Notre Dame Law Review Reflection

Volume 95 | Issue 3 Article 2

3-2020

FISA Section 702: Does Querying Incidentally Collected Information Constitute a Search Under the Fourth Amendment?

Rachel G. Miller
Notre Dame Law School

FISA SECTION 702: DOES QUERYING INCIDENTALLY COLLECTED INFORMATION CONSTITUTE A SEARCH UNDER THE FOURTH AMENDMENT?

Rachel G. Miller[*]

INTRODUCTION

An inherent source of conflict in the United States exists between protecting national security and safeguarding individual civil liberties. Throughout history, Americans have consistently been skeptical and fearful of the government abusing its power by spying on Americans. In an effort to curtail government abuses through surveillance, President Carter and Congress enacted the Foreign Intelligence Surveillance Act of 1978 (FISA).[1] The purpose of FISA was to establish a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."[2] FISA provides the government with the authority to engage in electronic surveillance, targeted at foreign powers or agents of foreign powers, for the purpose of gathering foreign intelligence information.[3] FISA initially permitted certain surveillance activities, almost all of which occurred within the United States, but excluded the vast majority of overseas foreign intelligence surveillance activities.[4]

Following 9/11, the government's interest in surveilling terrorists was at an all-time high. However, no authority existed under the current statutory scheme of FISA to surveil suspected terrorists and their communications with Americans without prior approval from the FISA Court.[5] In 2005, President Bush, relying on his Commander-in-Chief power and authorization under the Authorization for Use of Military Force Act, enacted the Terrorist Surveillance Program allowing the

* Candidate for Juris Doctor, Notre Dame Law School, 2020; Bachelor of Arts in Economics and Government, The University of Texas at Austin, 2016. I would like to thank Professor Jimmy Gurulé for his mentorship and advice throughout the writing process. I would also like to thank my family for their constant support, and my friends at *Notre Dame Law Review Reflection* for their sincere edits. All errors are my own.

1 Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–85 (2012).

2 H.R. Rep. No. 95-1283, pt. 1, at 22 (1978).

3 *See id.*

4 H.R. Rep. No. 114-109, pt. 1, at 3 (2015).

5 Elizabeth Goitein et al., *Lessons from the History of National Security Surveillance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 550 (David Gray & Stephen E. Henderson eds., 2017) ("FISA . . . required the government to obtain an order from the FISA Court [each time] it wished to obtain wire communications involving Americans.").

National Security Agency (NSA) to conduct surveillance and collect information without warrants.[6] Under this program, one of the individuals being surveilled had to be a suspected terrorist, and one was required to be located outside the United States.[7] However, the lack of warrants raised many concerns regarding individual privacy rights and civil liberties.[8] In response, Congress enacted section 702 in July 2008 as part of the FISA Amendments Act (FAA).[9] Section 702 broadened the scope of FISA allowing the government to conduct foreign intelligence surveillance outside the United States without an individualized application for each target.[10] The FAA garnered bipartisan support, notably from then-Senator Obama in 2008 and more recently former FBI director Christopher Wray, who stated section 702 is "one of the most valuable tools that we have in our toolbox to keep America safe."[11] Additionally, section 702 has proven commendable as a vast number of terrorist plots have been foiled through use of information obtained under section 702.[12] For example, information obtained under section 702 led to the arrest of Najibullah Zazi, a U.S. 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.[13]

However, during the process of collecting information from foreign targets, it is evident that collection of U.S. persons' information—not permitted to be intentionally obtained—may still be collected if a U.S. person is in contact with the intended foreign target. Concerns regarding incidental collection of U.S. persons' communications under section 702 surveillance began to grow.[14] Critics argued that collection of U.S. persons' communications violated the Fourth Amendment

---

6 *See* Gary L. Gregg II, *George W. Bush: Foreign Affairs*, MILLER CTR., https://millercenter.org/president/gwbush/foreign-affairs (last visited Nov. 13, 2018).

7 *Id.*

8 *See* Goitein, *supra* note 5, at 550–51.

9 FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008) (codified as amended at 50 U.S.C. § 1881a (2012)).

10 *See* Jessica Zuckerman, *Foreign Intelligence Surveillance Amendments Act of 2008*, HERITAGE FOUND. (Nov. 13, 2012), https://www.heritage.org/defense/report/foreign-intelligence-surveillance-amendments-act-2008#_ftn1.

11 Jack Goldsmith & Susan Hennessey, *The Merits of Supporting 702 Reauthorization (Despite Worries About Trump and the Rule of Law)*, LAWFARE (Jan. 18, 2018), https://www.lawfareblog.com/merits-supporting-702-reauthorization-despite-worries-about-trump-and-rule-law.

12 *See "Section 702" Saves Lives, Protects the Nation and Allies*, NAT'L SECURITY AGENCY & CENT. SECURITY SERV. (Dec. 12, 2017), https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1627009/section-702-saves-lives-protects-the-nation-and-allies/ (discussing various ways Section 702 collection has helped thwart terrorist activity).

13 *See* BRUCE HOFFMAN ET AL., 9/11 REVIEW COMM'N, FED. BUREAU OF INVESTIGATION, THE FBI: PROTECTING THE HOMELAND IN THE 21ST CENTURY 39 (2015); *see also* Gia Vang, *Kansas City Man Suspected in New York Terror Plot*, FOX4 (June 18, 2013), https://fox4kc.com/2013/06/18/kansas-city-man-suspected-in-new-york-terror-plot/ (discussing how the NSA used information collected under section 702 to uncover an al-Qaeda cell in Kansas City that was in the initial stages of planning an attack on the New York Stock Exchange).

