEE ON INTELLIGENCE (2013), https://web.archive.org/web/20140919065423/http://intelligence.house.gov/1-four-declassified-examples-more-50-attacks-20-countries-thwarted-nsa-collection-under-fisa-section; *see also David Coleman Headley Sentenced to 35 Years in Prison for Role in India and Denmark Terror Plots*, U.S. DEP'T OF JUSTICE (Jan. 24, 2013), https://www.justice.gov/opa/pr/david-coleman-headley-sentenced-35-years-prison-role-india-and-denmark-terror-plots.

[13] This article focuses on modifying the scope of surveillance of United States person information, and accordingly, focuses on privacy protections of United States persons. Within the last several years, privacy protections of non-United States persons have expanded as well. For example, Presidential Policy Directive-28 (PPD-28) provides in pertinent part that: "All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and persons have legitimate privacy interests in the handling of their personal information. U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the

history of compliance with the statutory requirements of Section 702 that preserve such privacy interests. For example, the Senate Select Committee on Intelligence found, based upon its numerous hearings and briefings since the enactment of Section 702, that Section 702 "has been implemented with attention to protecting the privacy and civil liberties of U.S. persons, and has been the subject of extensive oversight" by all three branches of the government.[14] Likewise, the Privacy and Civil Liberties Oversight Board (PCLOB), a bipartisan oversight agency within the executive branch,[15] found that the implementation of the Section 702 program has been subject to extensive oversight and concluded that there was "no evidence of intentional abuse."[16] Moreover, reports by the Attorney General (AG) and Director of National Intelligence (DNI) indicate that the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and Central Intelligence

individual to whom the information pertains or where that individual resides." *Presidential Policy Directive – Signals Intelligence Activities (PPD–28)*, THE WHITE HOUSE (2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. As another example, the FBI applies the "relevant provisions of PPD–28 to information it collects pursuant to FISA section 702" to further the principle that "all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information." *Presidential Policy Directive 28: Policies and Procedures,* FEDERAL BUREAU OF INTELLIGENCE, 1 (2014), https://www.fbi.gov/file-repository/ppd-28-policies-procedures-signed.pdf.

[14] *FAA Sunsets Extension Act of 2012*, S. REP. NO. 112–174, at 2 (2012), https://www.congress.gov/congressional-report/112th-congress/senate-report/174/1.

[15] The PCLOB is "an independent, bipartisan agency within the executive branch" that "is vested with two fundamental authorities: (1) To review and analyze actions the executive branch takes to protect the Nation from terrorism, ensuring the need for such actions is balanced with the need to protect privacy and civil liberties and (2) To ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism." PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov (last visited January 12, 2017). The PCLOB was established by the Implementing Recommendations of the 9/11 Commission Act, Pub. L. 110-53, signed into law in August 2007 (codified at 42 U.S.C. § 2000ee). *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE PROGRAM 2 (2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf [hereinafter PCLOB SECTION 215 REPORT] (explaining that its primary mission is to ensure that the executive branch's efforts to protect the United States from terrorist activities are balanced with "the need to protect privacy and civil liberties").

[16] PCLOB SECTION 215 REPORT, *supra* note 15, at 2.

Agency (CIA) implemented procedures related to Section 702 in a manner that reflects a "focused and concerted effort" by the Intelligence Community to comply with the requirements of Section 702.[17] Reviews have uniformly determined that the executive branch has not intentionally misused any of its authorities under Section 702 or intentionally violated any of the procedural safeguards that protect United States privacy interests.[18]

---

[17] *Release of a Summary of DOJ and ODNI Oversight of Section 702*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, IC ON THE RECORD (most recent oversight reports publicly released on Aug. 11, 2016 and Jan. 13, 2017), https://icontherecord.tumblr.com/tagged/section-702 (publicly releasing semiannual oversight reports dated March 2014, Oct. 2014, June 2015, Sept. 2015, Feb. 2016, and Nov. 2016). These reports have concluded that "the agencies have continued to implement the procedures and follow the guidelines in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702." In addition to the release of these oversight reports, ODNI publicly released minimization procedures. *Release of 2015 Section 702 Minimization Procedures*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, IC ON THE RECORD (August 11, 2016), https://icontherecord.tumblr.com/tagged/section-702 [hereinafter *Release of 2015 Section 702 Minimization Procedures*] (publicly releasing minimization procedures issued pursuant to Section 702 of the Foreign Intelligence Surveillance Act); *see* U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2015), https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf [hereinafter 2015 NSA MINIMIZATION PROCEDURES]; *see also* U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2015), https://www.dni.gov/files/documents/2015FBIMinimization_Procedures.pdf [hereinafter 2015 FBI MINIMIZATION PROCEDURES]; U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2015), https://www.dni.gov/files/documents/2015NCTCMinimizationProcedures_Redacted.pdf [hereinafter 2015 NCTC MINIMIZATION PROCEDURES]; U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2015), https://www.dni.gov/files/documents/2015CIAMinimizationProcedures_Redacted.pdf [hereinafter 2015 CIA MINIMIZATION PROCEDURES].

[18] *See FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 1–2. It is noted, however, that in 2011, the government revealed to the Foreign Intelligence Surveillance Court (FISC or FISA Court) that the NSA's upstream collection was much broader than the government had previously represented. Specifically, the government reported, for the first time, that it was collecting multi-communication transactions (MCTs) as part of its upstream collection. Based upon this new information, the FISC determined that NSA's minimization procedures, as the government proposed to apply them with respect to the retention of MCTs, did not comply with the statutory requirements. *Redacted*, 2011 WL 10945618, *9 (FISA Ct. Oct. 3, 2011) (citing 50 U.S.C. §§ 1801(h)(1) and 1821(4)(A)). The FISC also determined that

The FAA is scheduled to sunset in December 2017.[19] Some advocates contend that Section 702 should be renewed with tighter constraints placed upon executive branch authorities.[20] Others emphasize the critical contribution that Section 702 has made in preventing terrorist attacks and advocate for the renewal of Section 702.[21] In this article, I provide another view: Section 702 should be strengthened. Specifically, I propose that surveillance authorities should be strengthened to include the collection of foreign intelligence information on both United States and non-United States persons overseas without individualized judicial review for each collection, with additional safeguards for information collected on United States persons.[22] Further, I recommend against placing further constraints upon the

---

NSA's targeting and minimization procedures, as the government proposed to implement them in connection with MCTs, were not consistent with the Fourth Amendment. To comply with the FISC's findings, the NSA modified its minimization procedures with respect to MCTs. Specifically, NSA restricted access to the portions of its upstream collection that were most likely to contain wholly domestic communications and non-target information that was subject to statutory or Fourth Amendment protection. *Redacted*, 2012 WL 9189263 *2 (FISA Ct. Aug. 24, 2012) (citing *Redacted*, 2011 WL 10947772 *7–9 (FISA Ct. Nov. 30, 2011)). Procedures were also changed providing that all upstream acquisitions would be retained for a default maximum period of two years rather than five. The following month, the FISC found that the government adequately corrected the deficiencies and that the revised procedures complied with both the statute and the Fourth Amendment. *Redacted*, 2011 WL 10947772 (FISA Ct. Nov. 30, 2011). Moreover, NSA purged all data in its repositories that had been identified as having been acquired through upstream collection before the October 31, 2011 effective date of the amended NSA minimization procedures approved by the FISC. *Redacted*, 2012 WL 9189263 *3.

[19] *See* 50 U.S.C. §§ 1881a–1881g. For a comprehensive discussion of Section 702, including its history and evolution, *see* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L. & PUB. POL'Y 117, 125 (2015).

[20] *See, e.g.*, LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE IN A DIGITAL AGE 159 (Oxford University Press 2016) ("What is needed is more *robust* oversight, a stronger distinction between criminal law and national security, and a thoughtful reframing of the Fourth Amendment doctrine.") (emphasis in the original); Rainey Reitman, *In Hearing on Internet Surveillance, Nobody Knows How Many Americans Impacted in Data Collection*, ELECTRONIC FRONTIER FOUNDATION (May 10, 2016), https://www.eff.org/deeplinks/2016/05/hearing-internet-surveillance-nobody-knows-how-many-americans-impacted-data ("Section 702 of the FISA Amendments Act is set to sunset next year, which means Congress should be debating whether we benefit from renewing it at all...[A]bsent powerful reforms and safeguards for individual privacy, Congress should let Section 702 sunset altogether.").

[21] *See, e.g.*, Stmt. of Olsen, *supra* note 2, at 9 ("I urge the Committee to reauthorize Section 702 to ensure that our intelligence and law enforcement communities have the tools they need to defend the nation."); INGLIS, *supra* note 3 (providing a persuasive discussion of why Section 702 should be reenacted).

[22] *See* 50 U.S.C. § 1801(i) (defining a "United States person" as "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a)(20) of title 8),

government's ability to query its own databases that may include Section 702 information.

My article is divided into five parts. Part I traces the evolution of Section 702. Part II provides an overview of the constitutional parameters for the collection of foreign intelligence information. It highlights the tension between the President's constitutional mandate under Article II of the United States Constitution, *e.g.*, protecting United States national security interests, and the Fourth Amendment's requirement of prohibiting unreasonable searches and seizures by our government.[23] Part III provides a framework for strengthening Section 702 and restoring certain executive branch authorities to where they had been prior to the 2008 FAA. Part III also analyzes how the suggested changes to Section 702 are consistent with the Fourth Amendment and protect United States person privacy interests. Part IV addresses a recently proposed change to Section 702, namely placing additional constraints upon the government's ability to query lawfully-collected data under Section 702. Part IV contends that current safeguards for querying such information are adequate and recommends against placing further limitations upon the government's querying capabilities. Finally, Part V applies the concepts set forth in Parts III and IV of this article to a hypothetical scenario. In doing so, Part V endeavors to show the national security value of these recommendations and how United States privacy interests remain protected.

---

an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section").

[23] *See generally* United States v. Verdugo-Urquidez, 494 U.S. 259, 260, 266 (1990). In *Verdugo*, the Supreme Court held that the purpose of the Fourth Amendment "was to protect the people of the United States against arbitrary action by their own Government; 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." *Verdugo* held that the Fourth Amendment applies to United States person or non-United States who have "come within the territory of, and have developed substantial connections with, this country."

I. EVOLUTION OF SECTION 702

A. The Foreign Intelligence Surveillance Act of 1978

In the early 1970s, evidence that the executive branch had been misusing its intelligence and law enforcement authorities set the stage for congressional inquiry into executive branch activities.[24] Following a prolonged public debate over the Watergate scandal, Richard Nixon resigned as President on August 9, 1974.[25] Two years after Nixon's resignation, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known as the Church Committee, released reports documenting the executive branch's misuse of its intelligence authorities within the United States.[26] The Church Committee revealed that the CIA had construed its authorities to investigate domestic groups whose activities, including demonstrations, might have the potential to threaten CIA installations, recruiters, or contractors.[27] The committee further reported that the FBI had engaged in illicit strategies of using the media to discredit civil rights activists, including Dr. Martin Luther King, Jr., Stokely Carmichael, and Elijah Muhammad.[28] The House Permanent Select Committee on Intelligence established a parallel committee known as the Pike Committee which was also troubled about the executive branch's misuse of its authorities.[29] Around the

---

[24] *See, e.g.*, *Strengthening Intelligence Oversight*, BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW, 3, https://www.brennancenter.org/sites/default/files/publications/Church_Committee_Web_REVISED.pdf.

[25] *See* Carroll Kilpatrick, *Nixon Resigns*, WASH. POST (Aug. 9, 1974), https://www.washingtonpost.com/wp-srv/national/longterm/watergate/articles/080974-3.htm.

[26] *See* SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES (CHURCH COMMITTEE), FOREIGN AND MILITARY INTELLIGENCE, S. REP. NO. 94-755, bk. I and bk. II (1976) [hereinafter CHURCH COMMITTEE].

[27] *See id.,* bk. I, at 136–39.

[28] *See id.*, bk. II, at 86–89.

[29] *See* Gerald K. Haines, *The Pike Committee Investigations and the CIA, Looking for a Rogue Elephant*, CIA (Apr. 14, 2007, 12:22 PM), https://www.cia.gov/library/center-for-the-study-of-

same time, the Supreme Court, in *United States v. United States District Court for the Eastern District of Michigan (Keith)*, while determining that the Fourth Amendment warrant requirement applied to the collection of intelligence related to domestic security, left open the question of the scope of the President's surveillance authority with respect to collecting foreign intelligence information.[30]

Against this backdrop of misuse of intelligence authorities and an open constitutional question with respect to the collection of foreign intelligence information, compromise legislation known as the Foreign Intelligence Surveillance Act was enacted in 1978.[31] When first enacted, FISA did not require judicial review for acquiring foreign intelligence information for persons abroad, including United States persons.[32] Rather, Congress enacted FISA to govern "the use of electronic surveillance *in the United States* for intelligence purposes" and recognized that it did not "afford protections to

---

intelligence/csi-publications/csi-studies/studies/winter98_99/art07.html; *see also* DONOHUE, *supra* note 20, at 7–8.

[30] *See* United States v. United States District Court for the E.D. of Mich. (Keith), 407 U.S. 297, 308 (1972).

[31] Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1885(c). Under 50 U.S.C. § 1801(e), "foreign intelligence information" is defined as:

> (e) "Foreign intelligence information" means—
> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
> (A) the national defense or the security of the United States; or
> (B) the conduct of the foreign affairs of the United States.

[32] *See, e.g.*, DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 2D § 16:5 (2012); *Congressional Record--Senate 110th Proceedings And Debates of the Congress*, June 25, 2008 No. 106, Vol. 154, S6125, https://www.congress.gov/crec/2008/06/25/CREC-2008-06-25.pdf (statement of Senator Hatch).

U.S. persons who are abroad."[33] With the enactment of the FAA in 2008, Congress limited executive branch authority to the collection of foreign intelligence information of United States persons abroad.

In understanding the evolution of FISA and its application to United States persons abroad, it is necessary to consider the definition of electronic surveillance and its impact upon the method in which surveillance is conducted. As described by Steven Bradbury, former head of the Department of Justice (DOJ), Office of Legal Counsel, the original definition of electronic surveillance under FISA was narrow.[34] In 1978, when FISA was enacted, the definition of electronic surveillance included the acquisition of content from a *radio or wire communication* when such acquisition occurred in

---

[33] Jonathan W. Gannon, *From Executive Order to Judicial Approval: Tracing the History of Surveillance of U.S. Persons Abroad in Light of Recent Terrorism Investigations*, 59 GEORGETOWN J. OF NAT'L SECURITY L. & POL'Y 6, 71–72, http://jnslp.com/wp-content/uploads/2012/08/03_Gannon_Master-1.pdf (quoting 154 CONG. REC. S257 (daily ed. Jan. 24, 2008) (statement of Sen. Rockefeller)) (quoting H.R. REP. NO. 95-1283, at 22 (emphasis added by Gannon)); Steven G. Bradbury, *Understanding The NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 And Foreign-Targeted Collection Under Section 702*, LAWFARE RESEARCH PAPER SERIES, 19 (Sept. 1, 2013), https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/08/Bradbury-Vol-1-No-3.pdf.

[34] Steven G. Bradbury, *supra* note 33 at 16. When FISA was first enacted, electronic surveillance was defined as:

> "(1) the acquisition by, an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
> (2) the acquisition by an electronic, mechanical, or other surveillance device of tile contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
> (4) the installation or use of an electronic, mechanical, or other' surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."
> 50 U.S.C. § 1801(f) (1976).

the United States.[35] At the time of FISA's enactment, international communications were mainly transmitted by satellite, which fell outside of this definition.[36] However, with the expanding use of the Internet in the 1990s and 2000s, the way in which communications were transmitted evolved from satellite to undersea fiber optic cables.[37] As a result, international electronic communications that were once outside the scope of FISA because they were not wire or radio communications now fell within its governance because the communications were transmitted through undersea fiber optic cables (*e.g.*, a wire communication).[38]

Laura Donohue, Professor of Law at Georgetown University Law Center, offers another explanation for the necessity for modernizing FISA. She explained that when FISA was first enacted, "Congress explicitly exempted foreign-to-foreign wire communications from FISA's remit."[39] As an example, Professor Donohue described that a communication from a British citizen in London calling a French citizen in Paris was not governed by FISA because that communication never entered the United States.[40] She explained, however, that with the evolution of email communications, foreign-to-foreign communications originally exempted from FISA began to fall within its domain.[41] She believed that it "would be impractical and cumbersome" to require the Intelligence Community to obtain judicial review for every interception of foreign intelligence between foreign nationals outside of the United States.[42] Professor Donohue provided the following example to illustrate how evolving technology placed communications that

---

[35] *See* 50 U.S.C. § 1801(f) (1976); *see also* KRIS & WILSON, *supra* note 32, § 16:5 (discussing the evolving definition of "electronic surveillance," including its legislative history).
[36] *See* Bradbury, *supra* note 33, at 16.
[37] *See id.*
[38] *See* Bradbury, *supra* note 33, at 16–17; *but see* KRIS & WILSON, *supra* note 32, § 16:4 (stating that the actual percentage of calls transmitted by satellite was between "one-half and two-thirds").
[39] DONOHUE, *supra* note 19, at 147.
[40] *See id.*
[41] *See id.* at 147–48.
[42] *See id.* at 147.

were once outside the scope of FISA within its governance.

> U.S. Internet Service Providers (ISPs) store e-mail on servers in the United States. The same British subject, if she accesses her email from London (pulling it from a server within the United States), suddenly falls within FISA—even when the e-mail she is retrieving is sent by the same French citizen in Paris. In other words, merely by using an American ISP, non-citizens could obtain the protections of the more rights protective FISA framework—even where such persons had no other ties to the United States and presented a classic foreign intelligence threat (and would otherwise be covered by the less rigorous contours of Executive Order 12,333).[43]

As described by Mr. Bradbury and Professor Donohue, with evolving technologies more communications fell within the scope of FISA, including foreign-to-foreign communications.[44] This development resulted in the need to seek approval from the Foreign Intelligence Surveillance Court to acquire such communications where previously such judicial review had not been required.[45] Those who are familiar with the process of seeking FISC authorization to conduct surveillance explain the involved and time-consuming process of seeking judicial authorization.[46] As explained by the

---

[43] *Id.* at 147–48.

[44] *See* DONOHUE, *supra* note 19, at 147; *see also* Bradbury, *supra* note 33, at 16–17.

[45] *See* DONOHUE, *supra* note 19, at 147; *see also* Bradbury, *supra* note 33, at 16.

[46] *See, e.g.*, *The NSA Wiretapping Program*, FOR THE RECORD, A PUBLICATION OF THE CENTER ON LAW AND SECURITY AT THE NYU SCHOOL OF LAW, 1, 9 (2007), http://www.lawandsecurity.org/portals/0/documents/nsa_jan_07.pdf. The statutory language of FISA itself illustrates the involved process of obtaining a probable cause order from the FISC to conduct surveillance. To seek FISC approval to acquire foreign intelligence information, the executive branch must submit an application to the FISC containing the statutorily required information and obtain the requisite approvals. The application must include a certification by a high-level executive branch official, *e.g.*, Director or Deputy Director of a component of the Intelligence Community, such as the Director or Deputy Director of the FBI, certifying that a "significant purpose" of the surveillance is to obtain foreign intelligence information. 50 U.S.C § 1804(a)(6)(B). Further, for each application, the Attorney General or a DOJ designee, must review the application to determine whether it meets the statutory requirements. 50 U.S.C § 1804(d). In addition to this high-level review, each application must include, among other information: (1) description of the specific target of the electronic surveillance; (2) a statement of the facts relied upon by the applicant to justify his belief that the target of the electronic surveillance is a foreign power or an agent of a foreign power, and each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power; (3) a statement of the proposed minimization procedures; and (4) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance. 50 U.S.C §§ 1804(a)(2)–(5).