14 *See* Zuckerman, *supra* note 10.

because it was a warrantless search.[15] Nevertheless, courts have upheld the constitutionality of incidental collection and asserted that the collection is not a violation of the Fourth Amendment.[16] While the concerns regarding incidental collection have subsided,[17] a new Fourth Amendment challenge has presented itself. Information that has lawfully been obtained through section 702 surveillance, including information that has been incidentally collected, can later be "queried" or searched by intelligence agencies.[18] When the government conducts queries, they are able to access the contents of 702-acquired information and may be able to use the subsequently obtained information as evidence in unrelated criminal proceedings. Importantly, however, section 702 includes many comprehensive safeguards protecting the privacy interests of U.S. persons. Likewise, the Privacy and Civil Liberties Oversight Board ("PCLOB")[19]—a bipartisan oversight agency within the executive branch—found that section 702 is subject to extensive oversight and further concluded there was "no evidence of intentional abuse."[20]

This Note poses the question of whether subsequent queries conducted on incidentally collected section 702 communications constitute searches under the Fourth Amendment and therefore require a warrant. Part I discusses traditional FISA and provides background on protections that have been implemented to assure individual liberties. Part II discusses the FISA amendments and the specifics of section 702, including the newly implemented querying procedures. Part III addresses Fourth Amendment concerns regarding incidental collection and subsequent querying of U.S. persons' information. Part III additionally analogizes the constitutionality of queries conducted on section 702 information to similar searches done within DNA databases that are subsequently able to be used in unrelated criminal prosecutions. This Note concludes by suggesting that subsequent

15 *See* David G. Barnum, *Warrantless Electronic Surveillance in National Security Cases: Lessons from America*, 5 EUROPEAN HUM. RTS. L. REV. 514, 514–17, 535–38 (2006).

16 *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d. 1004, 1016 (FISA Ct. Rev. Aug. 22, 2008) [hereinafter *In re* Directives]; *see* United States v. Mohamud, 843 F.3d 420, 439 (9th Cir. 2016).

17 *See generally* Goldsmith & Hennessey, *supra* note 11.

18 *See* 50 U.S.C.A. § 1881a(f) (West, Westlaw through Pub L. No. 116-66).

19 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 & C.L. OVERSIGHT BD., https://www.pclob.gov (last visited Nov. 12, 2018). The PCLOB was established by the Implementing Recommendations of the 9/11 Commission Act, Pub. L. 110-53, signed into law in August 2007. *Id.*

20 *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 2, 5 (2014) [hereinafter PCLOB 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").

queries, including on incidentally collected information, are consistent with the Fourth Amendment. Further, because queries are constitutional under the Fourth Amendment, and several procedural restrictions are in place, the FBI may use queried section 702 information to bring criminal charges, unrelated to national security, against U.S. persons.

I. TRADITIONAL FISA

Enacted in 1978, FISA was aimed at curtailing abuses and delineating procedures to be employed by the government in conducting foreign intelligence surveillance.[21] FISA seeks to "provide effective, reasonable safeguards to ensure accountability and prevent improper surveillance."[22] Title I of FISA authorizes electronic surveillance within the United States for foreign intelligence purposes.[23] Electronic surveillance is limited to targeting foreign powers or agents of foreign powers located within the United States for the purpose of collecting foreign intelligence information.[24] In order to authorize such electronic surveillance, Congress created two specialized courts, the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISCR).[25] The statute empowers the FISC to grant or deny applications for surveillance orders in foreign intelligence investigations.[26] The FISC can authorize surveillance for foreign intelligence purposes if there is probable cause to believe that: (1) the target is a "foreign power" or an "agent of a foreign power," and (2) each of the specific "facilities or places at which the electronic surveillance is directed is being used . . . by a foreign power or an agent of a foreign power."[27] Further, a "significant purpose" of the order must be to obtain "foreign intelligence information."[28]

A. Foreign Intelligence Information

Foreign intelligence information is broadly defined to include two categories of information. Section 1801(e)(1) authorizes the collection of "counterintelligence" or "protective" foreign intelligence information.[29] Counterintelligence and protective information relate to the ability of the United States to protect against an actual or potential attack, international terrorism, or clandestine intelligence activities by a foreign power or agent of a foreign power.[30] Additionally, § 1801(e)(2) authorizes collection of "positive" foreign intelligence

21 ACLU v. Clapper, 785 F.3d 787, 793 (2d Cir. 2015).
22 S. Rep. No. 95-604, at 7 (1977).
23 50 U.S.C. §§ 1801–12 (2012).
24 *Id.* § 1802(a)(1).
25 *Id.* § 1803(a).
26 *Id.*
27 *Id.* § 1805(a)(2)(B).
28 *Id.* § 1804(a)(6)(B).
29 *See id.* § 1801(e)(1).
30 *See id.* § 1801(e)(1)(A)–(C).

information.[31] Positive information refers to information relating to "national defense or security of the United States" or "the conduct of the foreign affairs of the United States."[32] Therefore, the collection of foreign intelligence information is not limited to preventing terrorist attacks, and, further, there is no requirement that the information being sought is evidence of a crime or intended for use in a criminal prosecution.[33]

B. Use of FISA Evidence

So long as a significant purpose of the FISA surveillance was to gather foreign intelligence information, evidence of criminal activity thereby obtained may be introduced in subsequent criminal proceedings.[34] The use of FISA information must also be conducted in accordance with minimization procedures.[35] In the event the government intends to use any evidence derived from a FISA order in a criminal prosecution, prior notice must be provided to the "aggrieved person" against whom the information is to be used.[36] Upon receipt of such notice, the aggrieved person may seek to suppress the use of FISA-derived evidence on the grounds that the evidence was unlawfully acquired or the government did not act in conformity with the relevant FISA order.[37] Additionally, the aggrieved person may move to compel disclosure of FISA materials, including FISA applications, affidavits, court orders, and other documents related to the FISA surveillance.[38] However, if the defendant moves to compel disclosure of FISA evidence, the Attorney General may oppose such request by filing an affidavit stating that the disclosure "would harm the national security of the United States."[39] If the Attorney General opposes disclosure, the district court then must conduct a review of the FISA warrant and application materials to determine whether the surveillance was "lawfully authorized and conducted."[40] The district court has discretion to disclose portions of the documents, however, to date no court has found it necessary to disclose FISA materials in order to make a determination of the lawfulness of a FISA warrant.[41]

---

31 *See id.* § 1801(e)(2).

32 *Id.*

33 GEOFFREY S. CORN ET AL., NATIONAL SECURITY LAW AND THE CONSTITUTION 617–18 (2017).

34 JAMES G. CARR & PATRICIA L. BELLIA, 2 LAW OF ELECTRONIC SURVEILLANCE § 9:50, at 474 (2012).

35 50 U.S.C. § 1802(a)(2) (2012).

36 United States v. Warsame, 547 F. Supp. 2d 982, 986 (D. Minn. 2008). Because the standard for a FISA order is that only a "significant purpose" of the surveillance be to obtain foreign intelligence, if the surveillance reveals other criminal activity unrelated to national security, the government will be able to pursue criminal prosecutions.

37 *Id.*; *see* 50 U.S.C. § 1806(f).

38 50 U.S.C. § 1806(f).

39 *Id.*

40 *Id.*

41 CORN, *supra* note 33, at 665.

II. FISA AMENDMENTS ACT AND SECTION 702

Following the 9/11 attacks, President George W. Bush authorized the NSA to conduct warrantless wiretapping of telephone and email communications between suspected terrorists abroad and Americans.[42] In order to conduct warrantless wiretapping, one party to the communication must have been reasonably believed to be outside of the United States, and a participant in the communications must have been reasonably believed to be a member or agent of al-Qaeda or an affiliated terrorist organization.[43] This activity was in violation of the current FISA, which required the government to obtain individualized orders from the FISC if it wished to obtain surveillance involving communications of Americans.[44] However, based on intense public scrutiny of the Bush program, President Bush asked Congress to amend FISA to provide the government with authority to collect foreign intelligence information from non-U.S. persons located outside of the United States.[45] In 2008, Congress enacted the FISA Amendments Act, which "supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting . . . non-U.S. persons located abroad."[46] The 2008 FAA included a five-year sunset provision. The FAA was reauthorized in 2012, and on Friday, January 19, 2018, the FAA was reauthorized and signed into law for an additional six years.[47] Commentators across the political spectrum have proclaimed the FAA is a "critically important surveillance tool—one that has helped the nation respond to (and avert) planned attacks."[48]

Title VII of FISA includes section 702 which authorizes the executive branch to acquire foreign intelligence information on non-U.S. persons reasonably believed to be located outside of the United States without seeking individualized FISC orders for each acquisition.[49] The FISC thereby is permitted to issue a single order

42 Gregg, *supra* note 6; *see also* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

43 ACLU v. Nat'l Sec. Agency, 493 F.3d 644, 648 (6th Cir. 2007).

44 Goitein, *supra* note 5, at 550.

45 GEOFFREY CORN ET AL., NATIONAL SECURITY LAW: PRINCIPLES AND POLICY 219 (2015). In times of crises, it is exceedingly important to remember that good intentions are not the law.

46 Clapper v. Amnesty Int'l, 568 U.S. 398, 404 (2013); *see also* 50 U.S.C. § 1881a (2012).

47 Press Release, The White House, President Donald J. Trump Signs S. 139 into Law, (Jan. 19, 2018), https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-signs-s-139-law/.

48 Jennifer Daskal & Stephen I. Vladeck, *"Incidental" Foreign Intelligence Surveillance and the Fourth Amendment*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 101–02 (David Gray & Stephen E. Henderson eds., 2017).

49 *See* 50 U.S.C. § 1881a(a). "U.S. persons" is a term of art in the intelligence community that is defined to mean people who are American citizens *and* people who are permanent-resident aliens. DAVID R. SHEDD ET AL., MAINTAINING AMERICA'S ABILITY TO COLLECT FOREIGN INTELLIGENCE: THE SECTION 702 PROGRAM (May 13, 2016). The U.S. persons requirement establishes that neither citizens nor permanent residents of the United States can be targets of Section 702 surveillance. SHEDD ET AL., *supra*. As defined by Title I of FISA, a U.S. person is "a

approving more than one section 702 certification to acquire foreign intelligence information. Prior to collecting information under section 702, the Attorney General and Director of National Intelligence (DNI) must submit a written certification to the FISC, attesting, among other factors, that targeting, minimization, and querying procedures are in place; have been approved by the FISC; are consistent with the Fourth Amendment; and that a significant purpose of the acquisition is to obtain foreign intelligence information.[50]

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."[51] Further, section 702 mandates that all acquisitions comply with the requirements of the Fourth Amendment.[52] Once all procedures are satisfied, the FISC may authorize surveillance through issuance of an annual certification.[53] The following Sections address the expansive procedures that must be in place prior to the government receiving certification from the FISC.[54]

A. Targeting and Minimization Procedures

Prior to conducting surveillance under section 702, targeting procedures must be submitted to the FISC for approval. Targeting procedures are steps the government must take to ensure the target of the surveillance is outside the United States and not a U.S. person at any time surveillance is undertaken.[55] As demonstrated by the NSA's targeting procedures in the 2016 certification package, the NSA, prior to engaging in surveillance, must "determine[] whether a person is a non-United States person reasonably believed to be outside the United States in light of the totality of the circumstances."[56]

---

citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of [the Immigration and Nationality Act])." 50 U.S.C. § 1801(i); *see also* OFFICE OF CIVIL LIBERTIES, PRIVACY & TRANSPARENCY, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT: REGARDING USE OF NATIONAL SECURITY AUTHORITIES 6 (2019) [hereinafter TRANSPARENCY REPORT 2019], https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf.

50 *See* 50 U.S.C. § 1881a(g)(2)(A)(i), (ii), (iv), (v).

51 *Id.* § 1881a(b)(1)–(4).

52 *Id.* § 1881a(b)(5); *see also* TRANSPARENCY REPORT 2019, *supra* note 49, at 12.

53 50 U.S.C. § 1881a(h).

54 Each intelligence agency sets its own targeting, minimization, and querying procedures. However, due to the repetitiveness, discussion concerning the NSA's procedures is included in the targeting and minimization analysis. For the querying procedures, the analysis focuses on the FBI as their procedures substantially vary from the other intelligence agencies.