PCLOB, before an application for surveillance is submitted to the FISC, the executive branch conducts an extensive review of the application.[47] The PCLOB described the process as follows:

> It is first reviewed by lawyers at the FBI, the NSA, or other agencies, and then by lawyers at the National Security Division of the Department of Justice ("NSD"), who present the government's applications to the court. Review by the NSD frequently involves substantial back and forth between the agency seeking authorization and the DOJ lawyers, as the lawyers seek additional factual details about the target of the surveillance, technical information about the surveillance methodology, or assurances about how the information acquired will be used and disseminated. Agency personnel would say that at times these interactions are quasi-adversarial. At the conclusion of the process, the application will generally be quite lengthy and may have extensive supporting documentation, and it must be approved by the Attorney General, the Deputy Attorney General, or upon designation, the Assistant Attorney General for National Security.[48]

Carrie Cordero, former DOJ and Office of the Director of National Intelligence (ODNI) attorney who served in national security-related positions and is an Adjunct Professor of Law at Georgetown University Law Center, noted that to request an individualized FISC order, "the bureaucratic manpower . . . to supply and check facts, prepare applications and present these matters to the Court [is] substantial."[49] Likewise, Michael McConnell, former Director of National Intelligence, stated that "it took '200 man hours' to prepare an application 'for one [telephone] number.'"[50]

Further, as noted by scholars in a publication from the Center on Law and Security at the New York University (NYU) School of Law, it takes months for a FISA application to be processed due to the "endless editing

---

[47] *See* PCLOB SECTION 215 REPORT, *supra* note 15, at 177–78.
[48] *Id.*
[49] Carrie Cordero, *The Brennan Center Report on the FISA Court and Proposals for FISA Reform*, LAWFARE (Apr. 2, 2015), https://www.lawfareblog.com/brennan-center-report-fisa-court-and-proposals-fisa-reform.
[50] Chris Roberts, *Transcript: Debate on the Foreign Intelligence Surveillance Act*, EL PASO TIMES (Aug. 22, 2007), https://www.eff.org/files/filenode/att/elpasotimesmcconnelltranscript.pdf (quoting Michael McConnell, former National Intelligence Director).

and re-editing of documents by lawyers and bureaucrats."[51] Similarly, William E. Moschella, then Assistant Attorney General at the United States Department of Justice, described the process as follows: "In order to obtain judicial review by the FISA court before conducting surveillance, the Government must assemble a voluminous application, obtain the approval of the Attorney General himself and senior administration national security officials, submit the materials to the court, and await its decision."[52]

B. President's Surveillance Program

As discussed above, the unintended consequence of evolving technology expanded the governance of FISA. The tragic attacks of September 11, 2001 precipitated a recognition of the need for the intelligence community to conduct surveillance of international communications and overseas targets with much greater speed and agility. Seeking individual FISC orders to collect this type of foreign intelligence information was cumbersome and no longer proved feasible under the outdated version of FISA at the time.[53] The President and NSA believed that the ability to conduct "fast, flexible, and

---

[51] *See The NSA Wiretapping Program*, *supra* note 46, at 13.

[52] KRIS & WILSON, *supra* note 32, § 16:10 (quoting Letter from William E. Moschella, Assistant Attorney General, U.S. Department of Justice to F. Jams Sensenbrenner, Chairman, House Committee on the Judiciary). As provided in 50 U.S.C. § 1804(d):

> (1)(A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, *the Attorney General shall personally review* under subsection (a) of this section an application under that subsection for a target described in section 1801(b)(2) of this title.
> (B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.
> (C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.

[53] *See Modifying NSA Programs and Amending FISA Authorities, Open Hearing on Legislative Proposals Before the H. Permanent Select Comm. on Intelligence*, 113 CONG. 12 (2013), http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/bradbury10292013.pdf (statement of Steven G. Bradbury, former head of the Office of Legal Counsel in the U.S. Department of Justice).

broad-scale signals intelligence of international communications" was necessary to identify and prevent further attacks in the United States.[54] The structure of FISA at the time, however, encumbered the executive branch from achieving this objective.[55]

Following the September 11, 2001 attacks, to quickly collect foreign intelligence information of international communications and targets abroad, President Bush authorized the executive agencies to conduct warrantless surveillance in a then highly-classified program referred to as the President's Surveillance Program (PSP).[56] One aspect of the program was the collection of the content of communications into and out of the United States—without judicial review—where it was reasonable to conclude that a member of Al-Qaeda or a related terrorist group was a party to such communication.[57] Approximately four years after the inception of this surveillance program, the *New York Times* publicly disclosed the program in a December 16, 2005

---

[54] *Id.* at 12.

[55] *See id.*

[56] *See* OFFICE OF THE INSPECTORS GENERAL, DEPARTMENT OF DEFENSE, DEPARTMENT OF JUSTICE, CENTRAL INTELLIGENCE AGENCY, NATIONAL SECURITY AGENCY, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, 2009-0013-AS, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 1 (2009), https://oig.justice.gov/special/s0907.pdf [hereinafter OIG REPORT]; *see also The DOJ Releases Additional Documents Concerning Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (Dec. 12, 2014), http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1152-the-doj-releases-additional-documents-concerning-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11,-2001?highlight=WzcwMl0. To provide a legal justification for the warrantless surveillance program, DOJ, Office of Legal Counsel (OLC) Deputy Assistant Attorney General John Yoo, the only person in OLC who knew about the PSP from the start of the program in October 2001 until he left DOJ in May 2003, drafted a memorandum to support the program. *See* OIG REPORT, at 10. In a November 2, 2001 memorandum, Professor Yoo acknowledged that "FISA 'purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence,' but opined that '[s]uch a reading of FISA would be an unconstitutional infringement on the President's Article II authorities.'" *Id.* (quoting John Yoo, OLC Memorandum for the Attorney General, Nov. 2, 2001, at 9). Professor Yoo believed that "the ultimate test of whether the government may engage in warrantless electronic surveillance activities is whether such conduct is consistent with the Fourth Amendment, not whether it meets the standards of FISA." *Id.* at 11. Professor Yoo's memorandum, while providing legal justification for the program at the time, was later criticized as failing to consider significant legal issues. *See id.*, at 11-14.

[57] *See id.*

article.[58] Relying upon reports of anonymous government officials, the *New York Times* reported that: "the intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to Al Qaeda."[59] The day after the program was revealed by the *New York Times*, President Bush delivered a radio address to discuss the surveillance program, explaining that he "authorized the National Security Agency, consistent with United States law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations."[60]

Once this surveillance program became publicly known, controversy over the legality of the President's Surveillance Program arose. On one side of the

---

[58] *See* James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, NEW YORK TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0.

[59] *Id.*

[60] President George W. Bush, Radio Address to the American People (Dec. 17, 2005), http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html; *see also* OIG REPORT, *supra* note 56, at 1 (explaining that President Bush authorized the warrantless surveillance program "at intervals of approximately every 45 days"). For "each reauthorization the CIA and later the NCTC [The National Counterterrorism Center] prepared an assessment of current potential terrorist threats and a summary of intelligence gathered through the PSP and other means during the previous authorization period." OIG REPORT, at 10, *supra* note 56 at 6. Following receipt of the Intelligence Community's assessment, the Department of Justice's Office of Legal Counsel reviewed this information to assess whether there was "a sufficient factual basis demonstrating a threat of terrorist attacks in the United States for it to continue to be reasonable under the standards of the Fourth Amendment for the President to [continue] to authorize the warrantless searches involved" in the program. *Id.*; *see* 154 CONG. REC. S6121 (daily ed. June 25, 2008), https://www.congress.gov/crec/2008/06/25/CREC-2008-06-25.pdf (statement of Sen. Chambliss) (finding that in addition to DOJ review, Congressional leaders "kn[e]w about this program"); *see* 154 CONG. REC. S6117 (statement of Senator Bond) ("the big eight at the time—that is, the Republican and Democratic leaders of the House and the Senate and the leaders of their Intelligence Committees—were briefed on this program before it started."). Shortly after the program began, on October 25, 2001, White House officials and then-NSA Director Michael Hayden briefed the Chairman and Ranking Member of the House Permanent Select Committee on Intelligence, Nancy Pelosi and Porter Goss; and the Chairman and Vice Chairman of the Senate Select Committee on Intelligence, D. Robert Graham and Richard Shelby. Indeed, members of Congress were briefed 49 times about the PSP, "17 of which took place before the December 2005 media reports." The Presiding Judge of the FISC was also briefed about the President's Surveillance Program. OIG REPORT, at 10, *supra* note 56 at 16.

argument, the Department of Justice maintained that the President's Surveillance Program was consistent with the executive branch's statutory and constitutional authorities.[61] In support of its position, DOJ maintained that under Article II of the Constitution, the President, including in his capacity as Commander in Chief, has the responsibility to protect the United States from future attacks, and the Constitution provides the President with the requisite authority to fulfill such obligation.[62] DOJ believed that Congress supplemented this constitutional authority in the preamble to the Authorization for the Use of Military Force (AUMF) and the War Powers Resolution.[63] Specifically, DOJ asserted that the Supreme Court, in *Hamdi v. Rumsfeld*, recognized that the AUMF authorized "fundamental incident[s] of waging war."[64] After citing to examples of how intelligence gathering has been used as an integral part of engaging in war throughout history, DOJ contended that conducting surveillance to acquire foreign intelligence information against the enemy is a "fundamental incident" of the use of military force,[65] and accordingly, authorized by the AUMF. Based upon this analysis, DOJ concluded that, under *Youngstown Sheet & Tube v. Sawyer*, the President's authority to conduct warrantless surveillance to acquire

---

[61] Letter from The Department of Justice, to Pat Roberts, Chairman, Senate Select Comm. on Intelligence; Peter Hoekstra, Chairman, Permanent Select Comm. on Intelligence; John D. Rockefeller, Vice Chair, Senate Select Comm. on Intelligence; Jane Harman, Ranking Minority Member, Permanent Select Comm. on Intelligence (Dec. 22, 2005) (on file with the Office of Legislative Affairs) [hereinafter Letter from the Department of Justice].

[62] *See id.* at 2 (citing Prize Cases, 67 U.S. 635, 668 (1863)) (stressing that if the Nation is invaded, "the President is not only authorized but bound to resist by force . . . without waiting for any special legislative authority"); Campbell v. Clinton, 203 F.3d 19, 27 (D.C. Cir. 2000) (Silberman, J. concurring) ("[T]he Prize Cases . . . stand for the proposition that the President has independent authority to repel aggressive acts by third parties even without specific congressional authorization, and courts may not review the level of force selected.").

[63] *See* Letter from The Department of Justice, *supra* note 61, at 2–3 (citing to the AUMF of September 18, 2001, 115 Stat. 224 (2001)) ("[T]he President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States."); War Powers Resolution, 50 U.S.C. § 1541(c) ("The constitutional powers of the President as Commander in Chief to introduce United States Armed Forces into hostilities[] . . . [extend to] a national emergency created by attack upon the United States, its territories or possessions, or its armed forces.")).

[64] *Id.* at 3 (citing Hamdi v. Rumsfeld, 542 U.S. 507, 518–19 (plurality opinion), 587 (Thomas, J., dissenting)) (2004).

[65] *Id.*

intelligence information under the PSP was "at its maximum."[66]

On the other hand, some believed that conducting surveillance under the President's Surveillance Program violated FISA and that reliance on the AUMF was improper. One such view was expressed in a January 9, 2006 letter from scholars of constitutional law and scholars who were former government officials to congressional leaders.[67] The scholars directly countered DOJ's contentions that the PSP was both statutorily and constitutionally sound. One of the scholars' principal assertions was that, based upon the statutory language of FISA and 18 U.S.C. § 2511(2)(f), FISA was the exclusive means in which to conduct electronic surveillance for foreign intelligence purposes.[68] They asserted that the President acted "unilaterally and secretly" in violation of the explicit statutory language of FISA.[69] They contended that all electronic surveillance in the United States is governed by FISA and the criminal code—not the AUMF.[70] Further, the

---

[66] *Id.* (quoting Youngstown Sheet & Tube v. Sawyer, 343 U.S. 579, 635 (1952) (Jackson, J., concurring); Dames & Moore v. Regan, 453 U.S. 654, 668 (1981)).

[67] *See* Letter from Curtis A. Bradley, Professor of Law, Duke University, Former Counselor on International Law in the State Department Legal Adviser's Office; David Cole, Professor of Law, Georgetown University Law Center; Walter Dellinger, Professor of Law, Duke University, Former Assistant Attorney General, Office of Legal Counsel, Former Acting Solicitor General of the United States; Ronald Dworkin, Professor, New York University Law School; Richard Epstein, Professor, University of Chicago Law School, Peter and Kirsten Bedford Senior Fellow, Hoover Institution; Harold Hongju Koh, Dean and Professor of International Law, Yale Law School, Former Assistant Secretary of State for Democracy, Human Rights and Labor, Former Attorney-Adviser, Office of Legal Counsel, DOJ; Philip B. Heymann, Professor, Harvard Law School, Former Deputy Attorney General, Visiting Professor, Georgetown University Law Center, Former Attorney Advisor, Department of Justice Office of Legal Counsel; Beth Nolan, Former Counsel to the President, Deputy Assistant Attorney General, Office of Legal Counsel, Associate Counsel to the President, Attorney Advisor, Office of Legal Counsel; William S. Sessions, Former Director, FBI, Former Chief United States District Judge, Western District of Texas; Geoffrey R. Stone, Professor of Law, University of Chicago, Former Dean of the University of Chicago Law School and Provost of the University of Chicago; Kathleen M. Sullivan, Professor, Stanford Law School Former Dean, Stanford Law School; Laurence H. Tribe, Professor, Harvard Law School, William W. Van Alstyne, Professor, William and Mary Law School, Former Attorney, Department of Justice, to Congressional Leadership (Jan. 9, 2006) (on file with author), https://fas.org/irp/agency/doj/fisa/doj-response.pdf [hereinafter Letter from Bradley et al. to Congressional Leadership].

[68] *See id.* at 2.

[69] Letter from Bradley et al. to Congressional Leadership, *supra* note 67, at 3–4.

[70] *See* Letter from Bradley et al. to Congressional Leadership, *supra* note 67, at 3–4 (citing 18 U.S.C. § 2511(2)(f) (emphasis added by constitutional scholars)).

scholars believed that it was unreasonable to interpret the AUMF as authorizing warrantless electronic surveillance in the United States during wartime because Congress had addressed that specific issue in FISA.[71] Citing Justice Jackson's concurrence in *Youngstown Sheet*, the scholars concluded that the President acted contrary to congressional intent, and accordingly, his authority was "at its lowest ebb."[72]

Notably, in their letter the scholars recognized that had FISA, or any legislation, not been enacted governing the President's authority to conduct surveillance, the President's actions may have been consistent with his Article II powers.[73] With respect to this issue, the scholars wrote:

> had Congress taken no action in this area, *the President might well be constitutionally empowered to conduct domestic surveillance directly tied and narrowly confined to that goal*—subject, of course, to Fourth Amendment limits. Indeed, in the years before FISA was enacted, the federal law involving wiretapping specifically provided that "*[n]othing* contained in this chapter or in section 605 of the Communications Act of 1934 *shall limit the constitutional power of the President . . . to obtain foreign intelligence information deemed essential to the security of the United States*." 18 U.S.C. § 2511(3) (1976).[74]

However, the scholars maintained that FISA "specifically repealed" 18 U.S.C. § 2511(3) and replaced it with statutory language providing that FISA and the criminal code are the only authorities for conducting electronic surveillance.[75]

DOJ and the scholars both raised persuasive legal arguments as to whether the President's authority was "at its maximum" or "at its lowest ebb"

---

[71] *See* Letter from Bradley et al. to Congressional Leadership, *supra* note 67, at 3–4; *see also* 50 U.S.C. § 1811 (discussing that FISA provides in pertinent part: "[T]he President, through the Attorney General, may authorize electronic surveillance without a court order under this title to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war"); *see also* 50 U.S.C. § 1829 (stating similar language for physical search).

[72] Letter from Bradley et al. to Congressional Leadership, *supra* note 67, at 4 (citing *Youngstown*, *supra* note 66, at 637).

[73] *See* Letter from The Department of Justice, *supra* note 61(arguing for the President's constitutional authority to order warrantless foreign intelligence surveillance under Article II of the Constitution); *see also* Letter from Bradley et al. to Congressional Leadership, *supra* note 67, at 5–6.

[74] Letter from Bradley et al. to Congressional Leadership, *supra* note 67, at 6 (emphasis added).

[75] *Id.*

as described in Justice Jackson's *Youngstown Sheet* concurrence.[76] While the debate provided valuable insight into the President's constitutional authorities, the question as to the legality of the President's Surveillance Program was never officially resolved.[77] The program ended on February 1, 2007.[78]

C. Protect America Act of 2007

Once the PSP ended, the need still existed for the executive branch to obtain foreign intelligence information on persons abroad in an expeditious manner. In response to this critical need, legislation was passed authorizing the executive branch to continue warrantless surveillance on international communications and persons located outside of the United States, including United States persons, to acquire foreign intelligence.[79] Specifically, Congress passed legislation entitled the Protect America Act (PAA) which was enacted on August 5, 2007.[80] The PAA (the predecessor to Section 702 of FAA) was

---

[76] *Youngstown*, *supra* note 66, at 635–38; *see generally* KRIS & WILSON, *supra* note 32, at §§ 15:1–15:13 (discussing the legality of the PSP).

[77] *See, e.g.*, KRIS & WILSON, *supra* note 32, at § 15:12 ("[T]he constitutional question of whether and how a statute may restrict the President's power to conduct foreign intelligence surveillance remains very much alive.").

[78] *See* EDWARD C. LIU, REAUTHORIZATION OF THE FISA AMENDMENTS ACT 5 (2013) (citing Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2007 (FAA), S. REP. NO. 110-209, at 4 (2007)); *see also* Letter from Attorney General Gonzales to Senate Judiciary Committee Chairman Patrick Leahy and Senator Arlen Specter (Jan. 17, 2007) and P.L. 110-55, 50 U.S.C. §§1805(a)–1805(c)).

[79] *See* PAA, 50 U.S.C. §§ 1805(a)-(c) (repealed), http://www.gpo.gov/fdsys/pkg/PLAW-110publ55/html/PLAW-110publ55.htm. On August 3, 2007, the Senate approved the PAA, with 60 members voting in favor of the bill and 28 voting against it. The following day, on Aug 4, 2007, the House approved the PAA, with 227 members voting in favor of the legislation and 183 voting against it. *See also S. 1927 (110th): Protect America Act of 2007*, GOVTRACK, https://www.govtrack.us/congress/votes/110-2007/h836.

[80] *See id.*; *see also* Pub. L. 110–261, Title IV, § 403(a)(1)(A), July 10, 2008, 122 Stat. 2473. The PAA expired in February 2008 and was repealed on July 10, 2008. The PAA established a statutory framework that authorized the executive branch to conduct warrantless surveillance of persons abroad to acquire foreign intelligence information. Specifically, to collect foreign intelligence information under the PAA, the Director of National Intelligence (DNI) and the Attorney General (AG) could "for periods of up to one year authorize the acquisition of foreign intelligence information concerning [*both U.S. and non-U.S.*] persons reasonably believed to be outside the United States." 50 U.S.C. § 1805(B)(a) (repealed). Before approving the acquisition of the foreign intelligence information, the DNI and AG were required to determine whether the acquisition met certain factors. For example, the DNI and AG were

a stopgap measure with a sunset date of 180 days after the date of its enactment.[81] Subject to certain conditions, the PAA authorized the collection of foreign intelligence surveillance on individuals (including United States persons) reasonably believed to be located outside the United States without individualized judicial review for each acquisition.[82] Under the PAA, the executive branch was permitted to acquire foreign intelligence information of *any* persons outside of the United States *including United States persons*, without a probable cause order from the FISC.[83] In passing the legislation, one Congressman noted that the PAA "takes the 1978 law, it provides the same protection for Americans that they had in 1978 and 1988 and 1998. And now, as we approach 2008, it just simply lets us have the definitions of the law meet the technology of the time. This monitors the communication of people who are initiating their communication in a foreign country."[84]

Importantly, to protect United States person privacy interests, the PAA

---

required to determine: (1) "reasonable procedures are in place for determining that the acquisition of foreign intelligence information concerns persons reasonably believed to be located outside the United States," 50 U.S.C. § 1805(B)(a)(1) (repealed); (2) "the acquisition does not constitute electronic surveillance," 50 U.S.C. § 1805B(a)(2) (repealed); (3) "the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider," 50 U.S.C. § 1805(B)(a)(3) (repealed); (4) "a significant purpose of the acquisition is to obtain foreign intelligence information," 50 U.S.C. § 1805(B)(a)(4) (repealed); and (5) "the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under 50 U.S.C. § 1801(h)." 50 U.S.C. § 1805(B)(a)(5) (repealed).

[81] *See S. 1927 (110th): Protect America Act of 2007*, Pub. L. No. 110–55, § 6(c), 121 Stat 552, 557.

[82] *See In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1006 (FISA Ct. Rev. 2008) [hereinafter *In re Directives*] (citing 50 U.S.C. § 1805(b)(a)); *see also* KRIS & WILSON, *supra* note 32, at § 16:15 (citing Pub. L. No 110–55, 121 Stat. 52 (2007)). The PAA "allowed warrantless surveillance of international communications to or from the United States, even when acquired from a wire or cable (or an e-mail server) inside the United States; and it allowed warrantless surveillance of foreign-to-foreign e-mail messages acquired from storage on servers located in the United States."

[83] *See* 50 U.S.C. § 1805(B)(a) (repealed) (emphasis added); *see also In re Directives*, *supra* note 82, at 1004 ("The PAA allowed the government to conduct warrantless foreign intelligence surveillance on targets (including United States persons) 'reasonably believed' to be located outside the United States."); *see also* EDWARD C. LIU, SURVEILLANCE OF FOREIGNERS OUTSIDE THE UNITED STATES UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA), CONG. RESEARCH SERV., R44457 (2016), https://www.fas.org/sgp/crs/intel/R44457.pdf.