55 SHEDD ET AL., *supra* note 49.

56 JEFF SESSIONS, U.S. DEP'T OF JUSTICE, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE

In addition to targeting procedures, minimization procedures detail requirements the government must meet to use, retain, and disseminate section 702 information. Minimization procedures regarding section 702 information, must be "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[57] Minimization procedures include specific guidelines and restrictions on how the government handles nonpublicly available U.S.-person information acquired from section 702 collection of non-U.S.-person targets.[58]

B. Querying Procedures

With the reauthorization of FAA in 2017, Congress codified new querying procedures that must be submitted to the FISC, in addition to the targeting and minimization procedures, for review and approval prior to conducting surveillance.[59] Section 702 defines query as "the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized under [702](a)."[60] Included in the procedures adopted, the Attorney General and DNI must keep a record of each U.S. person query term used for a query.[61] Query terms may be date-bound and include telephone numbers and email addresses, or may be as individualized as querying using an individual's name.[62] Each agency has a different standard for conducting and reviewing contents of U.S. person queries. For example, the NSA may only query section 702 information if the query is "reasonably likely to return foreign intelligence information."[63] Additionally, the NSA makes all U.S. persons' communication queries and its articulated foreign intelligence purpose available to the DOJ and the Office of the Director of National Intelligence (ODNI) as part of its bimonthly oversight reviews.[64]

LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 1 (2017) [hereinafter NSA TARGETING PROCEDURES], https://www.dni.gov/files/documents/icotr/51117/2016_NSA_702_Targeting_Procedures_Mar_30_17.pdf.

57 50 U.S.C. §§ 1801(h)(1), 1821(4).

58 TRANSPARENCY REPORT 2019, *supra* note 49, at 11.

59 *Id.* at 12; *see also* 50 U.S.C.A. § 1881a(f)(1)(A) (West, Westlaw through Pub L. No. 116-66).

60 50 U.S.C.A. § 1881a(f)(3)(B) (West, Westlaw through Pub L. No. 116-66).

61 50 U.S.C.A. § 1881a(f)(1)(B).

62 TRANSPARENCY REPORT 2019, *supra* note 49, at 12.

63 *Id.*

64 NSA TRAINING ON FISA AMENDMENTS, OVCS1203: FISA AMENDMENTS ACT SECTION 702 TRAINING 54, [hereinafter NSA SECTION 702 TRAINING], https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20001001-001049%20-

Due to the broad power and authority the FBI has to bring unrelated criminal charges using information obtained under section 702, the PCLOB consistently pressured Congress to add additional limitations on the FBI's section 702 querying procedures.[65] With the reauthorization of FAA in 2017, Congress codified new requirements relating to the access of results of certain queries conducted by the FBI.[66] Specifically, under section 702(f)(2)(A), an order from the FISC is now required prior to the FBI reviewing the contents of a query if the query (1) was not designed to find and extract foreign intelligence information, and (2) was performed in connection with a predicated criminal investigation that does not relate to national security.[67] Each application made to the FISC further shall include the

> identity of the federal officer making the application; and an affidavit containing a statement of the facts and circumstances relied upon by the applicant to justify the belief that the contents in the communications [being described] would provide evidence of—criminal activity; contraband, fruits of a crime, or other items illegally possessed by a third party; or property designed for use, intended for use, or used in committing a crime.[68]

Following the submission of the application, the FISC enters an order approving the access of the contents of communications if the court finds probable cause to believe the contents would yield evidence of criminal activity.[69] Nevertheless, if the FBI determines there is a "reasonable belief that such contents could assist in mitigating or eliminating a threat to life or serious bodily harm," a FISA court order is not required to access the contents of the communications, and the FBI can proceed immediately.[70] Moreover, in general, any information concerning a U.S. person acquired under section 702 is not to be used in evidence against that U.S. person in any criminal proceeding.[71] Notwithstanding, there are two circumstances in which evidence against a U.S. person may be used in criminal proceedings. First, evidence may be used if the FBI obtained an order from FISC allowing access to queried information.[72] Second, evidence may be used if the Attorney General determines either (1) the criminal proceeding affects, involves, or is related to national security; or (2) the criminal proceeding involves death, kidnapping, serious bodily injury, conduct that constitutes a criminal offense that is a specified offense against a minor, incapacitation or destruction of critical infrastructure, cybersecurity, transnational crime, or human trafficking.[73]

%20Doc%2017.%20NSA%E2%80%99s%20Training%20on%20FISA%20Amendments%20Act%20Section%20702.pdf.

65 PCLOB REPORT, *supra* note 20, at 11–12.

66 50 U.S.C.A. § 1881a(f)(2)(A) (West, Westlaw through Pub L. No. 116-66).

67 *Id.*

68 50 U.S.C.A. § 1881a(f)(2)(C).

69 *Id.* § 1881a(f)(2)(D).

70 *Id.* § 1881a(f)(2)(E).

71 *Id.* § 1881e(a)(2)(A).

72 *Id.*

73 *Id.*

III. SECTION 702 AND THE FOURTH AMENDMENT

Once the government has obtained approval from the FISC, the specified agency may proceed with its intended collection of foreign intelligence surveillance of non-U.S. persons reasonably believed to be located outside of the United States. Such collection rarely raises constitutional concerns as the individuals targeted are generally not protected under the Constitution.[74] However, constitutional concerns specifically relating to the Fourth Amendment arise when U.S. persons' information is collected during this process and is subsequently retained.[75] Section A of this Part explains the process of incidental collection and provides an analysis for why incidental collection is consistent with the Fourth Amendment. Section B explains the process of querying—specific to the FBI—and analogizes to similar searches conducted on DNA databases to conclude querying is in fact consistent with the Fourth Amendment.

A. Incidental Collection

Section 702 expressly prohibits the targeting of any U.S. person or any person located in the United States.[76] The government is also prohibited from "reverse targeting"—defined as targeting a non-U.S. person outside the United States when the primary interest is to acquire the communications of any person in the United States or a U.S. person with whom the foreign target is in contact.[77] However, due to the nature of the surveillance and collection, it is inevitable that the government may incidentally collect nontargeted U.S. persons' communications. Incidental collection refers to the collection of U.S. persons' communications obtained from the lawful targeting of a non-U.S. person located abroad.[78] For example, if a foreign terrorist is the target of section 702 surveillance and is communicating with a U.S. person or an individual located within the United States, the information relating to the U.S. person is considered to be incidentally collected. Incidental collection of U.S. persons' communications arises due to two techniques the government uses to collect foreign intelligence information.[79] The two techniques are commonly referred to as downstream[80] and upstream collection.[81] Downstream collection, also known as PRISM, is widely known due to the efforts of Edward Snowden, and is

74 PCLOB REPORT, *supra* note 20, at 86.

75 *Id.* at 87.

76 50 U.S.C. § 1805 (2012).

77 NSA SECTION 702 TRAINING, *supra* note 64, at 24.

78 *See* Kenneth L. Wainstein & R. Brendan Mooney, *Ample Safeguards of Civil Liberties Warrant FISA Section 702's Reauthorization by Congress*, HERITAGE FOUND. (Dec. 1, 2017).

79 *Id.* ("Incidental collection is an inevitable byproduct of any of the existing types of electronic communications surveillance—whether that surveillance is conducted under Section 702, under traditional FISA, under the criminal investigative wiretap authority in 18 U.S.C. § 2518, or under Executive Order 12333.").

80 OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, SECTION 702 OVERVIEW [hereinafter SECTION 702 OVERVIEW], https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf (last visited Nov. 15, 2018).

81 SHEDD ET AL., *supra* note 49, at 3.

used by all intelligence agencies.[82] PRISM functions through the cooperation of internet service providers (ISPs).[83] Once the government has information that a particular individual's name or email address is linked to foreign terrorist organization, the government identifies that name or email as a "selector."[84] The ISP is then required to relay any communications it has, either sent or received, from the identified selector. All data collected is subsequently available to the government through PRISM.[85]

By contrast, the collection technique of upstream collection does not rely on ISPs. Only the NSA is permitted to conduct upstream collection, and less than ten percent of its collection results from this technique.[86] This process functions through bypassing the individual ISP and focuses on compelling assistance from the companies that provide the telecommunications "backbone" over which these communications travel.[87] Under upstream collection, entire streams of internet traffic flowing across major U.S. networks are acquired and searched, as opposed to PRISM collection, under which particular user accounts are monitored, and communications to or from those accounts are collected, including communications with U.S. persons.[88]

Due to the nature of these programs, it is evident that they may result in the unintentional collection of U.S. persons' information. However, the FAA provides adequate protections for safeguarding incidentally collected information. Prior to utilizing a selector, the government must apply its targeting procedures to ensure each identified selector is used by a non-U.S. person who is reasonably believed to be located outside of the United States and who likely possesses foreign intelligence information.[89]

1. Constitutionality of Incidental Collection

Courts have continually held that to the extent the government incidentally collects communications of a U.S. person who is communicating with a section 702 target, such "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."[90]

---

82 Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST (June 12, 2013), https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/?utm_term=.fdd10424fcc0.

83 *See, e.g.*, PCLOB REPORT, *supra* note 20, at 7.

84 *Id.* at 6–7.

85 *See id.*

86 DAVID S. KRIS, HOOVER WORKING GRP. ON NAT'L SEC., TECH. & LAW, TRENDS AND PREDICTIONS IN FOREIGN INTELLIGENCE SURVEILLANCE 9 (2016), https://www.hoover.org/sites/default/files/research/docs/kris_trendspredictions_final_v4_digital.pdf; SECTION 702 OVERVIEW, *supra* note 80, at 4, https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf (last visited Nov. 15, 2018).

87 PCLOB REPORT, *supra* note 20, at 7 (internal quotation marks omitted).

88 *See, e.g.*, PCLOB REPORT, *supra* note 20, at 7.

89 TRANSPARENCY REPORT 2019, *supra* note 49, at 17.

90 *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008); *see also* United States v. Kahn, 415 U.S. 143, 156–57

To determine whether section 702 incidental collection is compliant with the Fourth Amendment, the Ninth Circuit in *United States v. Mohamud*[91] analyzed (1) if a warrant was required for the incidental collection of U.S. persons' communications, and (2) whether the process is reasonable.[92] In *Mohamud*, the Ninth Circuit held that the section 702 incidental acquisition of the defendant's email communications did not violate the Fourth Amendment.[93] Because the government had lawfully targeted an overseas foreign national under section 702, the defendant's email communications were thereafter incidentally collected.[94] Additionally, the court held that no warrant was required to intercept the U.S. person's communications incidentally.[95]

a. Warrant Requirement

As a threshold matter, the court stated "the Fourth Amendment does not apply to searches and seizures by the United States against a non-resident alien in a foreign country."[96] The Ninth Circuit stressed that it is the location of the target, not where the collection takes place, that matters.[97] Therefore, even though the collection of information though ISPs was done within the United States, if the target was reasonably believed to be located outside the United States, the Fourth Amendment does not apply.[98] Further, the Ninth Circuit stated, "[t]he fact that the government knew some U.S. persons' communications would be swept up during foreign intelligence gathering does not make such collection any more unlawful in this context than in the Title III or traditional FISA context."[99] The court found that because the target was a non-U.S. person outside the United States at the time of the surveillance, the government was not required to obtain a warrant to collect the U.S. person's communications with the foreign target as an incident to its lawful search of the foreign target.[100] The court acknowledged that because the search was exempt from the warrant requirement, there was no need to analyze the foreign intelligence exception.[101]

(1974) (holding interception of communications of a woman that were incidentally collected pursuant to a criminal wiretap order targeting her husband were lawful); United States v. Bin Laden, 126 F. Supp. 2d 264, 280 (S.D.N.Y 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment.").

91 843 F.3d 420 (9th Cir. 2016).

92 *Id.* at 438–42.

93 *Id.* at 444.

94 *Id.* at 438.

95 *Id.* at 439.

96 *Id.* (quoting *United States v. Zakharov*, 468 F.3d 1171, 1179 (9th Cir. 2006)); *see also* United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990).

97 *Mohamud*, 843 F.3d at 439 (citing *United States v. Hasbajrami*, No. 11–CR–623, 2016 WL 1029500, at *9 n.15 (E.D.N.Y. Mar. 8, 2016)).