[84] Roy Blunt, Congressman, House of Representatives, Floor Speech: Protect America Act of 2007 (Aug. 4, 2007).

(as well as Section 702) contained multiple layers of procedural safeguards. For example, the PAA required the application of minimization procedures which are procedures designed to balance the privacy interests of United States persons with the government's ability to acquire, retain, and disseminate foreign intelligence information.[85] Privacy interests were also protected through the PAA's oversight procedures. For example, on a semi-annual basis, the AG was required to submit a report to the Intelligence and Judiciary Committees in both the House and Senate that included a description of non-compliance incidents and the number of certifications and directives issued during the reporting period.[86] Further, the DNI and AG were required to conduct reviews assessing the executive branch's compliance with the minimization procedures and submit their findings to the relevant congressional committees.[87]

The constitutionality of the application of the PAA was challenged in *In re Directives [redacted] Pursuant to Section 105B of The Foreign Intelligence Surveillance Act*. In this case, the Foreign Intelligence Surveillance Court of Review (FISCR or FISA Court of Review), the appellate court of review for the FISC, determined that a foreign intelligence exception to the Fourth Amendment's warrant requirement existed because the surveillance at issue was conducted to acquire foreign intelligence information for national security purposes and was "directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States."[88] After concluding that there was a foreign intelligence exception to the Warrant Clause, the FISCR

---

[85] *See* KRIS & WILSON, *supra* note 32, § 16:2. Minimization procedures, which play an integral role in protecting privacy interests of United States person, must be "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons." *See also* 50 U.S.C. § 1801(h)(1); 50 U.S.C. § 1881(a)(e)(1); *see also In re Directives*, *supra* note 82, at 1015.

[86] *See* 50 U.S.C. § 1805(B)(4)(1) (2007) (repealed 2008).

[87] *See* 50 U.S.C. § 1805(B)(d). The DNI and AG were required to submit their findings to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate.

[88] *In re Directives*, *supra* note 82, at 1012; for further discussion of *In re Directives*, *see* Part III.C of this article.

then considered whether the surveillance conducted under the PAA was consistent with the reasonableness requirement of the Fourth Amendment. In conducting this evaluation, the FISCR employed the "totality of the circumstances" test to evaluate whether the governmental action was reasonable under the Fourth Amendment, weighing the government's national security interests with individual privacy interests.[89] The FISCR recognized that "relevant governmental interest—the interest in national security—is of the highest order of magnitude."[90] The FISCR further stated that there was a strong likelihood that mandating a warrant would "hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake."[91] After weighing Fourth Amendment privacy interests with the national security interests at issue, the FISCR determined that the protections afforded to the privacy rights of targeted persons were reasonable in light of the government's national security interests.[92] Thus, the FISCR concluded that the warrantless acquisition of foreign intelligence information under the PAA—including the warrantless surveillance of United States persons outside of the United States—was reasonable under the Fourth Amendment.[93]

---

[89] *Id.* (citing Samson v. California, 547 U.S. 843 (2006); Tennessee v. Garner, 471 U.S. 1, 8–9, (1985); *see In re Directives*, *supra* note 82, at 1013). The FISCR believe that the following governmental safeguards provided for the protection of individual privacy interests: "targeting procedures, minimization procedures, a procedure to ensure that a significant purpose of a surveillance is to obtain foreign intelligence information, procedures incorporated through Executive Order 12333 § 2.5, and [redacted text] procedures [redacted text] outlined in an affidavit supporting the certifications."

[90] *Id.* at 1012 (citing Haig v. Agee, 453 U.S. 280, 307 (1981); In re Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002)).

[91] *Id.* at 1011 (citing United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980)) ("explaining that when the object of a surveillance is a foreign power or its collaborators, 'the government has the greatest need for speed, stealth, and secrecy'").

[92] *See id.* at 1013.

[93] *See id.* at 1016.

D. FISA Amendments Act of 2008

With a sunset date of 180 days after the date of the enactment,[94] and a fifteen day extension,[95] the PAA expired in February 2008.[96] On July 10, 2008, the successor statute of the PAA, the FISA Amendments Act of 2008 (FAA), was enacted.[97] The FAA was a compromise bill and adopted many of the same standards as the PAA.[98] As will be discussed in more detail below, the most well-known provision of the FAA, Section 702, authorizes the executive branch to acquire foreign intelligence information of non-United States persons reasonably believed to be located outside of the United States without seeking individualized FISC orders for each acquisition.[99] Sections 703 (acquisitions inside the United States), 704 (other acquisitions), and 705 (information located both inside and outside the United States) established procedures requiring the executive branch to obtain probable cause FISC orders to collect foreign intelligence information of United States persons located outside of the United States.[100]

Notably, the initial draft FAA legislation passed by the House of Representatives to replace the PAA authorized the surveillance of any person abroad without individualized orders, including United States persons.[101]

---

[94] *See* 50 U.S.C. § 1805(B)(c) (repealed); *see also* Protect America Act of 2007, *supra* note 81.
[95] *See* Gannon, *supra* note 33, at 84.
[96] *See* LIU, *supra* note 78, at 5.
[97] *See generally* 50 U.S.C. §§ 1881(a)–1881(g) (listing of the provisions adopted under the FISA Amendments Act of 2008); H.R. 6304 (110th), House vote: FISA Amendments Act of 2008, https://www.govtrack.us/congress/votes/110-2008/h437. The FAA passed Congress with a strong majority in favor of the bill. On June 20, 2008, the FAA passed the House with 293 members voting in favor of the legislation and 129 voting against it. Several weeks later, 69 Senators voted in favor of the FAA and 28 voted against it. *See generally* Gannon, *supra* note 33, at 69-80. President Bush signed the bill into law on July 10, 2008.
[98] *See* 154 CONG. REC. S618S6118 (daily ed. June 25, 2008) (statement of Sen. Bond), https://www.congress.gov/crec/2008/06/25/CREC-2008-06-25.pdf.
[99] *See* 50 U.S.C. § 1881(a)(a).
[100] *See id.* § 1881(b)–(d).
[101] *See* Gannon, *supra* note 33, at 81, (citing Elizabeth B. Bazan, The Foreign Intelligence Surveillance Act: Comparison of the Senate Amendment to H.R. 3773 and the House Amendment to the Senate Amendment to H.R. 3773 (Cong. Research Serv., RL34,533), (July 7, 2008)); Elizabeth B. Bazan, Cong. Research Serv., RL34279, The Foreign Intelligence

When the House of Representatives first passed successor legislation to the Protect America Act in November 2007, the legislation did not require individualized judicial review to conduct surveillance for United States persons overseas.[102] Rather, at a subsequent time, Senators Ron Wyden, Russ Feingold, and Sheldon Whitehouse introduced legislation requiring judicial review of the surveillance of United States persons abroad,[103] an amendment referred to as the "Wyden Amendment."[104] Those in favor of the Wyden Amendment believed that Americans' rights should not diminish when located outside of the United States.[105] Those opposing the amendment pointed out that the executive branch had not abused its authorities in collecting foreign intelligence information on United States persons abroad under Executive Order 12333, Section 2.5, which had governed the acquisition of information relating to United States persons abroad before the FAA.[106]

Critics of the Wyden Amendment voiced misgivings about broadening

---

Surveillance Act: A Brief Overview of Selected Issues (2008), http://fpc.state.gov/documents/organization/101789.pdf.

[102] *See id.*

[103] *See id.* (citing FAA, S. REP. NO. 110-209, *supra* note 78, at 29).

[104] FAA, S. REP. NO. 110-209, *supra* note 78, at 29 (statement of Sen. Chambliss) ("Senator Wyden introduced, and [SSCI] adopted, an amendment requiring that any time a U.S. person is the target of surveillance, regardless of where the collection occurs, the Attorney General must seek FISC approval for that collection.").

[105] *See id.* (quoting FAA, S. REP. NO. 110–209, *supra* note 78, at 50, (minority views of Senators Feingold and Wyden).

[106] *See id.* (citing FAA, S. REP. NO. 110–209, *supra* note 78, at 39, 50 (additional views of Senators Bond, Chambliss, Hatch and Warner). Mr. Gannon also noted that some senators believed that the amendment was "an attempt by Congress to micromanage the Intelligence Community." *see also* KRIS & WILSON, *supra* note 32, § 17:14 (noting that until the FAA, the acquisition of information relating to United States persons abroad "was not regulated by any statute—it was outside FISA's definition of 'electronic surveillance' and 'physical search,' and therefore not subject to the exclusivity provision or the statute's civil and criminal penalty provision for unauthorized acquisition. Instead, such acquisition was conducted under Section 2.5 of Exe. Order No. 12333." EO 12333, as amended, section 2.5, provides in pertinent part that "The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power." Exec. Order No. 12333, *United States Intelligence Activities*, as amended by Exec. Order Nos. 13284 (2003), 13355 (2004) and 13470 (2008).

the scope of judicial review for the collection of foreign intelligence information on those outside of the United States. For example, Kenneth Wainstein, then Assistant Attorney General, expressed concerns that the Wyden Amendment "would extend the role of the FISA Court, for the first time, outside our borders" by mandating judicial review for the surveillance of United States persons who were acting as agents of a foreign power outside the United States.[107] Similarly, Patrick Philbin, former Deputy Assistant Attorney General Department of Justice, Office of Legal Counsel noted: "In light of the limited purpose for which surveillance of U.S. citizens overseas is conducted, coupled with the lack of evidence of abuse, there is no reason to impair the flexibility of highly sensitive intelligence and counterterrorism investigations by adopting a warrant requirement in this context."[108]

Eventually, the Wyden Amendment was adopted into the language of the FAA. In passing the FAA, members of Congress recognized that they were expanding the scope of the FISC by requiring, for the first time, individual FISC orders finding probable cause to acquire foreign intelligence information of United States person outside of the United States.[109] Prior to the enactment of the FAA, the surveillance of United States persons overseas remained principally within the executive branch's discretion and was

---

[107] FISA Amendments: How to Protect Americans' Security and Privacy and Preserve the Rule of Law and Government Accountability: Hearing Before the S. Comm. On the Judiciary, 110th Cong. (2007) (statement of then Assistant Attorney General Kenneth Wainstein)).
[108] *Id.* (statement of Patrick Philbin, former Deputy Assistant Atty. General Department of Justice, Office of Legal Counsel)).
[109] Under the FAA, "for the first time, a court order must be obtained to conduct electronic surveillance for foreign intelligence purposes against an American who is located outside the United States." 154 CONG. REC. S6122 (daily ed. June 25, 2008) (statement of Sen. Chambliss). Indeed, the FAA, Section 702 "went farther than any legislation in history in protecting the privacy interests of American citizens or U.S. persons whose communications might be acquired through targeting overseas." 154 CONG. REC. S6118 (daily ed. June 25, 2008) (statement of Sen. Bond). As noted by Professor Donohue, "Congress itself was intensely aware that in passing the FAA, it was invoking its authority under separation of powers doctrine, to limit the scope of executive action when it came to gathering foreign intelligence." Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, *supra* note 19, at 204.

conducted under Section 2.5 of Executive Order 12333.[110] The FAA was a "significant departure" from the way in which the executive branch had conducted surveillance to collect foreign intelligence information.[111] As explained by Professor Donohue, the "FAA altered the *status quo*, requiring the government to go to a court to obtain an individualized order, prior to targeting a U.S. person overseas."[112] Professor Donohue further noted that the FAA was fundamentally different from how FISA had previously worked and introduced new statutory restrictions in a field previously under the purview of Executive Order 12333, Section 2.5.[113] The FAA eliminated the executive branch's ability to conduct surveillance of United States persons abroad to collect foreign intelligence information without first seeking judicial approval.

E. FAA Section 702, Procedures for Targeting Certain Persons Outside the United States Other than United States Persons

1. Certification to the FISC

To understand FAA Section 702 and its procedural safeguards, a brief overview if its statutory framework is provided in this section. Prior to

---

[110] *See* Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, *supra* note 19, at 80; *see also* KRIS & WILSON, *supra* note 32, § 16:6 (explaining that prior to 2008, "if a U.S. citizen traveled to Paris and telephoned another U.S. citizen in London, the U.S. government was always able (as a legal matter) to monitor the call without a warrant under FISA. And that was the case regardless of where the government did the monitoring—*i.e.*, even if the call was routed through the United States and wiretapped here").

[111] Gannon, *supra* note 33, at 60, 69 (citing 154 CONG. REC. S257 (daily ed. Jan. 24, 2008) (statement of Sen. Rockefeller)). Before the enactment of the FAA in 2008, the surveillance of United States persons abroad was governed by Executive Order 12333. As noted by Kris and Wilson, the FAA "largely displaces Section 2.5 [of EO 12333] by subjecting surveillance and searches of U.S. persons abroad to approval by the FISC." KRIS & WILSON, *supra* note 32, § 17:1. As reflected in the legislative history of the FAA, Congress knew that it was expanding FISA's reach to United States persons abroad, noting for example that the FAA "ensures that the Government cannot conduct electronic surveillance on an American anywhere in the world without a warrant. *No legislation has done that up to this point*." 154 CONG. REC. S6119 (daily ed. June 25, 2008) (statement of Sen. Feinstein) (emphasis added).

[112] Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, *supra* note 19, at 204.

[113] *See id.* at 154*; see also* KRIS & WILSON, *supra* note 32, § 17:14.

collecting information under Section 702, the Attorney General and Director of National Intelligence must submit a written certification to the FISC, attesting, among other factors that: (1) targeting and minimization procedures are in place, they have been approved by the FISC, and they are consistent with the Fourth Amendment;[114] (2) procedures are in place to ensure compliance with the limitations of Section 702;[115] (3) "a significant purpose of the acquisition is to obtain foreign intelligence information;"[116] and (4) "the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider."[117] Section 702 explicitly prohibits the intentional targeting of: (1) "any person known at the time of acquisition to be located in the United States;" (2) "a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;" (3) "a United States person reasonably believed to be located outside the United States;" or (4) "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."[118] Further, Section 702 mandates that acquisitions under this statute must comply with the requirements of the Fourth Amendment.[119]

2. Minimization Procedures

Before conducting surveillance under Section 702, minimization procedures must be submitted to the FISC for review and approval. Minimization procedures are statutorily required procedures that are designed

---

[114] *See* 50 U.S.C. § 1881(a)(g)(2)(A)(i), (ii), (iv).
[115] *Id.* § 1881(a)(g)(2)(A)(iii).
[116] *Id.* § 1881(a)(g)(2)(A)(v).
[117] *Id.* § 1881(a)(g)(2)(A)(vi).
[118] *Id.* § 1881(a)(b)(1)–(4).
[119] *Id.* § 1881(a)(b)(5).

to ensure that United States person information is protected.[120] The acquisition, retention, and dissemination of non-publicly available United States person information collected under Section 702 must comply with minimization procedures to protect United States persons privacy interests.[121] For example, with respect to the retention of data, under the NSA Section 702 minimization procedures, if information acquired under Section 702 has not been determined to be foreign intelligence information or evidence of a crime, such information generally ages off NSA systems within five years of the expiration of the certification.[122] If the Section 702 information has been acquired from the NSA's upstream collection, the data generally ages off NSA systems within two years of the expiration of the certification.[123] With respect to the dissemination of Section 702 information, under the FBI Section 702 minimization procedures United States person information may only be disseminated if the information "reasonably appears to be foreign intelligence information," "necessary to understand foreign intelligence information or assess its importance," or "reasonably appears to be evidence of a crime."[124]

---

[120] As defined in 50 U.S.C. § 1801(h), minimization procedures are "specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h).

[121] *See* 50 U.S.C. § 1881(a)(c)(1).

[122] *See FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 5–6.

[123] *See id.*; for a description of "upstream" collection, *see* Part I.E of this article.

[124] FBI MINIMIZATION PROCEDURES, *supra* note 17, at 1, 30-31; CIA MINIMIZATION PROCEDURES, *supra* note 17, 1, 4 (The CIA minimization procedures contain similar language in that they only permit the dissemination of a United States person's identity if "such person's identity is necessary to understand foreign intelligence information or assess its importance."); NSA MINIMIZATION PROCEDURES, *supra* note 17, 1, 14–15 (NSA's minimization procedures contain similar language as well); *see Release of 2015 Section 702 Minimization Procedures*, *supra* note 17. On August 11, 2016, the ODNI, in consultation with the Department of Justice, released the 2015 NSA Section 702 Minimization Procedures, 2015 FBI Section 702 Minimization Procedures, 2015 CIA Section 702 Minimization Procedures, and 2015 NCTC Section 702 Minimization Procedures.

3. Targeting Procedures

In addition to minimization procedures, targeting procedures must be followed. Targeting procedures require that the acquisition of foreign intelligence information is limited to targeting persons reasonably believed to be located outside the United States, and must prevent the intentional acquisition of any communication in which both the sender and intended recipients of the communications are known to be in the United States at the time of the acquisition.[125] NSA's targeting procedures require that the selector, such as an email address or telephone number, is used by a non-United States person reasonably believed to be located outside the United States.[126] An NSA analyst must carefully review information in the NSA's possession to determine whether a potential target is a non-United States person outside of the United States and document such decision.[127] Once an NSA analyst has concluded that a potential target is a non-United States person overseas, two senior NSA analysts must approve the determination.[128] NSA's decision is subsequently reviewed by the Department of Justice.[129]

4. FISC Review of Section 702 Certification Request

Following the required submissions to the FISC, the court reviews the certification packet to ensure that it meets the statutory requirement.[130] For example, the FISC must ensure that the targeting and minimization

---

[125] *See* 50 U.S.C. § 1881(a)(d)(1).
[126] *See FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 4–5.
[127] *See id.* at 5; *see also Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy and Civil Liberties, Hearing before the S. Comm. on the Judiciary Oversight*, 114th CONG. 2 (2016) (statement of David Medine, Former Chairman, Privacy and Civil Liberties Oversight Board), https://www.pclob.gov/library/20160510-SJC%20Medine%20Testimony.pdf.
[128] *See Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy and Civil Liberties, Hearing before the S. Comm. on the Judiciary Oversight*, *supra* note 127, at 2.
[129] *See FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary, supra* note 3, at 5.
[130] *See* 50 U.S.C. § 1881(a)(i).

procedures are consistent with the Fourth Amendment.[131] If the FISC believes that the government's submissions are inadequate, the FISC requires that the government provide additional information.[132] The FISC must evaluate the government's submissions to determine whether a proposed certification meets all statutory and constitutional requirements.[133] If the Court finds that submitted certification complies with these requirements, the FISC will approve the government's certification.[134]

5. Acquisition of Information under Section 702

If the FISC is satisfied that the statutory and constitutional requirements are met and approves the government's certification, the AG and DNI may issue a directive to an electronic communications service provider requiring its assistance to "immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition" and maintain "any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain."[135] After the government issues such a directive, the government can then identify specific selectors, such as telephone numbers or email addresses, that are associated

---

131 *See id.*

132 *See FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 4; § 1881(a)(g)(1)(B) (If "time does not permit the submission of a certification" as described above, the AG and DNI may authorize the acquisition of foreign intelligence information of non-U.S. persons outside of the United States without prior judicial approval. However, within seven days of making such determination, the AG and DNI must submit a certification to the FISC seeking such authorization"); *see also Redacted*, 2011 WL 10947772, *supra* note 18 (discussing that in 2011, the FISC determined that NSA's targeting and minimization procedures, as the government proposed to implement them in connection with MCTs, were not consistent with the Fourth Amendment. After the NSA modified its minimization procedures, the FISC found that the government adequately corrected the deficiencies and that the revised procedures complied with both the statute and the Fourth Amendment).

133 *See FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 4.

134 *See* 50 U.S.C. § 1881(a)(i)(3)(A; *see also* Case Redacted, Mem. Op. and Order (FISA Ct. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

135 50 U.S.C. § 1881(a)(h)(1)(A)-(B).

with targeted persons.[136] A provider has complete civil immunity for providing assistance to the government pursuant to a directive.[137] Further, a provider has the option of challenging a directive by filing a petition with the FISC.[138]

Information is collected under Section 702 in two ways: "PRISM" and "Upstream."[139]

1. In PRISM collection, the government identifies a specific user's account that it seeks to monitor, and then sends a selector, such as an email address or telephone number, to the appropriate electronic communications service provider to begin collection.[140]

2. Under upstream collection, NSA acquires electronic communications as they cross the Internet "backbone" within the United States.[141] Upstream collection allows the NSA to collect electronic communications that contain the targeted selector—such as an e-mail address—within the body of a communication between two third parties. This method of collection, often referred to as an "abouts" collection.[142] NSA also conducts upstream collection to acquire "telephony calls."[143] In contrast to the upstream collection of Internet communications (e.g., emails), NSA's upstream collection of telephony calls "only acquires communications that are to or from a specified telephone number of similar selector, not communications that are 'about' the tasked telephone

---

136 *See Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, 1, 7 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf; *see also* Jewel v. National Security Agency, No. C 08–04373, WL 545925, at *1 (N.D. Cal. Feb. 10, 2015*)* (detailing further background on the steps of the process).