98 *See id.*

99 *Id.* at 440.

100 *Id.* at 441.

101 *Id.* at 441 n.25.

b. Reasonableness Requirement

In deciding reasonableness under the Fourth Amendment, courts generally examine the totality of the circumstances and weigh "'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy.'"[102] In *Holder v. Humanitarian Law Project*,[103] the Court stated, "the Government's interest in combating terrorism is an urgent objective of the highest order."[104] In reviewing the government's interest, the court in *Mohamud* found that the government's sole interest was in protecting the United States from a terrorist threat.[105] In weighing the U.S. person's privacy interests whose communications have been incidentally collected, the court looks both at the reasonableness of individuals expectation of privacy and the government's minimization and targeting procedures.[106] The court in *Mohamud* relied on the third-party doctrine to demonstrate that the U.S. person had a diminished expectation of privacy when he assumed the risk to communicate with non-U.S. persons outside the United States.[107] The court then assessed the reasonableness of the inquiry based on whether the FISC-approved targeting and minimization measures sufficiently protected the privacy interests of the U.S. persons.[108] The court in *Mohamud* held government's minimization and targeting procedures sufficiently protected the U.S. person's privacy interests.[109] Therefore, the court held that even assuming the U.S. person is protected by a warrant requirement (which the court held U.S. person's incidental collection is not) that the search would still be reasonable under the Fourth Amendment.[110] As demonstrated by the court in *Mohamud*, information obtained through the lawful targeting of a non-U.S. person located abroad remains a constitutional acquisition whether or not the information collected is considered incidental.

102 Maryland v. King 569 U.S. 435, 448 (2013) (alteration in original) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

103 561 U.S. 1 (2010).

104 *Id.* at 28.

105 *See Mohamud*, 843 F.3d at 441.

106 *See id.* at 442–43.

107 *Id.* at 442; *see also* United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

108 *Mohamud*, 843 F.3d at 443.

109 *Id.* The court found the targeting procedures were reasonably designed to ensure the acquisition was limited to targeting persons reasonably located outside the United States and the minimization procedures were also reasonably designed to minimize the acquisition and retention of nonpublicly available information concerning U.S. persons. *Id.* at 443–44.

110 *See id.* at 444.

B. Queries

After finding that incidental collection is constitutional, there is a separate question of whether it is constitutional for intelligence agencies—particularly the FBI—to conduct subsequent warrantless queries on the collected communications to search the phone calls or emails of particular Americans, a practice known as "backdoor searches."[111] Following lawful acquisition of communications and information of non-U.S. persons located abroad, the government may conduct additional queries on section 702 collected information, including incidentally collected information.[112] Judge Hogan in a 2015 FISC opinion stated:

> Nothing in the statute precludes the examination of information that has otherwise been properly acquired through application of the targeting procedures and retained under the minimization procedures for the purpose of finding evidence of crimes, whether or not those crimes relate to foreign intelligence.[113]

Further, the House Permanent Select Committee on Intelligence stated:

> When NSA looks into its own database using U.S. person information, it is not a Fourth Amendment "search." NSA is not collecting any new information. Rather, NSA is simply looking through the database of foreign communications it already has.[114]

The NSA, FBI, and CIA's minimization procedures permit appropriately-trained personnel with access to section 702-acquired information to conduct

---

111 Elizabeth Goitein, *Americans' Privacy at Stake as Second Circuit Hears Hasbajrami FISA Case*, JUST SECURITY, (Aug. 24, 2018), https://www.justsecurity.org/60439/americans-privacy-stake-circuit-hears-hasbajrami-fisa-case/.

112 *Section 702: Backdoor Search Loophole*, CTR. FOR DEMOCRACY & TECH. (Mar. 15, 2017) [hereinafter *Section 702: Backdoor Search*], https://cdt.org/files/2017/06/2017-06-22-702-Backdoor-Search-One-pager.pdf. In this instance,

> [t]o "query" means to take a term, such as a name, phone number or email address, and use it to isolate communications with that term from a larger pool of data that an agency has already lawfully collected. Queries do not result in the additional collection of any information. Rather, they allow an agency to rapidly and efficiently locate foreign intelligence information, such as information potentially related to a terrorism plot against the United States, without having to sift through each and every communication that has been collected.

Letter from Dierdre M. Walsh, Dir. of Legislative Affairs, Office of the Dir. of Nat'l Intelligence, to Ron Wyden, U.S. Senator (June 27, 2014).

113 Memorandum Opinion & Order at 33, [Redacted], No. [Redacted], (FISA Ct. Nov. 6, 2015) [hereinafter 2015 Memorandum Opinion], https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf; *see also* Cody M. Poplin, *ONDI Releases Three FISC Opinions*, LAWFARE (Apr. 20, 2016), https://www.lawfareblog.com/odni-releases-three-fisc-opinions.

114 H.R. PERMANENT SELECT COMM. OF FOREIGN INTELLIGENCE, FISA SECTION 702 DEBATE 2, https://intelligence.house.gov/uploadedfiles/updated_usp_fact_check.pdf (last visited Nov. 15, 2018). The House Committee analogizes by stating, "This act is like police officers looking through an evidence locker to see if evidence from past crimes might help solve an open case. The police do not violate anyone's constitutional rights because they are simply reviewing evidence *already in their possession lawfully*, not carrying out a search." *Id.*

queries.[115] Queries are conducted by using an identifier, such as a phone number or email, to search through data that has already been acquired through section 702 collection.[116] However, as alluded to by Judge Hogan, information on U.S. persons' communications obtained through this additional warrantless query can be used to prosecute Americans for crimes unrelated to terrorism.[117] These additional queries, it is argued, are in direct violation of the Fourth Amendment as information pertaining to U.S. persons is obtained without a warrant and may be used to investigate and prosecute Americans for crimes unrelated to terrorism.[118]

In response to many concerns outlined in the PCLOB report, in 2018, Congress codified new requirements regarding access of U.S. person queries to the FBI.[119] Queries by FBI personnel of section 702 acquired data must be reasonably designed to "find and extract" either (1) foreign intelligence information, or (2) evidence of a crime.[120] Further, an order from the FISC is now required prior to the FBI reviewing contents of certain U.S.-person queries.[121] Specifically, a FISC order is required when the query is *not* designed to find and extract foreign intelligence information, and instead is performed in connection with a predicated criminal investigation not relating to national security.[122] Prior to issuance of an order based on probable cause from the FISC, a FBI agent must apply in writing and include justification that the query would provide evidence of criminal activity, which is to be approved by the Attorney General.[123] Enacted in 2015, the USA FREEDOM Act, instilled an additional requirement mandating public reporting of statistics regarding the number of U.S. person identifiers queried on section 702 information.[124] In 2018, the estimated number of search terms used in querying section 702 obtained communications of U.S. persons was 9637.[125] While the number of U.S. person query terms used to query section 702 content has risen consistently over the past three years, the FBI reported zero instances where FBI personnel reviewed section 702 information based on a query to return evidence of a crime unrelated to foreign intelligence.[126]

Additionally, information acquired under a section 702 query may *not* be introduced as evidence against that person in any criminal proceedings except with

115 *See* PCLOB REPORT, *supra* note 20, at 55.
116 *Id.*
117 *Section 702: Backdoor Search*, *supra* note 112.
118 *See id.*
119 *See* 50 U.S.C.A. § 1881a(f) (West, Westlaw through Pub L. No. 116-66); *see also* PCLOB REPORT, *supra* note 20, at 97 (calling for additional limits on the FBI's use and dissemination of section 702 data in connection with criminal investigations unrelated to foreign intelligence matters); *see also* Rachel Levinson-Waldman, *NSA Surveillance in the War on Terror*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 7, 36 (David Gray & Stephen E. Henderson eds., 2017).
120 50 U.S.C. § 1881a(f)(2)(A).
121 TRANSPARENCY REPORT 2019, *supra* note 49, at 14 n.1.
122 *Id.*
123 *Id.*
124 *Id.* at 13.
125 *Id.* at 14.
126 *Id.* at 16.

the approval of the Attorney General, and in criminal cases with national security implications or certain other serious crimes.[127] The 2017 FAA amendments additionally require the FBI to report on the number of instances in which they opened a criminal investigation of a U.S. person, who is not considered a threat to national security, based wholly or in part on section 702 acquired information.[128] As reported in the DNI Transparency Report, in 2017 and subsequently in 2018, there were zero instances in which the FBI opened a criminal investigation of a U.S. person who was not considered a threat to national security, based wholly or in part on section 702-acquired information.[129]

In 2015, the FISC held that the FBI's U.S.-person querying provisions within its minimization procedures, "strike a reasonable balance between the privacy interests of the United States person and persons in the United States, on the one hand, and the government's national security interests, on the other."[130] The 2015 FISC order also requires the government to report in writing, "each instance after December 4, 2015, in which FBI personnel receive and review section 702-acquired information that the FBI identifies as concerning a United States person in response to a query that is not designed to find and extract foreign intelligence information."[131] The new procedural requirements determine that the FBI is not permitted to engage in backdoor or pretextual searches of U.S. persons' incidentally collected information. Likewise, the data revealed in the DNI Transparency Report further demonstrates the FBI's compliance.

1. Constitutionality of Queries

Querying databases containing section 702 information does not result in any new acquisition of data; it is instead only an examination or reexamination of previously acquired information.[132] Therefore, queries are not separate searches for Fourth Amendment purposes.[133]

In similar database collections, such as DNA databases, courts have held that subsequent analyses of information previously collected do not rise to the level of a search under the Fourth Amendment, and thus can be used in unrelated criminal

127 2015 Memorandum Opinion, *supra* note113, at 30 n.28.

128 50 U.S.C.A. § 1873(b)(2)(D) (West, Westlaw through Pub L. No. 116-66).

129 OFFICE OF CIVIL LIBERTIES, PRIVACY & TRANSPARENCY, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT: REGARDING USE OF NATIONAL SECURITY AUTHORITIES 6 (Apr. 2018), https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017-----FINAL-for-Release-5.4.18.pdf*; see also* TRANSPARENCY REPORT 2019, *supra* note 49, at 16.

130 2015 Memorandum Opinion, *supra* note 113, at 44.

131 TRANSPARENCY REPORT 2019, *supra* note 49, at 16 (emphasis omitted).

132 SHEDD ET AL., *supra* note 49, at 6; Christopher Wray, Dir., FBI, Defending the Value of the FISA Section 702 at The Heritage Foundation (Oct. 13, 2017), https://www.fbi.gov/news/speeches/defending-the-value-of-fisa-section-702.

133 Office of the Dir. of Nat'l Intelligence, *The FISA Amendments Act: Q&A* (Apr. 18, 2017), https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf.

prosecutions.[134] For example, in *Maryland v. King*, the defendant was arrested and charged with first and second degree assault for "menacing a group of people with a shotgun."[135] As part of Maryland's routine booking procedures—pursuant to the Maryland DNA Collection Act—a DNA sample was collected from the defendant.[136] The DNA was uploaded to the Maryland DNA database and three weeks later was identified as a match for an unsolved rape case.[137] The DNA match resulted partly through the use of the Combined DNA Index System (CODIS), which connects DNA laboratories at the local, state, and national level.[138] The defendant was indicted and charged with the rape.[139] The defense sought to suppress the DNA match evidence on the grounds that the subsequent analysis of DNA in the Maryland DNA database violated the Fourth Amendment.[140] However, this argument was rejected and the defendant pleaded not guilty to the rape charges and was convicted and sentenced to life in prison without the possibility of parole.[141] Specific to the Maryland DNA Collection Act authorizing the initial intake of DNA, the Court reasoned that because the Act provided sufficient procedural protections[142] against further invasions of privacy, the initial collection and subsequent analysis was safeguarded from unconstitutional invasions of privacy.[143] Additionally, in weighing the interests of the parties, the Court reasoned that law enforcement's interest in being informed of potential dangers the arrestee posed to the public outweighed an arrested individual's diminished expectations of privacy.[144] The Court ultimately held that because the defendant's DNA was lawfully collected as part of routine booking procedure authorized by the Maryland DNA Collection Act, the subsequent analysis of the DNA, pursuant to procedures authorized by Congress in CODIS, did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment.[145]

---

134 Maryland v. King, 569 U.S. 435, 465 (2013); *see also* Scott L. Miley, *DNA Samples Linked to Unsolved Crimes*, TRIBSTAR (Apr. 17, 2017), https://www.tribstar.com/news/local_news/dna-samples-linked-to-unsolved-crimes/article_60ea852c-cb1c-5c91-89ff-426fda183caf.html (discussing forty-six matches to unsolved crimes from 3350 DNA samples taken over a three-month period after implementing enacting legislating for use of CODIS).