137 *See* KRIS & WILSON, *supra* note 32, § 17:10 (citing to 50 U.S.C. § 1881(a)(h)(3)).

138 *See* 50 U.S.C. § 1881(a)(h)(4). For further discussion of challenging a directive, *see* KRIS & WILSON, *supra* note 32, § 17:10.

139 United States v. Hasbajrami, 11-CR-623 (JG), 2016 WL 1029500, at *6 (E.D.N.Y. Mar. 8, 2016) (citing PCLOB 702 REPORT, *supra* note 11, at 7, 33).

140 *See id.* (citing PCLOB SECTION 702, *supra* note 11, at 32–33).

141 *FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 5. For example, with upstream collection, both "messages sent to and from a target's e-mail address, like BadGuy@ISP.com, [as well as] messages sent between non-targets that mention BadGuy@ISP.com (the e-mail address, not merely the name)" are collected. For further an in-depth description of "PRISM" and "upstream" collection, *see Redacted*, 2011 WL 10945618, *supra* note 18; *see also Redacted*, 2011 WL 10947772, *supra* note 18.

142 *Id.*

143 *Id.*

number."[144]

6. Oversight of Surveillance under Section 702

Extensive oversight of the implementation of Section 702 is conducted by all three branches of the government.[145] As recognized by Robert Litt, General Counsel, Office of the Director of National Intelligence, the Intelligence Community is committed to ensuring that its acquisition and use of Section 702 is "consistent with the law, the FISC's orders, and the protection of the privacy and civil liberties of Americans."[146] Congressionally mandated reports and audits concerning Section 702 include:

- At least every six months, the Attorney General and Director of National Intelligence must submit a report to the FISC and relevant congressional committees assessing compliance with the targeting and minimization procedures;[147]

- The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under Section 702 must conduct certain reviews. The OIG is required to provide a copy of each such review to the Attorney General, the Director of National Intelligence, and relevant congressional committees.[148]

---

144 *FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary, supra* note 3, at 5.
145 Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, *supra* note 19, at 140 ("The FAA created numerous reporting requirements."); 154 CONG. REC. S6126 (daily ed. June 25, 2008) (statement of Sen. Hatch). As noted by Senator Hatch in the legislative history of the FAA, built into the statutory scheme are many layers of oversight regulating the collection of information under Section 702. Senator Hatch detailed the "multiple oversight initiatives" placed in Section 702, including "audits conducted by the Inspector Generals of the Department of Justice and elements of the Intelligence Community, the Attorney General, and Director of National Intelligence." Senator Hatch believed that the level of oversight was so "onerous" that "the amount of oversight in this bill should be revisited in the future . . . to mandate more realistic and appropriate levels of review." Senator Hatch continued: "The multiple oversight initiatives in this legislation are not fulfilled by magic. It takes a tremendous amount of time and resources by the very analysts whose primary job is to track terrorists. As great as our analysts are, they can't be two places at once. There are only so many of them, and they don't have unlimited resources."
146 *FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary, supra* note 3, at 7.
147 50 U.S.C. § 1881(a)(l)(1) (requiring that reports to Congress be submitted to the House Permanent Select Committee on Intelligence, the Senate Select Committees on Intelligence, and the House and Senate Committee on the Judiciary).
148 50 U.S.C. § 1881(a)(l)(2). The OIGs must review the number of: (1) "disseminated intelligence reports containing a reference to a United States-person identity;" and (2) targets

- The head of each element of the intelligence community conducting an acquisition authorized under Section 702 must conduct an annual review to determine certain information about its Section 702 collection. The annual report must be provided to the FISC, Attorney General, the Director of National Intelligence, and relevant congressional committees.[149]

- At least every six months, the Attorney General must submit a report to the relevant congressional committees containing information including any certifications submitted, any directives issued, a description of the judicial review of such certifications and targeting and minimization procedures, any compliance reviews conducted by the Attorney General or the Director of National Intelligence, and a description of any incidents of noncompliance.[150]

In addition to these congressionally mandated reviews and reports, other oversight requirements and safeguards include:

- Approximately every two months, DOJ, NSD and ODNI conduct compliance reviews of the NSA, FBI, and CIA's application of its Section 702 minimization and/or targeting procedures.[151] DOJ reports all noncompliance incidents with the implementation of Section 702 to the FISC and and relevant congressional committees.

- Under Rule 13 of the FISC Rules of Procedure, the government must report non-compliance incidents to the FISC of any FISC-approved authorities that were "implemented in a manner that did not comply with the Court's authorization or approval or with applicable law."[152]
- The Privacy and Civil Liberties Oversight Board conducted an extensive review of the government's use of Section 702 and issued a comprehensive report on July 2, 2014, entitled, *Report on the*

---

that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed."

[149] 50 U.S.C. § 1881(a)(l)(3). The annual review must provide, information such as the number of "disseminated intelligence reports containing a reference to a United States-person identity" and "the number of targets that were later determined to be located in the United States."

[150] 50 U.S.C. § 1881(f) (requiring that reports must be submitted to the House Permanent Select Committee on Intelligence, the Senate Select Committee on Intelligence, and the House and Senate Committees on the Judiciary).

[151] *See Release of a Summary of DOJ and ODNI Oversight of Section 702*, *supra* note 17.

[152] UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT, RULES OF PROCEDURE, Rule 13 (2010), http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf [hereinafter FISC RULES OF PROCEDURE].

Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act.[153]

- Under Executive Orders 12333, as amended, and 13462, as amended, the head of each element of the intelligence community must report intelligence activities of their respective element to the President's Intelligence Oversight Board that they have reason to believe may be unlawful or contrary to executive order or presidential directive.[154]

- Judicial review in other courts "where Section 702 obtained or derived information has been used against criminal defendants."[155]

In sum, Section 702 governs the surveillance of non-United States persons reasonably believed to be located outside the United States to collect foreign intelligence information.[156] Collection under Section 702 does not require individual judicial orders authorizing the acquisition of foreign intelligence information against each individual.[157] Rather, the FISC considers whether the statutory and constitutional requirements for the certification have been met, and if satisfied, approves the annual certifications submitted by the Attorney General and the Director of National Intelligence.[158] Pursuant to the certifications, and subject to FISC-approved targeting and minimization procedures and a rigorous oversight regime, the government is able to acquire foreign intelligence information on non-United States person overseas without obtaining FISC approval for each individual collection.

F. FAA Section 703 (Acquisition Inside the United States Targeting United States Persons Outside the United States), Section 704 (Other Acquisitions Targeting United

---

153 PCLOB SECTION 702, *supra* note 11.
154 Exec. Order No. 12333, as amended, *supra* note 106; *President's Intelligence Advisory Board and Intelligence Oversight Board*, Exec. Order No. 13462, as amended by Exec. Order 13516 (2009).
155 *FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 8*; see, e.g.*, *Mem. Opinion and Order*, *supra* note 134; United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749 (D. Or., June 24, 2014), *aff'd*, United States. v. Mohamud, No. 14-30217, 2106 WL 7046751 (9th Cir., Dec. 5, 2016), http://cdn.ca9.uscourts.gov/datastore/opinions/2016/12/05/14-30217.pdf; *Hasbajrami*, *supra* note 139.
156 *See* 50 U.S.C. § 1881(a)(a) (2008).
157 *Section 702 of the Foreign Intelligence Surveillance Act*, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, IC ON THE RECORD, https://icontherecord.tumblr.com/topics/section-702.
158 *Id.*

States person Outside the United States), Section 705 (Joint Applications and Concurrent Authorizations)

While Section 702 governs the collection of foreign intelligence information of *non-United States persons* reasonably believed to be located outside the United States, Sections 703, 704, and 705 govern the collection of foreign intelligence information of *United States person*s located outside of the United States. Section 703 (50 U.S.C. § 1881b) and Section 704 (50 U.S.C. § 1881c) may be used to acquire foreign intelligence information of a United States person reasonably believed to be located outside the United States.[159] Before issuing an order authorizing the collection of such information under Sections 703 and 704, the FISC must make a probable cause finding that the target is: (1) "reasonably believed to be located outside the United States;"[160] and (2) "a foreign power, an agent of a foreign power, or an officer or employee of a foreign power" as defined in FISA.[161] The FISC must also

---

[159] 50 U.S.C. § 1881(b)(a); § 1881(c)(a)–(c).

[160] 50 U.S.C. § 1881(b).

[161] 50 U.S.C. § 1881(b)(b)(1)(C)(ii); 50 U.S.C. § 1881(c)(b)(3)(B). Under 50 U.S.C. § 1801(b), "agent of a foreign power" is defined as:

> (1) any person other than a United States person, who--
>
> (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section, irrespective of whether the person is inside the United States;
>
> (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
>
> (C) engages in international terrorism or activities in preparation therefore;
>
> (D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or
>
> (E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or
>
> (2) any person who--
>
> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

determine that the proposed minimization procedures are sufficient under these sections.[162] When the government seeks to collect foreign intelligence information on a United States person abroad, and expects to collect the information both inside and outside of the United States, the FISC can authorize both collections under Section 705.[163]

G. Reauthorization of the FISA Amendments Act

On December 30, 2012, Congress reauthorized the FAA for five years.[164] Other than extending the expiration date of the statute, no other substantive modifications were made. In reauthorizing Section 702, Congress noted that it was necessary to extend Section 702 because the intelligence acquired under Section 702 is essential to maintaining our national security. Congress believed that the information collected under Section 702 is "often unique, unavailable from any other source, and regularly provides critically important insights and operationally actionable intelligence on terrorists and foreign intelligence targets around the world."[165] Additionally, based upon numerous briefings, the Senate Select Committee on Intelligence found that:

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

[162] *See* 50 U.S.C. § 1881(c)(c)(1)(C).
[163] *See* 50 U.S.C. § 1881(d)(a).
[164] *See* FISA Amendments Act Reauthorization Act of 2012*,* House Report 112-645*, 2d Session Part 2* (2012), https://www.congress.gov/congressional-report/112th-congress/house-report/645/2 (discussing H.R. 5949)
[165] *Id.*

> the authorities provided under the FISA Amendments Act have greatly increased the government's ability to collect information and act quickly against important foreign intelligence targets. The Committee has also found that Title VII has been implemented with attention to protecting the privacy and civil liberties of United States persons, and has been the subject of extensive oversight by the Executive branch, the FISC, as well as the Congress.[166]

The current sunset date is for the FAA is December 31, 2017."[167]

II. CONSTITUTIONAL AUTHORITIES SUPPORTING THE COLLECTION OF FOREIGN INTELLIGENCE INFORMATION

In addition to providing a historical overview of the FAA, including Section 702, a discussion of the constitutional parameters of United States surveillance authorities is necessary to place Section 702 in context. At the outset, and as will be discussed further in Section III.C, it is noted that Congress, in passing the Foreign Intelligence Surveillance Act and its subsequent amendments (including the FAA, Section 702), placed constraints upon executive branch authorities beyond what is constitutionally mandated.[168] This article proposes returning some of those authorities back to the executive branch.

As reflected in the previous section, determining where to draw the line in regulating the executive branch's use of surveillance to collect foreign intelligence information, *i.e.*, authorization within the executive branch or judicial branch, highlights an inherent tension between Article II of the United States Constitution and the Fourth Amendment. On the one hand, under Article II, the President is constitutionally mandated to protect the

---

[166] FAA Sunsets Extension Act of 2012, S. Rept. 112-174 (June 7, 2012), https://www.congress.gov/congressional-report/112th-congress/senate-report/174/1.
[167] FISA Amendments Act Reauthorization Act of 2012*,* House Report 112-645*,* 2d Session Part 2 (2012) https://www.congress.gov/congressional-report/112th-congress/house-report/645/2 (discussing H.R. 5949).
[168] *See, e.g.*, *Keith*, *supra* note 30, at 315-16; *Truong Dinh Hung*, *supra* note 91, at 914–15.

national security interests of the United States.[169] On the other hand, the Fourth Amendment provides protections from unreasonable searches and seizures by our government.[170] These two deeply-rooted, and sometime competing, interests must be balanced to determine whether surveillance by the executive branch is reasonable under the Fourth Amendment. To understand how these interests are evaluated in the context of the acquisition of foreign intelligence information, significant cases addressing this issue will be highlighted.

The Fourth Amendment of the United States Constitution provides as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[171]

In *United States v. United States District Court for the Eastern District of Michigan (Keith)*, the Supreme Court was presented with the question of weighing individual privacy interests under the Fourth Amendment with the President's inherent duty to protect our country under Article II.[172] The Supreme Court considered whether the President's authorities, through the Attorney General, to authorize electronic surveillance in *internal security matters* without first obtaining a warrant was permissible under the Fourth Amendment.[173] To determine whether a warrant was required under the Fourth Amendment, the *Keith* Court balanced privacy and free expression with the government's

---

[169] *See Keith*, *supra* note 30, at 310.
[170] *See* discussion about *Verdugo–Urquidez, supra* note 23.
[171] U.S. Const. amend. IV; *see In re Directives*, *supra* note 82, at 1009. Under the Fourth Amendment, one must consider: (1) whether there is an exception to the Warrant Clause of the Fourth Amendment; and (2) whether the search conducted is reasonable.
[172] *See Keith*, *supra* note 30, at 299, 324 ("The issue before us . . . involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval.").
[173] *See Keith*, *supra* note 30, at 299.

responsibility to protect the domestic security of our country.[174] The *Keith* Court recognized that "the President of the United States has the fundamental duty, under Art. II, § 1, of the Constitution, to 'preserve, protect and defend the Constitution of the United States.'"[175] After weighing the President's Article II responsibilities with the individual interests of privacy and free expression, the Supreme Court concluded that the government must obtain a warrant before it conducts surveillance related to the *domestic* security of our country.[176] However, the Court left unanswered the question of whether a warrant was required for the President to conduct surveillance to collect foreign intelligence information in the United States and abroad.[177]

While the Supreme Court left open the question of whether the Fourth Amendment required a warrant with respect to the acquisition of foreign intelligence information,[178] federal appellate courts have consistently held that, under Article II, the President has inherent authority to conduct surveillance within the United States for foreign intelligence purposes without judicial review.[179] A year following the *Keith* decision, the Third Circuit, in *United States v. Butenko,* considered whether a warrant was required to conduct a search solely for the purpose of obtaining foreign intelligence information.[180] In this proceeding, the government relied upon the

---

[174] *See id.* at 314–15.
[175] *Id.* at 310 (quoting U.S. Const. Art. II, § 1).
[176] *See id.* at 321.
[177] *See id.* at 308.
[178] *See Keith*, *supra* note 30, at 308.
[179] *See* Bradbury, *supra* note 33, at 13 n. 31 (citing *Truong Dinh Hung*, *supra* note 91, at 914-15; United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); *but see* Zweibon v. Mitchell, 516 F.2d 594, 619-20 (D.C. Cir. 1975) (en banc) (plurality opinion suggesting in dicta that a warrant may be required even in a foreign intelligence investigation)); *see also In re Directives*, *supra* note 82, at 1012 ("a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States"); *Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *15 ("[Section] 702 surveillance falls within the foreign intelligence exception to the warrant requirement.").
[180] *See Butenko, supra* note 179, at 596, 605. In *Butenko*, A. Ivanov, a Soviet national, and John Butenko, an American by birth, were convicted of conspiring to transmit or communicate "to a foreign government . . . information relating to the national defense" of the United States. In

warrantless electronic surveillance of a United States person and a non-United States person who were in the United States at the time of the surveillance.[181] Defendants challenged the constitutionality of the warrantless collection. In rejecting the defendants' claim that the government's warrantless electronic surveillance violated their Fourth Amendment rights, the Third Circuit recognized the presidential authority to handle foreign affairs as set forth in Article II of the Constitution.[182] After balancing the government's need to collect foreign intelligence information with individual privacy rights,[183] the *Butenko* Court concluded that a warrantless surveillance did not violate defendants' Fourth Amendment rights because the surveillances was reasonable and conducted for the purpose of collecting foreign intelligence information.[184]

Likewise, the Fourth Circuit recognized a foreign intelligence exception to the warrant requirement in *United States v. Truong Dihn Hung*.[185] In challenging their convictions, the defendants argued that the warrantless surveillance conducted by the FBI violated the Fourth Amendment, and as a result, the evidence obtained through such surveillance must be suppressed.[186] The *Truong* Court rejected the defendants' argument, recognizing a foreign intelligence exception to the Warrant Clause of the Fourth Amendment. Specifically, the Court concluded that "because of the need of the executive branch for flexibility, its practical experience, and its constitutional

---

this proceeding, the government relied upon electronic surveillance that it had obtained without a warrant.

[181] *See id.*

[182] *See id.* at 603 (noting that the authority for the President to conduct electronic surveillance is "implied from his duty to conduct the nation's foreign affairs").

[183] *See id.* at 596.

[184] *See id.* at 605–606 (quoting finding of district court judge).

[185] *See Truong Dinh Hung*, *supra* note 91, at 911–12. Truong Dinh Hung (a Vietnamese citizen living in the United States) and Ronald Humphrey (a United States person and an employee of the United States Information Agency) were convicted of several espionage-related offenses. As part of the investigation, the government conducted electronic surveillance on Truong's telephones and placed a microphone in his apartment without a warrant. Rather, the government had received approval of the surveillance from the Attorney General.

[186] *See id.*

competence, the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance."[187] The *Truong* court, as well as all courts that have considered this issue, have concluded that the President has the inherent authority to conduct warrantless surveillance to obtain foreign intelligence information.[188]

While these decisions recognize the executive branch's inherent authority to conduct warrantless surveillance within the United States to collect foreign intelligence information, the search must satisfy the reasonableness requirement of the Fourth Amendment.[189] As the Supreme Court explained in *United States v. Knights*, the "touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'"[190] The Foreign Intelligence Surveillance Court of Review considered the reasonableness requirement in *In re Directives [redacted] Pursuant to Section 105B of The Foreign Intelligence Surveillance Act*.[191] In this case, the FISCR reviewed whether the warrantless collection of foreign intelligence information of persons overseas under the PAA was reasonable under the Fourth Amendment.[192] In reaching its decision, the FISCR noted that it must weigh national security interests against the Fourth

---

[187] *Id.* at 914–95 (citing *Butenko, supra* note 179; *Brown, supra* note 179; United States v. Clay, 430 F.2d 165 (5 Cir. 1970); *contra Zweibon*, *, supra* note 179 (dictum in plurality opinion in case involving surveillance of domestic organization having an effect on foreign relations but acting neither as the agent of nor in collaboration with a foreign power).

[188] *Truong Dinh Hung*, *supra* note 91; *see In re Sealed Case*, *supra* note 90, at 742 (noting that although "the plurality opinion in *Zweibon* suggested the contrary in dicta, it did not decide the issue.").

[189] Illinois v. McArthur, 531 U.S. 326, 330 (2001) (quoting Texas v. Brown, 460 U.S. 730, 739, 103 S. Ct. 1535, 75 L.Ed.2d 502 (1983)) (stating that the Fourth Amendment's "'central requirement' is one of reasonableness").

[190] *United States v. Knights*, 534 U.S. 112, 118–19 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[191] *See In re Directives*, *supra* note 82, at 1012 ("[W]e must determine whether the protections afforded to the privacy rights of targeted persons are reasonable in light of this [national security] important interest."); *See* discussion of *In re Directives*, *supra* Part I.C.

[192] *See In re Directives*, *supra* note 82, at 1006.

Amendment privacy interests of United States persons.[193] After balancing these two interests, the FISCR affirmed the FISC's decision that the search was reasonable under the Fourth Amendment.[194]

III. CONGRESS SHOULD RESTORE EXECUTIVE BRANCH AUTHORITIES TO PERMIT THE COLLECTION OF FOREIGN INTELLIGENCE INFORMATION OF BOTH UNITED STATES AND NON-UNITED STATES PERSONS OVERSEAS WITHOUT INDIVIDUALIZED JUDICIAL REVIEW, WITH ADDED PROTECTIONS FOR UNITED STATES PERSONS

A. Threat of Americans Joining Terrorist Groups Abroad

With the historical context and the constitutional parameters of Section 702 in mind, this section contemplates whether certain legal authorities should be restored to the executive branch. Due to the increasing threat of Americans joining terrorist organizations around the world,[195] this article proposes a modification to Section 702 to return certain authorities back to the executive branch where they had resided prior to 2008, namely the collection of foreign intelligence information on both United States and non-United States persons overseas without individualized judicial review for each collection, with additional safeguards for United States persons. In September 2015, the United States House of Representatives Homeland Security Committee released a comprehensive report documenting the growing threat to the United States from Americans who assist or join terrorist groups abroad.[196] The Homeland Security Committee determined

---

193 *See id.*

194 *See id.* at 1007; *see also* In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 157, 167 (2d Cir. 2008) ("The Fourth Amendment's warrant requirement does not govern searches conducted abroad by U.S. agents; such searches of U.S. citizens need only satisfy the Fourth Amendment's reasonableness requirement.").