135 *King*, 569 U.S. at 440.

136 *Id.*

137 *Id.*

138 *Id.* at 444–45. CODIS was authorized by Congress in 1994 and is supervised by the FBI. CODIS sets uniform national standards for DNA matching and facilitates connections between local law enforcement agencies. *Id.*

139 *Id.* at 441.

140 *Id.*

141 *Id.*

142 Procedural protections included how the DNA was to be collected and stored as well as how and when DNA samples were to be tested. *Id.* at 443–44.

143 *Id.* at 463–65.

144 *Id.* at 437.

145 *Id.* at 465; *see also* Boroian v. Mueller 616 F.3d 60, 68 (1st Cir. 2010) ("[T]he "FBI's retention and periodic matching of the profile against other profiles . . . for the purpose of identification is not an intrusion on the offender's legitimate expectation of privacy and thus does not constitute a separate Fourth Amendment search."); Johnson v. Quander, 440 F.3d 489, 498

The same reasoning applies to section 702 queries with equal force. Similar to the Maryland DNA Collection Act, section 702 authorizes the collection of information; specifically, foreign intelligence information on non-U.S. persons located abroad.[146] As analyzed in Part III, information incidentally collected regarding U.S. persons is deemed constitutional and within the scope of section 702.[147] Once intelligence agencies have collected the information, it is held within databases.[148] Similar to how the DNA was analyzed through the Maryland DNA database and CODIS, queries are run through the previously acquired section 702 data and do not result in obtaining new or additional information. Therefore, if the FBI conducts a query and the results connect an individual to separate, unrelated criminal activity, similar to how the subsequent unrelated charge was brought in *King*, the FBI holds the requisite authority to make an arrest on the newly identified criminal activity. Additionally, the Court in *King* stressed the importance of the procedural protections the Maryland DNA Collection Act offered.[149] Section 702 has vast procedural protections at the outset of collecting foreign intelligence, including both the required targeting and minimization procedures. Section 702, however, provides even further procedural protections for the information once it is obtained and subsequently queried, including the querying procedures and rigorous oversight.[150] For instance, prior to the FBI reviewing contents of U.S. person queries unrelated to national security, the agents must receive explicit approval from the FISC.[151] Similar to the scope of DNA searches, queries are limited to information that has previously been collected under section 702 surveillance; therefore, the breadth of content is unlikely to be immensely personal.

In weighing the interests of the parties, here the U.S. person whose information was acquired incidentally may not have received notice of such acquisition, but viewed in a light similar to the third-party doctrine, because the U.S. person assumed the risk by communicating with a foreign national likely to be targeted under section 702, the U.S. person's expectation of privacy is diminished. Whereas, the government continues to have a heightened interest in pursuing queries to detect and prevent national security threats. Further, implementing a requirement that the government must obtain a warrant before using a U.S. person identifier to query section 702 would severely hamper the speed and efficiency of operations by creating an unnecessary barrier to national security professionals' ability to identify

(D.C. Cir. 2006) ("[A]ccessing the records stored in the [DNA] database is not a 'search' for Fourth Amendment purposes.").

146 50 U.S.C.A. § 1881a (West, Westlaw through Pub L. No. 116-66).

147 *See supra* Section III.A.

148 *See* TRANSPARENCY REPORT 2019, *supra* note 49, at 31.

149 *King*, 569 U.S. at 465.

150 50 U.S.C.A. § 1881a(f); *see also* Wainstein & Mooney, *supra* note 78 (discussing Executive, Congressional, and Judicial oversight of Section 702); Wray, *supra* note 132.

151 50 U.S.C.A. § 1881a(f)(2)(A). This additional layer of protection provides substantially more oversight and protection of individual liberty and privacy than exists in the context of the DNA databases, thus further strengthening the claim that subsequent queries are not searches subject to the Fourth Amendment.

potential threat information already in the lawful possession of the intelligence community.[152]

It is clear that the Court's decision and reasoning in *King* is directly applicable to the question of queries conducted on section 702 information. Therefore, because collection of information is lawfully obtained under section 702, and the statute provides narrow and precise procedural protections, the subsequent querying and unrelated charges brought do not amount to additional searches or significant invasions of privacy under which the Fourth Amendment would be implicated.[153]

CONCLUSION

FISA—and in particular section 702—remain vital and fundamental resources necessary for protecting national security. Yet, protecting national security should never come at the expense of impinging individual privacies and liberties. It is inevitable that the government will continue to be faced with challenges in reaching an appropriate balance of protecting national security while safeguarding individual liberties. However, section 702, specifically the process of querying, should perhaps be an example to Congress for the extent of procedural protections that must be in place for surveillance and subsequent searches to be consistent with the Fourth Amendment. The updated querying protections in the 2017 amendments provide sufficient limitations on queries in order to protect U.S. persons' incidentally collected information. Section 702 collection and subsequent queries provide the appropriate resources for intelligence agencies to conduct surveillance to protect national security while protecting U.S. persons' information that may be incidentally collected and subsequently queried.

152 OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, THE FISA AMENDMENTS ACT: Q&A 9 (2017).

153 This conclusion mirrors that of Judge Hogan, who in the 2015 FISC opinion stated that "[n]othing in the statute precludes the examination of information that has otherwise been properly acquired through application of the targeting procedures and retained under the minimization procedures for the purpose of finding evidence of crimes, whether or not those crimes relate to foreign intelligence." *See* 2015 Memorandum Opinion, *supra* note 113, at 33.