195 *See, e.g.*, David S. Kris, *Trends And Predictions In Foreign Intelligence Surveillance: The FAA And Beyond*, 8 J. NAT'L SECURITY L. & POL'Y 3 (2016) at 389 (citing John McLaughlin, *The Paris Attacks: Former CIA Chief Weighs In*, OZY (Nov. 15, 2015), http://www.ozy.com/pov/the-paris-attacks-former-cia-chief-weighs-in/66155) ("By late 2015, ISIL had probably recruited at least 4,500 Westerners to its cause, many of them with European passports, and some of whom returned to Europe to conduct attacks.").

196 *See* HOMELAND SECURITY COMMITTEE REPORT, *supra* note 2, at 2 (explaining that in March 2015, the U.S. House of Representatives Homeland Security Committee launched a bipartisan

that more than 250 Americans thus far have attempted or succeeded in traveling to Syria and Iraq to fight with militant groups.[197] The Committee found that the threat of Americans assisting or joining terrorist overseas terrorist organization presents a "serious counterterrorism challenge" for the United States.[198] With respect Syria, in late 2013, dozens of Americans had sought to join Syrian rebels; in July 2014, around 100 had tried to join; and by July 2015, more than 250 American sought to join terrorist groups in Syria.[199]

As the Homeland Security Committee indicates, "many U.S. suspects have tread a common path: espousing their support for ISIS on social media and then attempting to leave America, en route to the so-called caliphate."[200] Once these United States citizens reach Syria or their intended destination, they attempt to recruit other Americans to join them.[201] Moreover, several dozen of these citizens have returned to the United States.[202] One of those who had returned was arrested for planning a terrorist attack against a United States military base.[203] The Homeland Security Committee cautioned that the "unprecedented speed at which Americans are being radicalized by violent extremists is straining federal law enforcement's ability to monitor and intercept suspects."[204]

Task Force on Combating Terrorist and Foreign Fighter Travel. Eight Members of Congress were assigned to examine the threat to the United States from "foreign fighters"—individuals who leave home, travel abroad to terrorist safe havens, and join or assist violent extremist groups. The Task Force assessed domestic and overseas efforts to obstruct terrorist travel, as well as security gaps).

[197] *See id.* at 15 (citing Barbara Starr, *A Few Dozen Americans' in ISIS Ranks*, CNN, July 15, 2015, http://www.cnn.com/2015/07/15/politics/isis-american-recruits/).

[198] *Id.* at 15.

[199] *See id.* at 16 (citations omitted).

[200] *Id.* Here, ISIS stands for the Islamic State of Iran and Syria. Other names have been used for this terrorist group, including ISIL (Islamic State of Iraq and Levant) and IS (Islamic State). Because the United States House of Representatives Homeland Security Committee refers to this terrorist organization as "ISIS," this terrorist group generally will be referred to as "ISIS" throughout this article. *See* HOMELAND SECURITY COMMITTEE REPORT, *supra* note 2.

[201] *See id.*

[202] *See* HOMELAND SECURITY COMMITTEE REPORT, *supra* note 2, at 6.

[203] *See id.* at 8 (citing John Bacon, *Ohio Man Accused of Planning U.S. Terror Strike*, USA TODAY, Apr. 16, 2015, http://www.usatoday.com/story/news/na- tion/2015/04/16/ohio-indicted-islamic-state-terrorism/25879443/.

[204] *Id.* at 6; *see* Jeremy Diamond, *Congressional Report: U.S. Has 'Failed' to Stop Flow of Foreign Fighters to ISIS*, CNN (Sept. 29, 2015), http://www.cnn.com/2015/09/29/politics/foreign-

Whereas the Homeland Security Committee report focuses on Americans joining ISIS, other reports demonstrate that this disquieting phenomenon extends beyond Syria and Iraq. In a February 2015 report, the Anti-Defamation League reported that a group of Americans who traveled to Somalia to fight with Al Shabaab, a terrorist group with links to al-Qaeda, were described by the FBI as one of the "highest priorities in anti-terrorism."[205] At least 50 United States citizens and permanent residents are thought to have joined, attempted to join, or aided Al Shabaab since 2007.[206] Americans continue to attempt to join this terrorist group.[207] The FBI believes that these individuals have been recruited by Al Shabaab both on the Internet and in person."[208] Furthermore, the FBI is concerned that these Americans may return to the United States and attempt to commit terrorist acts in our country.[209]

---

fighters-isis-congressional-task-force-report/ ("The U.S. is losing the battle to stop Americans from traveling abroad to enlist in ISIS, a bipartisan congressional task force concluded in a report released Tuesday."); Ed Payne, *More Americans volunteering to help ISIS*, CNN (Mar. 5, 2015), http://www.cnn.com/2015/03/05/us/isis-us-arrests/ (providing an overview of individual accounts of United States persons attempting to join or joining ISIS). For example, Abdi Nur, after leaving Minnesota for Syria in 2014, "spent months persuading his friends in Minneapolis to join him. His peer-to-peer recruiting nearly worked, as six of his friends attempted to leave the United States for Syria." HOMELAND SECURITY COMMITTEE REPORT, *supra* note 2, at 16 (citing Evan Perez and Shimon Prokupecz, *ISIS Arrests Highlight Role of American Recruiter*, CNN (Apr. 20, 2015), http://www.cnn.com/2015/04/20/politics/isis-minnesota-arrests-abdi-nur/); *see* Andrew Grossman, Ben Kesling, and Tamara Audi, *Federal Authorities Arrest Six Men in Minneapolis and San Diego on Charges Related to a Terrorism Investigation,* WALL ST. J. (Apr. 20, 2015), http://www.wsj.com/articles/terrorism-probe-yields-six-arrests-u-s-authorities-say-1429518994 ("Six Minnesota men were charged Monday in connection with attempts to join Islamic State, following a 10-month investigation into a network of young Somali-Americans that authorities say underscores the power of Westerners who have traveled overseas to recruit friends back home to join extremist groups."). As another example, "Ohio suspect Abdirahman Sheik Mohamud was urged by his brother Aden to join him overseas." HOMELAND SECURITY COMMITTEE REPORT, *supra* note 2, at 16 (citing *Columbus, Ohio, Man Charged with Providing Material Support to Terrorists*, U.S. DEPARTMENT OF JUSTICE, OFFICE OF PUBLIC AFFAIRS (Apr. 16, 2015), http://www.justice.gov/opa/pr/columbus-ohio-man-charged- providing-material-support-terrorists). Mohamud "agreed to join him and left the United States for Syria, though his brother was later killed in the fighting."

[205] ANTI-DEFAMATION LEAGUE REPORT, AL SHABAAB'S AMERICAN RECRUITS, *supra* note 2, at 1.

[206] *See id.*

[207] *See id.*

[208] *Id.*

[209] *See id.* One of these recruits, 22-year-old Abidsalan Hussein Ali from Minneapolis, "was one of two suicide bombers who attacked African Union troops on October 29, 2011." Ali is the

While Americans leaving the United States to join terrorist organizations increased through mid-2015, within the last year, the number of Americans traveling abroad to join terrorist groups has declined.[210] Despite this decline, James Comey, Director, FBI, noted that ISIS is "still attracting 'troubled souls' through social media who pose potential terror threats, resulting in more than 1,000 active FBI investigations into online recruitment — a slight increase from over a year ago."[211] He also noted that the FBI was still deeply concerned about the threat of foreign fighters returning to either the United States or to western Europe.[212] Likewise, Matt Olsen recognized that the number of Americans and citizens of "visa waiver" countries in Europe who have traveled to Syria and Iraq to fight "raises the real danger that these individuals could be deployed here to conduct attacks similar to the attacks in Paris and Brussels."[213] Mr. Olsen noted that ISIS continues to "target Americans for recruitment, including through the use of focused social media, in order to identify and mobilize operatives here."[214]

B. Proposed Modification to Section 702

Based upon these events, and with the increasing globalization of terrorist organizations and their sophisticated ability to recruit new members, Congress should consider enhanced surveillance tools, within constitutional limits, that might help the United States anticipate future terrorist threats. Any revisions to the surveillance authorities must include appropriate

---

"third American Al Shabaab suicide bomber." The first, Shirwa Ahmed, "carried out a suicide bombing at the Ethiopian Consulate and the presidential palace in Hargeisa killing 24 people in October 2009." The second, Farah Mohamad Beledi, "carried out a suicide bombing on May 30, 2011, targeting a military base outside Mogadishu, the Somali capital, killing two African Union peacekeepers and a Somali soldier." Further, "Al Shabaab claimed that three Americans took part in its assault on the Westgate Mall in Nairobi, Kenya, on September 21, 2013."

[210] *See* Michael Isikoff, *Steep Decline in U.S. Recruits To ISIS, FBI Chief James Comey Says*, YAHOO! NEWS (May 11, 2016), https://www.yahoo.com/news/steep-decline-in-us-recruits-to-isis-fbi-chief-212138680.html.

[211] *Id.* (citing to comments by James Comey).

[212] *See id.*

[213] Stmt. of Olsen, *supra* note 2, at 3.

[214] *See id.*

safeguards for United States person privacy interests. As such, this article proposes that Section 702 should be strengthened to authorize the collection of foreign intelligence information on both United States and non-United States persons overseas without individualized judicial review, subject to additional judicial oversight for United States persons. In setting forth this proposed change, the following concepts are highlighted:

1. Under Article II, the President has a duty to protect the United States.[215] The Fourth Amendment provides protections to United States persons, and persons in the United States who have developed substantial connections with this country, from unreasonable searches and seizures by our government.[216] These two fundamental interests must be balanced to determine whether surveillance without individualized judicial review is reasonable under the Fourth Amendment.

2. The President has the constitutional authority to collect foreign intelligence information without first seeking judicial approval, *e.g.*, foreign intelligence exception to the Fourth Amendment Warrant Clause. If a person is protected by the Fourth Amendment, the surveillance of that persons must meet the reasonableness requirement.[217]

3. As originally enacted, FISA only governed the collection of foreign intelligence information inside of the United States. FISA did not govern international calls or electronic communications of United States persons abroad.[218]

4. With evolving technologies, more communications fell within the scope of FISA; this development resulted in the need to seek FISC approval to acquire such communications where previously such judicial review had not been required.

---

[215] U.S. Const. art. II; *see Keith*, *supra* note 30, at 315–16; *Truong Dinh Hung*, *supra* note 91, at 914–15.
[216] U.S. Const. IV amend; *see Verdugo-Urquidez*, *supra* note 23, at 270–71 (citing *Plyler, supra* note 23, at 212).
[217] *See Keith*, *supra* note 30, at 315–16; *Truong Dinh Hung*, *supra* note 91, at 914–15.
[218] *See* Elizabeth B. Bazan and Jennifer K. Elsea, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, CONG. RESEARCH SERV., 20 (2006) https://www.fas.org/sgp/crs/intel/m010506.pdf.

5. The attacks of September 11, 2001 precipitated a recognition of the need for the intelligence community to conduct surveillance of international communications and oversea targets at a much greater speed and with increased flexibility.[219] Seeking individual FISC orders for international and oversea communications under the outdated version of FISA no longer proved feasible.[220]

6. The 2007 PAA permitted the warrantless collection of foreign intelligence information of both United States and non-United States persons outside of the United States.[221] The FISCR concluded that the warrantless acquisition of foreign intelligence information under the PAA was reasonable under the Fourth Amendment.[222]

7. The 2008 FAA, for the first time, requires the executive branch to obtain individual FISC approval each time it seeks to acquire foreign intelligence information of United States persons outside of the United States. The process of preparing FISA applications and presenting them to the FISC is "substantial" [223] and is beyond what is constitutionally mandated.[224]

8. The FAA mandates extensive safeguards and oversight provisions to protect the privacy interests of United States persons, including minimization procedures, targeting procedures, mandatory reviews, and mandatory reports to the FISC and Congress. In addition, oversight of the implementation of Section 702 includes compliance with FISC Rules of Procedure, the PCLOB review, and requirements of Executive Order 13462, as amended. Reviews have uniformly determined that the executive branch has not intentionally misused any of its authorities under Section 702.[225]

---

[219] *See Open Hearing on Legislative Proposals for Modifying NSA Programs and Amending FISA Authorities: Open Hearing before the H. Permanent Select Comm. on Intelligence*, 113th Cong. 12 (2013) (testimony of Steven Bradbury, former head of the Office of Legal Counsel in the United States Dept. of Justice), http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/bradbury10292013.pdf.

[220] *See id.*

[221] *See* Protect America Act of 2007, *supra* note 81.

[222] *See In re Directives*, *supra* note 82, at 1016.

[223] *See, e.g., Cordero, supra* note 49.

[224] *See Keith*, *supra* note 30, at 315–16; *see also Truong Dinh Hung*, *supra* note 91, at 914–15.

[225] *FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary, supra* note 3, at 1–2.

> 9. With the increasing globalization of terrorist organizations and their sophisticated ability to recruit new members, the United States must anticipate future threats and ensure that our country has the necessary legal authorities to counter them, including the ability to act with speed and agility in the collection of foreign intelligence information. The Homeland Security Committee cautioned that the "unprecedented speed at which Americans are being radicalized by violent extremists is straining federal law enforcement's ability to monitor and intercept suspects."[226]

In light of these guiding principles, Section 702 should be strengthened to permit the collection of foreign intelligence information of both United States and non-United States persons abroad without seeking individualized judicial review. Returning these authorities to the executive branch will provide it with the essential flexibility that it needs to collect foreign intelligence information on terrorist groups overseas, including United States persons who join them. While individualized judicial approval would not be required, the acquisition would be subject to the statutory protections of Section 702. For example, the government must comply with FISC-approved targeting and minimization procedures pertaining to United States person information.[227] Further, the extensive oversight provisions would apply to this collection, such as congressionally mandated reports and audits.[228]

In addition to the statutory requirements and oversight mechanisms pursuant to the FAA, collection of United States person information would be subject to the requirements set forth in Executive Order 12333, as amended, section 2.5, which provides:

> *Attorney General Approval.* The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the

---

226 HOMELAND SECURITY COMMITTEE REPORT, *supra* note 2, at 6.
227 *See* 50 U.S.C. § 1801(h) (2015); *see also* 50 U.S.C.S. § 1881(a)(c)(1), (d)(1); *see also* Benjamin Wittes, *The Minimization and Targeting Procedures: An Analysis*, LAWFARE (June 23, 2013, 4:19 PM), https://lawfareblog.com/minimization-and-targeting-procedures-analysis.
228 *See, e.g.*, Exec. Order No. 12333, as amended, *supra* note 106; Exec. Order No. 13462, as amended, *supra* note 154; 50 U.S.C. §§ 1881(a)(l)(1)–(l)(3), 1881(f); PCLOB SECTION 702, *supra* note 11.

> United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.[229]

The proposed modifications to the FAA would no longer mandate individualized findings of probable cause *by the FISC* to conduct surveillance of a United States person abroad. Rather, under the proposed statutory structure, the authority to determine probable cause to conduct surveillance of United States persons overseas would reside within the executive branch. Under the recommended framework, pursuant to Executive Order 12333, Section 2.5, before collecting foreign intelligence information on a United States person overseas, the Attorney General must make a probable cause finding that surveillance is conducted "against a foreign power or an agent of a foreign power."[230] In other words, the Attorney General would determine probable cause—rather than the FISC—that surveillance is conducted "against a foreign power or an agent of a foreign power." As such, the authority for deciding probable cause would return to the executive branch where it had resided before the enactment of the FAA in 2008.[231]

To ensure that United States persons' privacy interests are protected under the proposed framework, in addition to the protections currently mandated by Section 702, this article proposes one more: the FISC should conduct oversight of the AG's probable cause findings under Executive Order 12333 Section 2.5 with respect to United States persons.[232] This

---

[229] EO 12333, Section 2.5, *supra* note 106 (providing that the authority delegated to the Attorney General, including "the authority to approve the use of electronic surveillance as defined in the Foreign Intelligence Surveillance Act of 1978, as amended, shall be exercised in accordance with that Act").

[230] *Id.; see supra* note 161 for definition of "agent of a foreign power" under 50 U.S.C. § 1801(b).

[231] *See In re Directives, supra* note 82.

[232] Thank you to Judge James Baker and Professor William Buzbee for their suggestion of additional oversight of the AG's probable cause findings under EO 12333 Section 2.5 with respect to United State persons.

judicial oversight is critical to the proposed changes to Section 702. While returning the authority to conduct surveillance of United States persons overseas to the executive branch, the judicial branch would provide oversight of these executive branch decisions. Such oversight could be conducted as part of the FISC's review of the government's certification requests that are submitted to the court on an annual basis. To accomplish this oversight, language should be added to the FAA requiring that the Attorney General, as part of the annual certification process, provide the FISC with a report documenting the number of AG probable cause determinations for United States persons that were authorized pursuant to Executive Order 12333, Section 2.5, and a description of the basis for each determination. The FISC would then be required to review these AG probable cause determinations to ensure that they are consistent with the Fourth Amendment and Executive Order 12333, Section 2.5.

Based upon the above discussion, the proposed modifications to the FAA include:

- Delete the words "other than United States persons" from the language in the title of 50 U.S.C. § 1881a (§ 702).[233]
- Repeal 50 U.S.C. § 1881a(b)(3).[234]
- Repeal 50 U.S.C. § 1881b (§ 703), *Certain acquisitions inside the United States targeting United States person outside the United State*s.[235]
- Repeal 50 U.S.C. § 1881c (§ 704), *Other acquisitions targeting United States person outside the United States*.[236]

---

[233] *See* 50 U.S.C. § 1881(a).
[234] *See id.* § 1881(a)(b)(3) (prohibiting the intentional targeting of a "United States person reasonably believed to be located outside the United States").
[235] *See id.* § 1881(b)(c) (requiring FISC must make a probable cause finding that the United States person is: (1) "reasonably believed to be located outside the United States;" and (2) "a foreign power, an agent of a foreign power, or an officer or employee of a foreign power" as defined in FISA).
[236] *See id.* § 1881(c)(c) (stating that FISC must make a probable cause finding that the United States person is (1) "reasonably believed to be located outside the United States;" and (2) "a foreign power, an agent of a foreign power, or an officer or employee of a foreign power").

- Repeal 50 U.S.C. § 1881d (§ 705), *Joint applications and concurrent authorizations*.[237]

- Repeal 50 U.S.C. §§ 1881f(b)(2) and 1881f(b)(3), *Congressional oversight*.[238]

- Add language mandating FISC review of the AG probable cause determinations pursuant to Executive Order 12333, Section 2.5, as part of the annual certification process. For example:

    - Under 50 U.S.C. § 1881a(g)(2), *Certification Requirements*, add a requirement that the Attorney General, as part of the annual certification review, provide the FISC with a report documenting the number of AG probable cause determinations made to authorize surveillance on United States persons pursuant to Executive Order 12333, Section 2.5, and a description of the basis for each such determination, including facts establishing probable cause that the technique is directed against a foreign power or an agent of a foreign power.

    - Under 50 U.S.C. § 1881a(i), *Judicial review of certification and procedures*, add language requiring FISC assessment of whether such AG probable cause determinations are consistent with the Fourth Amendment and Executive Order 12333, Section 2.5.[239]

---

[237] *See id.* § 1881(d)(a) ("[i]f an acquisition targeting a United States person under section 1881(b) or 1881(c) of this title is proposed to be conducted both inside and outside the United States, a judge having jurisdiction under section 1881(b)(a)(1) or 1881(c)(a)(1) of this title may issue simultaneously, upon the request of the Government in a joint application complying with the requirements of sections 1881b(b) and 1881c(b) of this title, orders under sections 1881b(c) and 1881c(c) of this title, as appropriate.").

[238] *See* 50 U.S.C. §§ 1881(f)(b)(2), (3) (requiring reports to Congress for surveillance conducted under 50 U.S.C. §§ 1881(b) and 1881(c) containing the total number of applications made for orders, the total number of such orders, the total number of emergency acquisitions authorized by the Attorney General, and the total number of subsequent orders approving or denying such applications).

[239] *See* 50 U.S.C. § 1881(a)(i). The current statute states that a FISC shall review a certification submitted by the Attorney General or Director of National Intelligence to assure it meets the required targeting and minimization procedures.

Pursuant to this proposed framework, the executive branch would have the flexibility to quickly begin surveillance on United States persons outside of the United States where there is probable cause to believe that such person is acting as a foreign power or an agent of a foreign power. Importantly, the executive branch's probable cause determinations would be subject to judicial oversight to ensure adherence to the Fourth Amendment and the standards set forth in Executive Order 12333, Section 2.5.

C. The Proposed Modifications to Section 702 Comply with the Fourth Amendment

Fundamentally, while the proposed modifications to Section 702 will provide the executive branch with stronger surveillance tools and greater flexibility to protect our national security interests, such modifications must comport with the requirements of the Fourth Amendment of the Constitution. For United States persons, who are afforded Fourth Amendment protections both inside and outside of the United States, the collection of this information must be consistent with the Fourth Amendment.[240] Currently, Section 702 places statutory constraints upon the executive branch beyond what is constitutionally mandated.[241] Under the Fourth Amendment, two issues must be considered: (1) whether the search conducted under the Fourth Amendment requires a warrant; and (2) whether the search conducted under the Fourth Amendment is reasonable.[242] As

---

[240] *See, e.g.*, *Verdugo-Urquidez*, *supra* note 23, at 270–71; *Keith*, *supra* note 30, at 315–16; United States v. Barona, 56 F.3d 1087, 1096 (9th Cir. 1995) (quoting *Verdugo-Urquidez*, *supra* note 23, at 1234 (Wallace, J., dissenting)) (discussing that the term "People of the United States" includes "American citizens at home and abroad"); *Truong Dinh Hung*, *supra* note 91, at 914-15; United States v. Bin Laden, 126 F. Supp. 2d 264, 284–86 (S.D.N.Y. 2000).

[241] *See Truong Dinh Hung*, *supra* note 91, at 914–15; *see also Butenko*, *supra* note 179, at 605 (holding that the President has the constitutional authority to collect foreign intelligence information without first seeking judicial approval under the foreign intelligence exception to the Fourth Amendment Warrant Clause); *see also Keith*, *supra* note 30 (holding that the government must obtain a warrant before it conducts surveillance related to the *domestic* security of our country, but leaving unanswered the question of whether a warrant was required for the President to conduct surveillance to collect foreign intelligence information in the United States and abroad).

[242] *See In re Directives, supra* note 82, at 1012.

discussed in Section II, courts recognize a foreign intelligence exception to the Warrant Clause of the Fourth Amendment.[243] Because courts recognize a foreign intelligence exception to the Warrant Clause, the next issue to be considered is whether the proposed changes to Section 702 meet the reasonableness requirement. In *In re Directives*, the FISCR considered whether the acquisition of foreign intelligence information under the PAA (which permitted overseas collection of foreign intelligence information of both United States and non-United States persons) was reasonable.[244] In doing so, the FISCR, applying Supreme Court precedent, employed a "totality of the circumstances" test, balancing individual privacy interests with the governmental interest at stake.[245] The FISCR recognized that "the relevant governmental interest—the interest in national security—is of the highest order of magnitude."[246] The court continued that it must consider whether the privacy interests of targeted person are reasonable in light of the strong national security interests.[247]

The court, employing the totality of the circumstances test, considered several factors to determine whether the privacy protections in the PAA and those required under the certifications and directives established reasonableness under the Fourth Amendment.[248] Applying a totality of the

---

[243] *See, e.g.*, *Truong Dinh Hung*, *supra* note 91, at 914–15; *Buck*, *supra* note 179, at 875; *Butenko*, *supra* note 179, at 605; *In re Directives, supra* note 82, at 1012; *Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *15.

[244] *See In re Directives, supra* note 82, at 1012.

[245] *Id.* (citing *Samson*, *supra* note 89, at 848; *Gardner*, *supra* note 89, at 8–9)); *see Mohamud*, No. 14-30217, *supra* note 155 at *18 (quoting Maryland v. King, 133 S.Ct. 1958, 1970 (2013) (in deciding reasonableness, the Ninth Circuit examined the totality of the circumstances and weighed "'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy'"); *see also* Donohue, *supra* note 19, at 252-63, for a thorough discussion about the reasonable standard as it relates to the collection of information pursuant to Section 702.

[246] *In re Directives, supra* note 82, at 1012 (citing *Agee*, *supra* note 90, at 307; *In re Sealed Case*, *supra* note 90, at 746).

[247] *See id.* at 1013.

[248] *Id.* The factors that the FISCR balanced to make this determination included: (1) targeting procedures, (2) minimization procedures, and (3) procedures to ensure that a "significant purpose of a surveillance is to obtain foreign intelligence information," (4) procedures incorporated through Executive Order 12333, section 2.5, and (5) procedures outlined "in an affidavit supporting the certifications."

circumstances test to the proposed modification to Section 702, four of the factors set forth in *In re Directives* will be considered, including (1) targeting procedures, (2) minimization procedures, (3) procedures to ensure that a "significant purpose of a surveillance is to obtain foreign intelligence," and (4) compliance with Executive Order 12333, section 2.5.[249] In addition to these four issues, the extensive oversight of the implementation of Section 702 is considered.

Under the "totality circumstances" test set forth in *In re Directives*, the proposed changes to the FAA satisfy the reasonableness standard under the Fourth Amendment. First, prior to collecting information under Section 702, the Attorney General and Director of National Intelligence must submit a written certification to the FISC attesting that a significant purpose of the collection is to acquire foreign intelligence information.[250] Second, the proposed modification to Section 702 will be subject to minimization procedures to protect United States persons' information.[251] Third, targeting procedures will ensure that the collection is directed at persons located outside of the United States.[252] The fourth factor to consider is compliance with Executive Order 12333, as amended, section 2.5.[253] While the proposed modifications to the FAA would no longer mandate an individualized finding

---

[249] *Id.* at 1012.

[250] *See* 50 U.S.C. § 1881(a)(g) (emphasis added). The government cannot target anyone under the court-approved procedures for Section 702 collection "unless there is an appropriate, and documented, foreign intelligence purpose for the acquisition."

[251] As discussed in section I.D.1, minimization procedures, which play an integral role in protecting privacy interests of United States persons, are statutorily required procedures that are designed to ensure that United States personal information is protected. 50 U.S.C. § 1801(h) states that minimization procedures are "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1); *see* FBI, CIA, AND NSA SECTION 702 MINIMIZATION PROCEDURES, *supra* note 17.

[252] 50 U.S.C. § 1881(a)(d)(1). Under the proposed Section 702, the targeting procedures would follow the language in 50 U.S.C. § 1881(a)(d)(1) to ensure that acquisition "is limited to targeting persons reasonably believed to be located outside the United States" and to "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."

[253] *See* Executive Order No. 12333, *supra* note 106.

of probable cause by the FISC to conduct surveillance of a United States person abroad, pursuant to Executive Order 12333, the Attorney General must determine that there is probable cause to believe that surveillance is conducted against a foreign power or an agent of a foreign power.[254] Under the proposed framework, the FISC would conduct oversight of the AG's probable cause findings with respect to United States persons overseas to ensure compliance with the Fourth Amendment and Executive Order 12333.

Finally, in evaluating the reasonableness of the proposed changes, the oversight requirements must be considered. Oversight of Section 702 is conducted by all three branches of our government.[255] These oversight regimes ensure that the executive branch complies with the Fourth Amendment, statutory requirements, minimization procedures, and targeting procedures. For example, the FISC engages in a comprehensive review of submitted certifications.[256] As more FISC opinions are publicly released, one can see the careful analysis that goes into deciding complex issues that arise

---

[254] *See id.*

[255] *See, e.g.*, Exec. Order No. 12333, *supra* note 106; Exec. Order No. 13462, *supra* note 154, 50 U.S.C. §§ 1881(a)(l)(1)–(3); 50 U.S.C. § 1881(a)(f); PCLOB SECTION 702, *supra* note 11; FISC RULES OF PROCEDURE, *supra* note 152.

[256] 50 U.S.C. § 1881(a)(i)(3)(A), (B). Targeting and minimization procedures must also be submitted to the FISC to determine whether they are consistent with the Fourth Amendment and meet the statutory requirements. If the FISC determines that these criteria are met, it may approve the certification and the use of the procedures for acquisition. If the FISC determines that these requirements have not been met, the FISC will order the government to "correct any deficiency identified by the Court" or "cease, or not begin, the implementation of the authorization for which such certification was submitted." Contrary to a belief that the FISC is merely a "rubber stamp" for the executive branch's requests, this is not the case. Letter from Reggie B. Walton, Presiding J., U.S. Foreign Intelligence Surveillance Ct., to the Hon. Patrick Leahy, Chairman, Comm. on the Judiciary, U.S. Senate (July 29, 2013), http://fas.org/irp/news/2013/07/fisc-leahy.pdf (explaining that FISC is not a "rubber stamp" court). Judge Walton explained that the FISC's approval rate of applications "reflect only the number of final applications submitted to and acted on by the Court. These statistics do not reflect the fact that many applications are altered prior to final submission or even withheld from final submission entirely, often after an indication that a judge would not approve them." *Id.* at 3. As further explained by Judge Walton, "Notably, the approval rating for Title III wiretap applications . . . is higher than the approval rate for FISA applications, even using the Attorney General's FISA statistics as the baseline for comparison, as recent statistics show that from 2008 through 2012, only five of 13,593 Title III wiretap applications were requested but not authorized." *Id.* at 3 n. 6.

before the FISC.[257] As another example, at least every six months the Attorney General and Director of National Intelligence must submit a report to the FISC and Congress assessing compliance with the targeting and minimization procedures.[258] In recent semiannual reports that were submitted to the FISC and Congress, and are now publicly released, the AG and DNI indicated that the NSA, FBI, and CIA implemented targeting and minimization procedures "in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702."[259] Likewise, the PCLOB conducted a thorough review of the use of Section 702 and "found no evidence of intentional abuse."[260]

Under the totality of the circumstances test, applying the factors discussed above, one can conclude that the proposed modifications to Section 702 are reasonable under the Fourth Amendment.[261] As recognized by the FISCR, combatting terrorism and collecting foreign intelligence information to counter threats to the United States are "of the highest order of magnitude."[262] The FISCR has noted that "there is a high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national

---

[257] *See, e.g.*, *In re Sealed Case*, *supra* note 90; *In re Directives, supra* note 82; *Redacted*, 2011 WL 10945618, *supra* note 18; *Redacted*, 2011 WL 10947772, *supra* note 18; FOREIGN INTELLIGENCE SURVEILLANCE COURT, PUBLIC FILINGS, http://www.fisc.uscourts.gov/public-filings (last visited Oct. 9, 2016); Office of the Dir. of Nat'l Intel., *Release of Three Opinions Issued by the Foreign Intelligence Surveillance Court*, IC ON THE RECORD (Apr. 19, 2016), https://icontherecord.tumblr.com/post/143070924983/release-of-three-opinions-issued-by-the-foreign. The June 2015 revisions to FISA under the USA FREEDOM Act likely will lead to greater transparency of the FISC's proceedings. Under the USA FREEDOM Act, the government must make "publicly available to the greatest extent practicable" each FISC or FISCR decision "that includes a significant construction or interpretation of any provision of law." 50 U.S.C.S. § 1872 (LexisNexis PL 114-29, approved Sept. 30, 2016).

[258] 50 U.S.C. § 1881(a)(l)(1) (2012) (reports to Congress must be submitted to the congressional intelligence committees and the Committees on the Judiciary of the House of Representatives and the Senate).

[259] *See Release of a Summary of DOJ and ODNI Oversight of Section 702*, *supra* note 17.

[260] PCLOB SECTION 702 REPORT, *supra* note 11, at 2.

[261] *See In re Directives, supra* note 82, at 1012.

[262] *Id.* (citing *Agee*, *supra* note 90, at 307).

security interests that are at stake."[263] Likewise, the Fourth Circuit recognized efforts to "counter foreign threats to the national security require the utmost stealth, speed, and secrecy."[264] The proposed modifications would strengthen United States surveillance authorities by providing the executive branch with the flexibility and speed that it needs to help protect the American public and our national security interests.[265]

In view of these compelling national security interests, the question then turns to whether privacy protections of targeted persons are reasonable.[266] Under the proposed framework, and as mandated by FISA, Executive Order 12333, and targeting and minimization procedures, United States person privacy interests are protected at all stages of the process, from collecting foreign intelligence information through using and disseminating such information. Moreover, statutorily mandated oversight of the modified Section 702 program would be conducted by all three branches of the government, ensuring that United States persons privacy interests are protected. Under the totality of the circumstances analysis, the proposed changes to the FAA would satisfy the reasonableness standard under the Fourth Amendment.[267]

IV. CONGRESS SHOULD NOT LIMIT THE ABILITY TO QUERY INFORMATION COLLECTED UNDER SECTION 702

In a recent article, *Trends and Predictions in Foreign Intelligence Surveillance, The FAA and Beyond*, David S. Kris, General Counsel of Intellectual Ventures, and former Assistant Attorney General for the United States Department of

---

[263] *Id.* at 1011 (citing *Truong Dinh Hung*, *supra* note 91, at 915) ("explaining that when the object of a surveillance is a foreign power or its collaborators, 'the government has the greatest need for speed, stealth, and secrecy'").
[264] *Truong Dinh Hung*, *supra* note 91, at 915.
[265] *See* 154 CONG. REC. S6118 (daily ed. June 25, 2008) (statement of Sen. Bond), https://www.congress.gov/crec/2008/06/25/CREC-2008-06-25.pdf. Section 702's "more agile targeting requirements" provide the Intelligence Community with the "ability to acquire important foreign intelligence information in a timely manner."
[266] *See In re Directives, supra* note 82, at 1012.
[267] *See id.* at 1012 (citing *Samson*, *supra* note 89, at 848; *Gardner*, *supra* note 89, 8–9).

Justice, National Security Division, predicts that the querying of information obtained under Section 702 with United States person identifiers will be one of the six issues most likely to be addressed while considering the reenactment of Section 702.[268] In fact, recently both Congress and scholars have proposed limitations to querying foreign intelligence information collected under Section 702.[269] This article maintains that adding statutory limitations to querying lawfully collected Section 702 information would create unnecessary obstacles in an area where no fix is needed.

As explained below, courts consistently have determined that the current procedures for querying Section 702 data comply with the requirements of the Fourth Amendment.[270] Further, protections exist for the querying of Section 702 data and the executive branch has a record of complying with

---

[268] *See* Kris, *supra* note [195], at 377–78. In his article, Kris predicts that there will be six major themes that "dominate" congressional debate in reenacting Section 702. Kris predicts the following issues will play a major role when Congress debates the reenactment of Section 702:

> [1] the "upstream" collection of communications about non-U.S. persons located abroad (less than 10 percent of FAA collection, and probably unavoidable for technical reasons); [2] U.S. person queries of FAA data (fewer than 200 conducted by NSA in 2013, more by other agencies); [3] statutorily required or forbidden sharing of raw FAA data with foreign partners (now dealt with through FISA Court-approved minimization procedures); [4] the authorized purposes of FAA collection (likely not to affect existing collection very much); [5] NSA compliance issues (already well publicized, dealt with by the court and congressional oversight, and unlikely to result in significant FAA amendments, but perhaps significant for the long run as the intelligence community moves data to the cloud); . . . [and 6] surveillance under Executive Order 12333, which is very likely to arise in connection with FAA renewal but is difficult to discuss at present because it is the subject of a forthcoming report from the PCLOB.

[269] *See id.* at 18–19 (citing Charlie Savage, *Statement at The Second Annual Cato Surveillance Conference, After FREEDOM: A Dialogue on NSA in the Post-Snowden Era*, NEW YORK TIMES, (Oct. 21. 2015)).

[270] *See Case Redacted*, *supra* note 134, at 44-45 (the FISC concluded that querying provisions set forth in the minimization procedures comply with the requirements of the Fourth Amendment because they "strike a reasonable balance between the privacy interests of United States persons and persons in the United States, on the one hand, and the government's national security interests, on the other"); *see also Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *26 (holding that querying of collected information is not a separate search and does not make surveillance conducted under Section 702 unreasonable under the Fourth Amendment); *see also Hasbajrami*, *supra* note 139, at *12 N. 20 (determining that it would be inconsistent to permit the government to review information in its possession, but prohibit queries of the same information).

these procedural safeguards.[271] The procedures for querying lawfully collected Section 702 information are found in FBI, NSA, and CIA minimization procedures which restrict what type of queries may be conducted.[272] For example, CIA Minimization Procedures state that its "queries must be reasonably likely to return foreign intelligence information."[273] Similarly, NSA Minimization Procedures require that queries be limited to "selection terms reasonably likely to return foreign intelligence information."[274] The FBI Minimization Procedures provide that queries must be designed "to find, extract, review, translate, and assess whether such [FISA-acquired] information reasonably appears to be foreign intelligence information, to be necessary to understand foreign intelligence information or assess its importance, or to be evidence of a crime."[275]

A. Recent Court Decisions Discussing Querying of Section 702 Information

In a November 2015 decision, the FISC considered whether the procedures for querying information collected under section 702, especially queries that were designed to return information concerning United States persons, were consistent with the Fourth Amendment and Section 702.[276] The FISC appointed an amicus curiae, Amy Jeffress, to address these issues through written and oral argument.[277] Ms. Jeffress focused on the FBI Minimization Procedures, and maintained that they "'go far beyond the

---

[271] *See Release of a Summary of DOJ and ODNI Oversight of Section 702*, *supra* note 17 (March 2014 at 8–11; Oct. 2014 at 8–10; June 2015 at 8–11; Sept. 2015 at 8-12; Feb. 2016 at 8–13; Nov. 2016 at 8–12) (noting that as part of its reviews, DOJ and ODNI review the querying of unminimized Section 702-acquired communications using United States person identifiers).
[272] *FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary, supra* note 3, at 6; Kris, *supra* note 195, at 395–96 n. 66.
[273] CIA MINIMIZATION PROCEDURES, *supra* note 17, at 3.
[274] NSA MINIMIZATION PROCEDURES, *supra* note 17, at 7.
[275] FBI MINIMIZATION PROCEDURES, *supra* note 17, at 11.
[276] *See Case Redacted*, *supra* note 134, at 6 (citing NSA MINIMIZATION PROCEDURES, *supra* note 17, at 7; FBI MINIMIZATION PROCEDURES, *supra* note 17, at 11-12; CIA MINIMIZATION PROCEDURES, *supra* note 17, at 3-4) (This opinion was publicly released by the DNI on April 19, 2016).
[277] Ms. Jeffress was appointed pursuant to 50 U.S.C. § 1803(i)(2)(B).

purpose for which the Section 702-acquired information is collected in permitting queries that are unrelated to national security.'"[278] The FISC disagreed with Ms. Jeffress' legal assertion.[279]

As explained by the court, FISA does not require that acquisitions under Section 702 be conducted *solely* for a foreign intelligence purpose.[280] Rather, an acquisition under Section 702 is permitted if the foreign intelligence purpose for the collection is only a significant purpose, and not the primary purpose, of the acquisition.[281] NSA's targeting procedures ensure that a significant purpose of each Section 702 targeting decision is for the acquisition of foreign intelligence information.[282] Moreover, FISA contemplates that the collection of information under Section 702 may be used in criminal proceedings.[283] For example, FISA explicitly mandates that the government develop procedures pertaining to the retention and dissemination of Section 702-acquired information that is evidence of a crime for law enforcement purposes.[284] As another safeguard, the FISC noted that the FBI Minimization Procedures place considerable limitations on the use and dissemination of information obtained from queries.[285] Based upon these

---

[278] *Case Redacted*, *supra* note 134, at 30 (quoting Amicus Br. for the Ct. at 19).
[279] *See id.* at 30–45.
[280] *See id.* at 31.
[281] *See id.* (citing *In re Sealed Case*, *supra* note 90, at 734 (pursuant to the "'significant purpose' standard, an acquisition under Section 702 is permissible 'even if 'foreign intelligence' is only a significant—not a primary—purpose' of the targeting decision.")).
[282] *See id.*
[283] *See Case Redacted*, *supra* note 134, at 32; *see also* 50 U.S.C. § 1801(h)(3) (providing in pertinent part that minimization procedures with respect to electronic surveillance include "procedures that allow for the retention and dissemination of 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 disseminated for law enforcement purposes").
[284] *See Case Redacted*, *supra* note 134, at 32. FISA does not "foreclose any examination or use of information acquired pursuant to Section 702 that lacks a purpose relating to foreign intelligence." The FISC pointed out that FISA requires that minimization procedures "'allow for the retention and dissemination of information that is evidence of a crime.'"
[285] *Id.* at 35. Further, as noted by David Kris, NSA's 2014 minimization procedures do not permit the "querying upstream (rather than downstream) data with U.S. person identifiers," and "neither the FBI nor the CIA has access to un-minimized upstream data." Kris, *supra* note 195, at 396 (citing U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE

considerations, the FISC concluded that the NSA, FBI, and CIA Minimization Procedures, including the querying provisions, comply with the statutory requirements.

The FISC also evaluated whether NSA, FBI, and CIA Minimization and Procedures were consistent with the requirements of the Fourth Amendment. The FISC primarily focused its analysis on the FBI's minimization procedures. The FISC concluded that the minimization procedures, including the querying procedures, complied with Fourth Amendment mandates. In reaching this decision, the FISC explained:

> [T]he purpose of permitting queries designed to elicit evidence of ordinary crimes is not entirely unconnected to foreign intelligence. Such queries are permitted in part to ensure that the FBI does not fail to identify the foreign-intelligence significance of information in its possession. One of the main criticisms of the government following the attacks of September 11, 2001, was its failure to identify and appropriately distribute information in its possession that could have been used to disrupt the plot.[286]

The FISC reiterated that the FBI Minimization Procedures place considerable restrictions on the use and dissemination of information derived from queries.[287] The FISC further noted that the FBI queries only a subset of the information that is collected by the government under Section 702.[288] For example, the FBI does not receive any unminimized information acquired through NSA's upstream collection under Section 702.[289] The Court also noted that FBI queries designed to obtain evidence of crimes unrelated to foreign intelligence "rarely, if ever," generate responsive results from data collected under Section 702.[290] Based upon these considerations, the FISC

SURVEILLANCE ACT OF 1978, AS AMENDED (2014), § 3(b)(5), https://www.dni.gov/files/documents/0928/2014%20NSA%20702%20Minimization%20Procedures.pdf; PCLOB SECTION 702 REPORT, *supra* note 11, at 7, 35, 161 n.571 ("Data from upstream collection is received only by the NSA: neither the CIA nor the FBI has access to unminimized upstream data").

[286] *Case Redacted*, *supra* note 134, at 42.

[287] *See id.*

[288] *Id.* at 43.

[289] *See Id.* (the "FBI acquires only a 'small portion' of the unminimized Section 702 collection").

[290] *Id.* at 44 (citing PCLOB 702 REPORT, *supra* note 11, at 59–60).

determined that the querying provisions of the FBI Minimization Procedures achieve a reasonable balance between the privacy interests of United States persons and the national security interests of our country.[291] Accordingly, the FISC concluded that the minimization procedures, including the querying provisions, comply with the mandates of the Fourth Amendment.[292]

Similar to the findings of the FISC, in *United States v. Mohamud*, the U.S. District Court for the District of Oregon recognized that "[S]ubsequent querying of a § 702 collection, even if U.S. person identifiers are used, *is not a separate search* and does not make § 702 surveillance unreasonable under the Fourth Amendment."[293] Likewise, in *United States v. Hasbajrami*, the U.S. District Court for the Eastern District of New York held that it would be inconsistent to permit the government to review information in its possession, but prohibit queries of the same information.[294] Specifically, the *Hasbajrami* Court wrote: "[i]t would be perverse to authorize the unrestricted review of lawfully collected information but then restrict the targeted review of the same information in response to tailored inquiries."[295]

B. Recent Congressional Activity Regarding the Querying of Section 702 Information

In 2014, 2015, and 2016, legislation was introduced in Congress to limit the FBI, CIA, and NSA's ability to query information collected pursuant to Section 702.[296] Most recently, in June 2016, Representatives Thomas Massie

---

[291] *Id.*

[292] *See Case Redacted*, *supra* note 134, at 44–45.

[293] *Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *26 (emphasis added). While the Ninth Circuit affirmed the *Mohamud* decision on appeal, the appellate court did not consider the issue of whether the querying of incidentally-collected communications was reasonable under the Fourth Amendment. *Mohamud*, No. 14-30217, *supra* note 155, at *15 (holding that because "no retention and querying of the incidentally-collected communications is at issue in this case, an argument regarding reasonableness was outside the scope of this court's review").

[294] *See Hasbajrami*, *supra* note 139, at *12 n. 20.

[295] *Id.* (quoting Gov't Br. at 71–72).

[296] *See Final Vote Results for Roll Call 321*, OFFICE OF THE CLERK, U.S. HOUSE OF REPRESENTATIVES (June 16, 2016), http://clerk.house.gov/evs/2016/roll321.xml (showing that the Massie Amendment recently was defeated in a 222-198 vote); Steven Nelson, *House Rejects NSA Reforms After Orlando Massacre Mass Murderer Omar Mateen Claims Another Victim: A*

and Zoe Lofgren introduced legislation (Massie Amendment) that would prohibit the appropriations of funds to query foreign intelligence information collected under Section 702 using a United States person identifier.[297] Representative Massie stated that he introduced the legislation to ensure that querying Section 702 information complies with the requirements of the Fourth Amendment.[298] He believed that probable cause and a warrant were required before the government could query information legally obtained and in its possession.[299] Similarly, Representative Lofgren advocated that the government should be prohibited from querying its databases for information concerning United States citizens without a warrant.[300]

In opposition to the Massie Amendment, Representative Christopher Stewart urged that the amendment be defeated, noting that Congress "should be focusing on thwarting terror attacks, not on thwarting the ability of intelligence professionals to investigate and to stop them."[301] Representative Rodney Frelinghuysen echoed these concerns, stating that the amendment would restrict the intelligence community's ability "to protect our national security and create an impediment to the government's ability to locate threat information already in its possession."[302] Representative Frelinghuysen further noted that "Lawful queries can enable analysts to identify potential terror plots, to identify foreign nations trying to hack into our networks, to locate foreign intelligence officers spying within our borders."[303]

Once-Popular Push for Privacy Protections Against 'Backdoor' Surveillance, U.S. NEWS, (June 16, 2016), http://www.usnews.com/news/articles/2016-06-16/house-rejects-nsa-reforms-after-orlando-massacre (finding that in 2015, "the House passed the measure in a 255-174 vote after an even more lopsided 293-123 victory in 2014. After both votes, the amendment was not considered by the Senate and was axed in budget deals brokered by more hawkish congressional leaders").

[297] *See* Amendment to H.R. 5293, as Reported Offered by Mr. Massie of Kentucky, https://lofgren.house.gov/uploadedfiles/massie_041_xml.pdf.

[298] *See* 162 CONG. REC. H3894 (daily ed. June 15, 2016) (statement of Representative Massie), https://www.congress.gov/crec/2016/06/15/CREC-2016-06-15-pt1-PgH3892-2.pdf.

[299] *See id.*

[300] *See id.* (statement of Representative Lofgren).

[301] *Id.* (statement of Representative Stewart). Representative Stewart further stated that "section 702 is an extremely powerful tool that has proven effective in disrupting terror plots."

[302] *Id.* (statement of Representative Frelinghuysen).

[303] *Id.*

Representative Robert Goodlatte believed that the amendment would prohibit the government from querying data already in its possession that had been legally collected under section 702.[304] On June 16, 2016, the Massie Amendment was defeated in a 222 to 198 vote.[305] One media outlet attributed the defeat of the amendment to the June 2016 Orlando attack.[306]

C. Recent Scholarship Discussing the Regarding the Querying of Section 702 Information

In a recently-published book, Professor Donohue raised concerns similar to those of Representatives Massie and Lofgren regarding the querying of information collected under Section 702.[307] Professor Donohue wrote that, under the current procedures, "[American] citizens' communications collected via Section 702 can now be mined using [American] citizens' information as part of the queries."[308] She is troubled about the querying of incidentally collected Section 702 information,[309] particularly in the context of criminal matters.[310] Professor Donohue expressed concern that the "FBI stores unminimized Section 702 data together with information obtained from traditional FISA orders, allowing agents to search both caches of information simultaneously."[311] She points out that FBI queries of Section 702 information may not be related to national security threats against our

---

304 *See* 162 CONG. REC. H3895 (statement of Representative Goodlatte).
305 *See Final Vote Results For Roll Call 321*, *supra* note 296. While this amendment recently was defeated in June 2016, the House passed the measure in 2015 (255–174 vote); in 2014, the same amendment was passed in "an even more lopsided 293–123" vote. Nelson, *supra* note 296. Following the passage of the amendment in 2014 and 2015 by the House, the amendment was not considered by the Senate and "was axed in budget deals."
306 *See* Nelson, *supra* note 296 ("U.S. citizen Omar Mateen's murder of 49 people at a Florida nightclub on Sunday appears to have doomed a legislative push to rein in warrantless surveillance with defeat of an amendment that twice passed by wide margins.").
307 *See* DONOHUE, *supra* note 20, at 72–74.
308 *Id.* at 73.
309 *See id.*
310 *See id.*
311 *Id.* at 73–74; Donohue, *supra* note 19, at 198; Kris, *supra* note 195, at 398. David Kris likewise noted that a "related question concerns the FBI's ability to query un-minimized FAA § 702 data for evidence of a crime, particularly a crime not related to foreign intelligence."

country.[312] Professor Donohue asserts that the querying of Section 702 information, including incidentally-collected information for criminal purposes, leads to a problematic convergence between criminal law and national security law raising Fourth Amendment concerns.[313] For example, Professor Donohue believes by allowing the FBI to query this data, information collected for foreign intelligence purposes can now be used for law enforcement purposes without the government demonstrating probable cause of criminal activity and in the absence of a warrant.[314]

The FISA Court of Review considered the dichotomy between criminal and intelligence investigations in 2002 in *In re Sealed*.[315] In this case, the FISA

---

[312] *See* DONOHUE, *supra* note 20.

[313] *Id.* at 74. As explained by Mr. Kris, United States persons' communications could be collected incidentally under Section 702 in several ways. Kris, *supra* note 195 at 396. For example, a United States person could communicate with an individual who is the target of the surveillance under Section 702. In this situation, the communication of the United States person is incidentally-collected information. Incidental collection may also be acquired when "two non-U.S. persons discuss a U.S. person." PCLOB SECTION 702 REPORT, *supra* note 11, at 6. With respect to upstream collection, a U.S. person's communication could be obtained as part of an "about" collection concerning an individual who is targeted. Kris, *supra* note 195, at 396.

[314] *See* DONOHUE, *supra* note 20. Professor Donohue also raises the issue that certain FISC orders, including those issued under Section 702, are similar, and may be considered, general warrants which are unconstitutional under the Fourth Amendment. *See id; see*, *e.g.*, *Steagald v. United States*, 451 U.S. 204, 220 (1981) (stating that the "Fourth Amendment was intended partly to protect against the abuses of the general warrants that had occurred in England and of the writs of assistance used in the Colonies"); *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (holding that the "Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched and the persons or things to be seized.'"). Whether FISC authorization under Section 702 constitutes a general warrant is beyond the scope of this article. Briefly however, and as discussed in Part II of this article, federal appellate courts, as well as the FISA Court of Review, consistently hold that, under Article II, the President has the inherent authority to conduct warrantless surveillance for foreign intelligence purposes. *See, e.g., Truong Dinh Hung*, *supra* note 91, at 914–15; *Butenko, supra* note 179, at 596, 605; *In re Sealed Case*, *supra* note 90, at 742; *In re Directives*, *supra* note 82, at 1012. These appellate courts recognize a foreign intelligence exception to the Warrant Clause of the Fourth Amendment. Likewise, as held in *United States v. Mohamud*, surveillance conducted under Section 702 surveillance "does not trigger the Warrant Clause" and falls within the foreign intelligence exception to the warrant requirement. *Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *15. As recognized in these decisions, a warrant is not required to acquire foreign intelligence information under Section 702. The Warrant Clause is not implicated in authorizing Section 702 surveillance.

[315] *See In re Sealed Case*, *supra* note 90. Prior to events of September 11, 2001, policies had been implemented to stovepipe information collected under intelligence authorities from criminal investigations. As found by the 9/11 Commission, these policies had a detrimental impact on the Intelligence Community's abilities to disrupt terrorist activities. THE 9/11 COMMISSION

Court of Review evaluated whether a barrier—known as "the wall"—between intelligence investigations and law enforcement investigations was mandated by statute or the Constitution.[316] After reviewing the arguments set forth by the government as well as amici, the FISA Court of Review concluded that the wall between intelligence and law enforcement investigations was not mandated by FISA or the Constitution.[317] Notably, the Court believed that FISA did not "preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution."[318]

With respect to the concern of querying Section 702 for purely criminal investigative purposes, it is noteworthy that layers of statutory and procedural safeguards are built into the Section 702 querying provisions to protect constitutional privacy interests.[319] Courts have considered the impact of querying this data on privacy interests and have concluded that the querying procedures present no Fourth Amendment impediments.[320] As discussed above, the FISC considered whether procedures for querying information collected under section 702, including for criminal purposes, were consistent with the Fourth Amendment.[321] The FISC observed that FISA-mandated and FISC-approved minimization procedures place substantial constraints upon the government's ability to acquire, retain, query, and disseminate

---

REPORT, 78-80, 271 (July 2004), https://9-11commission.gov/report. In sharing frustration about the barrier between criminal and intelligence investigations, in August 2001, shortly before the attacks, an FBI agent presciently wrote: "Whatever has happened to this--someday someone will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.'" *Id.* at 271.

316 *See In re Sealed Case*, *supra* note 90, at 721.

317 *Id.* at 719–20.

318 *Id.* at 727.

319 *See*, *e.g.*, 50 § 1881(a)(b)(1)-(4), 50 U.S.C. § 1881(a)(g)(2); FBI MINIMIZATION PROCEDURES, *supra* note 17; CIA MINIMIZATION PROCEDURES, *supra* 17; NSA MINIMIZATION PROCEDURES, *supra* note 17.

320 *See Case Redacted*, *supra* note 134, at 6; *Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *26; *Hasbajrami*, *supra* note 139, at *12 n. 20.

321 *Case Redacted*, *supra* note 134, at 6 (citing NSA MINIMIZATION PROCEDURES, *supra* note 17, at 7; FBI MINIMIZATION PROCEDURES, *supra* note 17, at 11–12; CIA MINIMIZATION PROCEDURES, *supra* note 17, at 3-4) (This opinion was publicly released by the DNI on April 19, 2016).

information obtained under Section 702.[322] Moreover, the FISC recognized that the purpose of allowing queries that were designed to obtain information about possible crimes is not completely disassociated with foreign intelligence information.[323] The FISC comprehensively reviewed the Fourth Amendment implications and concluded that the minimization procedures, including the querying provisions, strike a reasonable balance between the privacy interests of United States persons and the national security interests of our country, and thus, comply with the mandates of the Fourth Amendment.[324] Likewise, the U.S. District Court for the District of Oregon and the U.S. District Court for the Eastern District of New York believed the querying provisions to be acceptable.[325]

A principal concern with querying Section 702 data is that incidentally-obtained information concerning United States persons may be included in the information that is queried. In enacting Section 702, Congress recognized that United States person information could be incidentally collected under Section 702 and mandated minimization procedures to safeguard such privacy interests.[326] For example, Senator Feinstein noted: "There is always the possibility of someone outside the country talking to a U.S. person inside the

---

322 *See Case Redacted*, *supra* note 134, at 30–45.
323 *See id.* at 42.
324 *See id.* at 44–45. PCLOB Board Chairman David Medine and Board Member Patricia Wald "recommended requiring judicial approval for the use of U.S. person queries of Section 702 data for foreign intelligence purposes." PCLOB, Feb. 5, 2016, at 17 n. 4. In contrast, Mr. Kris noted that "recent authority" holds that querying information collected pursuant to Section 702 is "best seen as part of the overall Fourth Amendment event described by the FAA, which includes but is not limited to acquisition, retention, querying, and dissemination of information," rather than as a "separate, stand-alone Fourth Amendment event, such that it must satisfy constitutional requirements on its own." Kris, *supra* note 195, at 398–99 (citing *Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *26 ("[S]ubsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment.")).
325 *See Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *26; *see also Hasbajrami*, *supra* note 139, at *12 n. 20.
326 *See* PCLOB 702 REPORT, *supra* note 11, at 82–83 (explaining that the incidental communications "between a U.S. person and a non-U.S. person located outside the United States, as well as communications of non-U.S. persons outside the United States that may contain information about U.S. persons, was clearly contemplated by Congress at the time of drafting").

country. The bill addresses this with a process known as minimization."[327]

Courts that have considered the constitutionality of incidental collection have determined that such collections comply with the Fourth Amendment. In *In re Directives*, the FISC concluded that "[i]t is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."[328] Likewise, in *United States v. Hasbajrami*, the United States District Court for the Eastern District of New York held that when surveillance is lawfully conducted, including domestic surveillance of United States persons pursuant to a warrant or the surveillance of non-United States persons outside of the United States under Section 702, it follows that the incidental collection of non-targeted United States persons' communications with the targeted persons is also lawfully acquired.[329]

Recently, in *United States v. Mohamud*, the Ninth Circuit considered whether the acquisition of incidentally-collected United States person information under Section 702 is constitutional. In this case, Mohamed Mohamud was convicted of attempting to detonate a large bomb during an annual Christmas tree lighting ceremony in a crowded area in downtown Portland, Oregon. Following a conviction, Mohamud appealed, arguing in part that the incidental collection of his email communications with a foreign

---

[327] *See* 154 CONG. REC. S6119 (daily ed. June 25, 2008) (statement of Sen. Feinstein).
[328] *In re Directives*, *supra* note 82, at 1015; *see Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *15 ("The § 702 acquisition targeting a non-U.S. person overseas is constitutionally permissible, so, under the general rule, the incidental collection of defendant's [a U.S. citizen's] communications with the extraterritorial target would be lawful."); *see Mohamud*, No. 14-30217, *supra* note 155 at *17 ("The mere fact that more communications are being collected incidentally does not make it unconstitutional to apply the same approach to § 702 collection, though it does increase the importance of minimization procedures once the communications are collected."); *see also Hasbajrami*, *supra* note 139, at *7, 8 ("The search of communications between a U.S. person and individuals who are legitimate targets of Section 702 surveillance is constitutional." "The collection of U.S. persons' communications—incidentally obtained through lawful targeting—does not require a separate warrant.").
[329] *See Hasbajrami*, *supra* note 139, at *9 (citing *Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *15).

national under Section 702 violated the Fourth Amendment.[330] The Ninth Circuit disagreed with Mohamud's position. While the Ninth Circuit expressed concern about the large number of incidental communications collected through the use of Section 702,[331] the court concluded that the acquisition of incidental collection was constitutional.[332] The Ninth Circuit determined that when the underlying surveillance conducted is lawful, including surveillance conducted under Section 702, then the incidentally-collected communication of a non-targeted United States person is lawful as well.[333]

Incidental communications of individuals in the United States has proven

---

[330] *See Mohamud*, No. 14-30217, *supra* note 155 at *15. The Ninth Circuit noted that through the monitoring of a foreign national's email account, the government learned that Mohamud was in contact with a foreign national outside of the United States. The communications collected from this contact, which included a limited number of emails between Mohamud and the foreign national, were used to obtain a FISA warrant to conduct surveillance of Mohamud. However, the collected emails between Mohamud and the foreign national were not introduced at trial.

[331] *See id.* at *17 (quoting PCLOB 702 REPORT, *supra* note 11, at 114 (noting that the "term 'incidental' is appropriate because such collection is not accidental or inadvertent, but rather is an anticipated collateral result of monitoring an overseas target. But the term should not be understood to suggest that such collection is infrequent or that it is an inconsequential part of the Section 702 program")). Mohamud asserted that large volume of incidental collection distinguishes it from prior cases. The Ninth Circuit recognized that the "most troubling aspect" of incidental collection under Section 702 is its "vast" volume, but nevertheless concluded that "the mere fact that more communications are being collected incidentally does not make it unconstitutional to apply the same approach to § 702 collection, though it does increase the importance of minimization procedures once the communications are collected."

[332] *See id.* Both the United States District Court for the District of Oregon and the Ninth Circuit held that, under the third-party doctrine, Mohamud had a "reduced expectation of privacy in his communications to third parties." *Id.* at 45. The Ninth Circuit noted that when communications are sent to a third party, an individual's privacy interest in those communications are somewhat diminished. *See id.* at 46 (citing United States v. Miller, 425 U.S. 435, 443 (1976); United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); *Hasbajrami*, *supra* note 139, at *11 & n.18). Referring to these same cases, the Ninth Circuit believed that an individual's privacy interests are diminished even more if the third party had provided the communications to the government voluntarily.

[333] *See id.* at 40-42 (citing *In re Directives*, *supra* note 82, at 1015 (holding that "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful"); United States v. Donovan, 429 U.S. 413, 436 n. 24 (1977) (holding that a Title III wiretap warrant is not made unconstitutional by "failure to identify every individual who could be expected to be overheard," but "the complete absence of prior judicial authorization would make an intercept unlawful"); United States v. Bin Laden, 126 F. Supp. 2d 264, 280 (S.D.N.Y 2000) (explaining that "in the Title III context, incidental interception of a person's conversations during an otherwise lawful surveillance" does not violate the Fourth Amendment); *Hasbajrami*, *supra* note 139, at *9)).

to be essential to the disruption of terrorist plots in our country. For example, incidental Section 702 information was crucial to the detection and disruption of a plan to attack the New York City subway system in 2009.[334] In connection to the subway plot, the FBI arrested Najibullah Zazi, a United States citizen in the United States, for his role in an al-Qaeda plot to carry out suicide attacks on the New York City subway system.[335] Zazi was arrested before he and his accomplices could carry out this potentially catastrophic attack.[336] As noted by the PCLOB, "[w]ithout the initial tip-off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702 [*i.e.*, incidental collection], the subway-bombing plot might have succeeded."[337]

Incidental collection obtained through the use of Section 702 was also used to uncover an al-Qaeda cell in Kansas City, Missouri that was in the preliminary stages of planning an attack on the New York Stock Exchange in 2008.[338] The United States Intelligence Community learned about the plot because the NSA was conducting surveillance under Section 702 targeting an email address used by an extremist in Yemen.[339] Through the 702 surveillance, the NSA discovered a connection between the extremist based in Yemen and an unknown individual in Kansas City, Missouri.[340] The NSA gave the information to the FBI which then identified the unknown person as Khalid Ouazzani, a naturalized United States citizen.[341] The NSA

---

334 *See* THE NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHT AND PARTNERSHIPS (August 2013), https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf; *see also* A. G. Sulzberger and William K. Rashbaum, *Guilty Plea Made in Plot to Bomb New York Subway*, NY TIMES (Feb. 22, 2010) (stating that in February 2010, Zazi pleaded guilty to "one of the most serious threats to the United States" since the attacks of September 11, 2001).

335 *See* THE FBI: PROTECTING THE HOMELAND IN THE 21ST CENTURY, *supra* note 7, at 39.

336 *See id.*

337 PCLOB 702 REPORT, *supra* note 11, at 109.

338 *See* Katersky, Meek, Margolin, and Ross, *supra* note 11 (quoting FBI Assistant Director Sean Joyce's testimony before the House Permanent Select Committee on Intelligence).

339 *See* PCLOB 702 REPORT, *supra* note 11, at 108.

340 *See id.*

341 *See id.*

subsequently discovered that Ouazzani was connected to Al Qaeda associates based in the United States who had previously been part of an abandoned plan to bomb the New York Stock Exchange. These individuals later pled guilty to providing and attempting to provide material support to Al Qaeda.[342]

With respect to querying databases containing Section 702 data for information unrelated to national security matters, including incidentally-collected information, the FISC and two federal district courts considered this issue and concluded that privacy interests were protected.[343] FISA-mandated and FISC-approved minimization procedures provide safeguards to protect United States person information collected under the Section 702, including incidental collection. Further, as noted by Robert Litt, procedural checks are placed upon the government's use of Section 702 data in criminal proceedings.[344] Mr. Litt explained that, similar to all information collected under FISA, Section 702-acquired information may only be used in a criminal proceeding with the approval of the Attorney General, Deputy Attorney General, or Assistant Attorney General for National Security.[345] Moreover, procedures have been developed to ensure that information obtained under Section 702 will only be used in a criminal proceeding for: (1) matters related to national security including terrorism, proliferation, espionage, or cybersecurity;[346] or (2) serious criminal matters involving "(i) death; (ii)

---

[342] *See id.*; *see also* Gia Vang, *Kansas City man suspected in New York terror plot*, FOX4KC.COM (June 18, 2013, updated at 09:18 PM), http://fox4kc.com/2013/06/18/kansas-city-man-suspected-in-new-york-terror-plot/.

[343] *See Case Redacted*, *supra* note 134, at 24–45; PCLOB 702 REPORT, *supra* note 11, at 59–60 (recognizing that "FBI queries designed to elicit evidence of crimes unrelated to foreign intelligence rarely, if ever, produce responsive results from Section 702-acquired data").

[344] *See FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 6; 50 U.S.C. § 1806(b).

[345] *Id.*

[346] Kris, *supra* note 195, at 398 n. 75 (quoting Robert S. Litt, Gen. Counsel, ODNI, Prepared Remarks on Signals Intelligence Reform at the Brookings Institute (Feb. 4, 2015)); *see FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 6 ("The Administration announced an additional restriction that prohibited the use in a criminal proceeding of any communication to or from, or information about, a U.S. person acquired under Section 702 except for crimes involving national security or several other serious crimes.").

kidnapping; (iii) substantial bodily harm; (iv) conduct that constitutes a criminal offense that is a specified offense against a minor as defined in 42 USC 16911; (v) incapacitation or destruction of critical infrastructure as defined in 42 USC 5195c(e); (vi) cybersecurity; (vii) transnational crimes; or (vii) human trafficking."[347]

In addition to the limitations of when Section 702 information may be used in criminal proceedings, under FISA, the government must provide notice to an aggrieved person when the government intends to use Section 702 information in any proceeding, hearing, or trial.[348] The aggrieved person may then choose to seek to suppress the evidence on the grounds that (1) the information was unlawfully acquired; or (2) the surveillance was beyond the scope of what had been authorized by the court.[349]

For the reasons discussed above, I recommend against placing further constraints upon the government's ability to query its own databases that may include Section 702 information. Such querying capabilities permit the executive branch "to quickly and effectively locate foreign intelligence information, such as information potentially related to a terrorist plot against the United States, without having to sift through each individual communication that has been collected."[350] Statutory and procedural safeguards protect United States privacy interests with respect to querying information collected under Section 702. Further, the executive branch has a record of complying with these safeguards.[351] Recent court decisions consistently have found that the querying provisions present no constitutional

---

[347] Kris, *supra* note 195, at 398 n. 75 (quoting Litt, Prepared Remarks on Signals Intelligence Reform at the Brookings Institute, *supra* note 346).
[348] *See* 50 U.S.C. § 1881(e); 50 U.S.C. § 1806(c); 50 U.S.C. § 1801(k) (stating that an "aggrieved person" is "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance").
[349] 50 U.S.C. § 1881(e); 50 U.S.C. § 1806(e).
[350] *FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 6.
[351] *See Release of a Summary of DOJ and ODNI Oversight of Section 702*, *supra* note 17 (March 2014 at 8–11; Oct. 2014 at 8–10; June 2015 at 8–11; Sept. 2015 at 8-12; Feb. 2016 at 8–13; Nov. 2016 at 8-12) (noting that as part of its reviews, DOJ and ODNI review the querying of unminimized Section 702-acquired communications using United States person identifiers).

infirmities: the FISC concluded that querying procedures comply with the requirements of the Fourth Amendment;[352] the U.S. District Court for the District of Oregon recognized that querying of collected information is not a separate search and does not make surveillance conducted under Section 702 unreasonable under the Fourth Amendment;[353] and the U.S. District Court for the Eastern District of New York held that it would be inconsistent to permit the government to review information in its possession, but prohibit queries of the same information.[354] As recognized by the FISC, following the September 11, 2001 attacks, the government was heavily criticized for its failure to identify information that may have disrupted them.[355] Statutory and procedural safeguards, including minimization procedures, exist with respect to the querying databases that contain lawfully collected Section 702. These safeguards ensure that United States person privacy interests are protected. Placing further constraints upon the government's ability to query its own databases would inhibit the government's effectiveness in identifying information critical to our national security interests.

V. APPLICATION OF THESE PRINCIPLES TO A HYPOTHETICAL

To demonstrate how the matters discussed in this article balance our fundamental privacy interests with national security interests, the below hypothetical is used. The imagined facts of the hypothetical are as follows.

> Anne, a nineteen-year old United States citizen from Denver, Colorado, is a recent high school graduate. Upon graduating from high school, Anne had trouble finding a job, but eventually secured a

---

352 *Case Redacted*, *supra* note 134, at 44–45; see Kris, *Trends And Predictions In Foreign Intelligence Surveillance: The FAA And Beyond*, *supra* note 195, at 399 (citing *Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *26 ("[S]ubsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment.").

353 *See Mohamud*, No. 3:10-CR-00475-KI-1, *supra* note 155, at *26.

354 *Hasbajrami*, *supra* note 139, at *12 n. 20.

355 *See Case Redacted*, *supra* note 134, at 42.

minimum-wage position at ShoeWorld. She could not afford her own apartment, so she lived at home with her parents and three younger brothers.

At ShoeWorld, Anne became friendly with two of her coworkers, Belinda, also aged nineteen, and Carl, twenty-four years old, both United States citizens. At work, the coworkers discussed the conflicts in Syria and Iraq and became increasingly angry and frustrated about the casualties in those conflicts overseas.[356] Other than her two coworkers, Anne does not have many friends. When she was home, she spent much of her time alone in her room perusing the Internet. Several months ago, through the Internet, she came into contact with a young man, Dave, who immigrated to Syria from England and joined ISIS. Dave described how he and other ISIS members were working together to build a utopian "Caliphate state."[357] Dave also told Anne that there was a group of young women, just like her, who were part of a "sisterhood" of women to help achieve their utopian goal. After several months, Anne decided to travel to Syria to join Dave and the other members of ISIS. Without her parents' knowledge, Anne traveled to Aleppo, Syria. There, she was met by Dave.

After several weeks, Anne was tasked with trying to recruit other Western nationals to join ISIS. Soon thereafter, the executive branch learned of her activities. Under the modified Section 702 proposed in this article and Executive Order 12333, as soon as the executive branch learned of Anne's conduct, it was able to initiate electronic surveillance of her communications. Through this surveillance, the executive branch learned that Anne had convinced Belinda to join ISIS. In their conversations, the two teenagers discussed Belinda's travel arrangements. Belinda also told Anne that she had stolen a suitcase from Target to prepare for her trip.

With the knowledge of Belinda's travel plans, learned through the Section 702 collection, the FBI arrested Belinda at Denver International Airport where she had intended to fly to Turkey, and then join Anne in Syria. Upon her arrest, Belinda told the FBI that

---

[356] While the facts in this scenario are fictional, they are based, in part, upon Erin Marie Saltman & Melanie Smith, *'Till Martyrdom Do Us Part': Gender and the ISIS Phenomenon*, INSTITUTE FOR STRATEGIC DIALOGUE 4, 12 (2015), http://www.strategicdialogue.org/Till_Martyrdom_Do_Us_Part_Gender_and_the_ISIS_Phenomenon.pdf; Guillame N. Beaurpere, *ISIS and Protracted War: Why Violent Extremists Persist in the Face of Defeat*, 6 COUNTER TERRORIST TRENDS AND ANALYSIS 4, 4-5 (2014), http://www.rsis.edu.sg/wp-content/uploads/2014/09/CTTA-September14.pdf.

[357] *See, e.g.*, Saltman and Smith, *supra* note 356, at 13–14.

> she believed in the ISIS cause and intended to take up arms and join in their fight.[358] She professed her belief in the legitimacy of violent jihad and declared her hopes to someday join the battlefield on behalf of a jihadist group. Belinda was charged with conspiring to provide material support to ISIS.[359]
>
> Anne also communicated with Carl. Through Anne and Carl's communications, the government learned that Carl, with Anne's encouragement, decided to help the ISIS cause by setting off explosives in a crowded area in Denver. The government queried its databases, using Carl's telephone number as an identifier, and learned that Carl had a previous conviction for unlawful possession of firearms. Pursuant to a warrant, the FBI searched Carl's home and found explosive materials and illegal firearms. Carl was arrested and his plot was thwarted. Carl was charged with conspiring to provide material support to ISIS and conspiring to use weapons of mass destruction.[360]
>
> Before their respective trials, as required by FISA, the government informed Belinda and Carl that it intended to use foreign intelligence information collected under Section 702. Based upon information collected under Section 702, both Belinda and Carl were convicted of the crimes for which they were charged. Belinda was sentenced to five years and Carl was sentenced to 43 years in prison.

As illustrated by this fictional scenario, through the use of Section 702 as proposed in this article, almost immediately upon learning of Anne's activities, the government obtained the authority to conduct electronic surveillance of Anne's telephone number. To receive such authority, the executive branch was required to satisfy both (the proposed) Section 702 and Executive Order 12333. For example, pursuant to Executive Order 12333,

---

358 *See* Jenny Deam, *Colorado Woman Who Tried to Join Islamic State Sentenced to 4 Years*, LA TIMES (Jan. 23, 2015), http://www.latimes.com/nation/la-na-shannon-conley-sentencing-20150123-story.html (describing that an ISIS "recruiter . . . encouraged Douglas McAuthur McCain, 33, to leave Minnesota and go to Syria to take up arms with Islamic State").

359 *See, e.g.*, *id.* (detailing that Shannon Maureen Conley, a 19-year old Colorado woman who tried to join the Islamic State terrorist group and was sentenced to 48 months in prison. Conley "pleaded guilty in September to one count of conspiracy to provide material support to a foreign terrorist organization").

360 *See, e.g.*, *Charges Unsealed Against Five Alleged Members of Al-Qaeda Plot to Attack the United States and United Kingdom*, DEPARTMENT OF JUSTICE, OFFICE OF PUBLIC AFFAIRS (July 7, 2010), https://www.justice.gov/opa/pr/charges-unsealed-against-five-alleged-members-al-qaeda-plot-attack-united-states-and-united.

the Attorney General was required to determine that there was probable cause to believe that Anne was acting as a foreign power or an agent of a foreign power before conducting surveillance.[361] Under the proposed framework, the FISC would review the AG's probable cause findings with respect to Anne. Further, at all stages, including the collection, retention, querying, use, and dissemination of Anne's communications, minimization procedures would play an integral role in protecting her privacy interests.[362]

Belinda and Carl's communications are incidentally collected information. Unlike Anne, they were not the targets of the Section 702 surveillance. However, because they were communicating with Anne, their communications were collected as part of the surveillance. Like Anne, as U.S persons, Belinda and Carl's communications are protected under minimization procedures, including the collection, retention, querying, use, and dissemination of their communications. As illustrated by this hypothetical scenario, collecting and querying incidentally collected information is critical to our national security interests. If someone in the United States is communicating with a terrorist overseas, it is essential that the government is able to obtain this information to expose possible terrorist threats within our country. Through these incidentally collected communications, the government learned that Belinda planned to join ISIS in Syria, and that Carl, a homegrown terrorist, planned to set off explosives in Denver.

With respect to the criminal prosecution of Belinda and Carl, the information collected about them could only be used with the approval of the Attorney General, Deputy Attorney General, or Assistant Attorney General for National Security.[363] Further, such information could only be used if it

---

[361] *See* Executive Order 12333, *supra* note 106, § 2.5.
[362] *See* NSA MINIMIZATION PROCEDURES, *supra* note 17, at 7; *see also* FBI MINIMIZATION PROCEDURES, *supra* note 17, at 11–12; *see also* CIA MINIMIZATION PROCEDURES, *supra* note 17, at 3–4.
[363] *See FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 6.

related to national security or involved a serious crime.[364] As such, while the information collected likely could be used as evidence of conspiring to provide material support to ISIS and conspiring to use weapons of mass destruction, the government likely would be prohibited from using the information as evidence of Belinda's theft of a suitcase. As a further safeguard, the government would be required to provide Belinda and Carl with notice that they intended to enter their communications collected under Section 702 at trial.[365] Belinda and Carl would have the option of seeking to suppress the evidence upon the grounds that (1) the information was not obtained lawfully; or (2) the surveillance was beyond the scope of what the court authorized or approved.[366]

Anne, Belinda, and Carl are protected under the Fourth Amendment. The government's surveillance of their communications must be reasonable.[367] Strong national security interests are at stake, *e.g.*, what United States persons are joining the terrorist group ISIS, efforts they were taking to undermine the security of the United States, intent to use explosives in a crowded area, and ability to quickly obtain information related to these matters. Equally significant, robust oversight requirements and procedural safeguards ensure the protection of United States person privacy interests. Their privacy interests are protected at all stages of the process, from collecting foreign intelligence information, querying the information, and then using the information to pursue criminal convictions.[368] Under the

---

364 *See* Kris, *Trends And Predictions In Foreign Intelligence Surveillance: The FAA And Beyond*, *supra* note 195, at 398 n. 75 (quoting Litt, Prepared Remarks on Signals Intelligence Reform at the Brookings Institute, *supra* note 345); *see also FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note 3, at 6. In 2015, "the Administration announced an additional restriction that prohibited the use in a criminal proceeding of any communication to or from, or information about, a U.S. person acquired under Section 702 except for crimes involving national security or several other serious crimes."

365 *See* 50 U.S.C. § 1881(e); 50 U.S.C. § 1806(c).

366 *See* 50 U.S.C. § 1881(e); 50 U.S.C. § 1806(e).

367 *See In re Directives*, *supra* note 82, at 1012.

368 *See* 50 U.S.C. § 1801(h); *see also* 50 U.S.C. § 1881(a)(c)(1), a(d)(1), (e); *see also* 50 U.S.C. § 1806(c), (e); *see also FISA Amendments Act: Hearing Before the H. Comm. on the Judiciary*, *supra* note

hypothetical, applying the totality of the circumstances test, the executive branch's collection of Anne's electronic communications, and the incidental collection of her friends' communications, are reasonable under the Fourth Amendment.[369]

VI. CONCLUSION

The proposed recommendations set forth in this article would strengthen Section 702 by authorizing the executive branch to acquire foreign intelligence information of both United States and non-United States persons outside of the United States without individualized judicial review, with added safeguards for United States persons. Restoring these essential surveillance authorities to the executive branch would serve to counter the evolving threat of Americans leaving our country to join terrorist organizations abroad. Importantly, comprehensive safeguards and oversight provisions are built into the proposed modifications that would protect United States person privacy interests.

The misuse of intelligence authorities of the 1960s and 1970s as documented by the Church and Pike Committees has been addressed. The executive branch has an established history of compliance with the statutory

---

3, at 6; Kris, J. NAT'L SECURITY L. & POL'Y, *supra* note 195, at 21 n. 75 (quoting Litt, Prepared Remarks on Signals Intelligence Reform at the Brookings Institute, *supra* note 346)).

[369] *See In re Directives*, *supra* note 82, at 1012 (citing *Samson*, *supra* note 89, at 848; *Garner*, *supra* note 89, at 8–9); *see also Mohamud*, No. 14-30217, *supra* note 155 at *18–20. *United States v. Mohamud* is analogous to the hypothetical presented here. As discussed above, Mohamud, a United States person in the United States, was convicted of attempting to detonate a large bomb during an annual Christmas tree lighting ceremony in a crowded area in downtown Portland, Oregon. Through the monitoring of a foreign national's email account under Section 702, the government learned that Mohamud was in contact with a foreign national outside of the United States. The government used this incidentally-collected information to obtain a FISA warrant to conduct surveillance of Mohamud. Mohamud challenged the constitutionality of the collection. The Ninth Circuit applied a totality of the circumstance test to determine whether the protections set forth in Section 702 were reasonable under the Fourth Amendment. While the Ninth Circuit did not give much weight to the oversight procedures, the court concluded that the targeting and minimization procedures adequately protected Mohamud's privacy interest. After evaluating the safeguards mandated in Section 702, and in light of the government's national security interests, the Ninth Circuit concluded that as applied to Mohamud, Section 702 was reasonable under the Fourth Amendment.

requirements of Section 702.[370] Reports by the PCLOB, Attorney General, and Director of National Intelligence consistently show that the executive branch is fulfilling its statutory and procedural obligations. Moreover, in reauthorizing the FAA, including Section 702, the Senate Select Committee on Intelligence found that the statutory provisions have been implemented in a manner that protects the privacy and civil liberties of United States persons and is subject to extensive oversight by all three branches of our government.[371]

The proposed changes to the FAA, particularly Section 702, are well-grounded in constitutional law, provide essential safeguards to privacy concerns, and strengthen the executive branch's surveillance authorities to counter those engaged in terrorist activities. Historically, it had been within the discretion of the executive branch to acquire foreign intelligence information of persons outside of the United States without seeking judicial review. The FAA limits this executive branch authority, beyond what was constitutionally required. The FAA is scheduled to sunset in December 2017. It is recommended that Congress adopt the proposed changes to the FAA, including Section 702, outlined in this article, and restore these authorities to the executive branch.

Moreover, it is recommended that no further limitations be placed upon the government's ability to query the information already in its possession. Multiple layers of protections currently exist for the querying of Section 702 data and the executive branch has a record of complying with these procedural safeguards.[372] As stated in *United States v. Hasbajrami*, "in this era there are individuals and groups dedicated to inflicting grave harm on our nation," and the government's intelligence tools "are a critical component of

---

[370] *See Release of a Summary of DOJ and ODNI Oversight of Section 702, supra* note 17.
[371] S. Rept. 112-174, FAA SUNSETS EXTENSION ACT OF 2012, at 1, 3–4 (June 7, 2012), https://www.congress.gov/congressional-report/112th-congress/senate-report/174/1.
[372] *See Release of a Summary of DOJ and ODNI Oversight of Section 702*, *supra* note 17 .

our government's efforts to protect us from harm."[373] Our government "has a duty to respect and protect our constitutional rights while simultaneously ensuring the nation's security."[374] The proposed recommendations set forth in this article would strengthen our surveillance authorities while protecting individuals rights to help achieve this goal.

[373] *Hasbajrami*, *supra* note 139, at *1.
[374] *Id.*