Washington Law Review

Volume 94 | Number 1

3-1-2019

Striking a Balance: Privacy and National Security in Section 702 U.S. Person Queries

Brittany Adams

STRIKING A BALANCE: PRIVACY AND NATIONAL SECURITY IN SECTION 702 U.S. PERSON QUERIES

Brittany Adams*

Abstract: The transformation of U.S. foreign intelligence in recent years has led to increasing privacy concerns. The Foreign Intelligence Surveillance Act of 1978 (FISA) traditionally regulated foreign intelligence surveillance by authorizing warrant-based searches of U.S. and non-U.S. persons. Individualized court orders under traditional FISA were intended to protect U.S. persons and limit the scope of intelligence collection. In a post-9/11 world, however, the intelligence community cited concerns regarding the speed and efficiency of collection under traditional methods. The intelligence and law enforcement communities recognized the "wall" preventing information sharing between the communities as a central failure leading to the 9/11 attacks. In response, the scope and authorizations of foreign intelligence collection were expanded with numerous statutory measures, culminating in the passage of Section 702. Under Section 702, only non-U.S. persons located abroad may be surveillance targets, but no warrant is required for the intelligence collection. Since its passage, the intelligence community and privacy advocates have intensely debated the implications of incidental collection of U.S. person communications, including the use of U.S. person queries. Despite the significant expansion of surveillance authorized in the shift from traditional FISA to Section 702, minimization and targeting procedures regulated by the new statute are designed to protect U.S. persons and balance national security and privacy interests.

This Comment addresses the uncomfortable question of whether the U.S. Constitution permits the minor intrusion of a few to protect national security and argues that Section 702 queries are searches under the Fourth Amendment that require a justification independent from the overall surveillance to be constitutional. Nonetheless, the Fourth Amendment protects against only unreasonable searches or seizures by the government, and U.S. person queries are reasonable searches characterized by critical foreign intelligence interests and robust safeguards that outweigh limited impacts on privacy. While the Fourth Amendment does require probable cause warrants for U.S. person queries conducted for criminal investigative purposes, such queries are rare. Striking the proper balance between privacy and security, particularly in the modern technological era, is a complex and challenging legal question. In this context, considerations must include policy and value-laden choices that weigh the statute's own regulatory measures against the rights protected by the Fourth Amendment. Such an approach renders U.S. person queries reasonable Fourth Amendment searches, albeit subject to more stringent requirements than courts and the government have previously found.

---

* J.D. Candidate, University of Washington School of Law, Class of 2019. Special thanks to David Kris for his guidance on the topic and invaluable insights on earlier drafts of this Comment. I would also like to thank the staff of *Washington Law Review* for their thoughtful suggestions and editorial work.

INTRODUCTION

After the September 11, 2001 terrorist attacks, the Intelligence Community (IC) urged Congress to grant it broader authority for surveillance of foreign persons.[1] Congress's responsive efforts led to the passage of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA).[2] Section 702[3] is a provision of the FAA that permits the government to collect intelligence on non-U.S. persons[4] located abroad by conducting targeted surveillance.[5] The government—namely the National Security Agency (NSA), the Central Intelligence Agency (CIA), and the Federal Bureau of Investigation (FBI)—uses the intelligence collected under Section 702 to "protect the United States and its allies from hostile foreign adversaries, including terrorists, [weapons] proliferators, and spies, and to inform cybersecurity efforts."[6] Section 702 intelligence has been used to prevent attacks on U.S. Armed Forces abroad, thwart weapons proliferation in the Middle East, prevent cybersecurity attacks on U.S. infrastructure, and recruit CIA assets.[7] Accordingly, officials in the IC have stated that Section 702 is "one of the most valuable tools that we have in our toolbox to keep America safe."[8]

---

1. *See, e.g.*, NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 78–80, 273–76 (2004) (discussing legal constraints and barriers preventing adequate counterterrorism responses within the intelligence community pre-9/11); *Administration Defends NSA Eavesdropping to Congress*, CNN (Dec. 23, 2005, 10:51 AM), http://www.cnn.com/2005/POLITICS/12/23/justice.nsa/index.html [https://perma.cc/CX74-BFN9] (discussing a Justice Department letter to Congress explaining that FISA lacks the "speed and agility" necessary to detect and prevent threats).

2. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified as amended in scattered sections of 50 U.S.C.).

3. *Id.* § 702 (codified at 50 U.S.C. § 1881a (2018)).

4. As defined in the statute, U.S. persons include U.S. citizens, U.S. permanent residents, groups substantially composed of U.S. citizens or permanent residents, and U.S. corporations. 50 U.S.C. § 1801(i). Non-U.S. persons are those persons who fall outside the statutorily enumerated categories of U.S. persons, including corporations or associations that are foreign powers. *Id.* § 1801(a)(1)–(3).

5. *See* FISA Amendments Act § 702.

6. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, SECTION 702 OVERVIEW, https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf [https://perma.cc/YB58-42A3].

7. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 108 (2014) [hereinafter PCLOB REPORT], https://www.pclob.gov/library/702-Report.pdf [https://perma.cc/D5Z7-D3BU] (discussing the use of Section 702 collected intelligence to protect national security, including the prevention of an attack on U.S. soil by a U.S. citizen connected to al-Qaeda).

8. Christopher Wray, Dir., Fed. Bureau of Investigation, Remarks at The Heritage Foundation: Defending the Value of FISA Section 702 (Oct. 13, 2017), https://www.fbi.gov/news/speeches/defending-the-value-of-fisa-section-702 [https://perma.cc/44XN-Q4ZV].

Notwithstanding these advantages, privacy and civil liberty advocates have raised concerns that Section 702 does not adequately protect U.S. persons' privacy.[9] Particularly, privacy advocates have challenged the use of terms identifying U.S. persons to "query," or search, the databases of Section 702 collected information.[10] Querying raises Fourth Amendment concerns over governmental access to U.S. person information incidentally collected during authorized surveillance on non-U.S. persons.[11] Even though U.S. persons cannot be targets of Section 702 surveillance, U.S. persons' communications may be swept up in the process.[12] Because U.S. person information may be incidentally yet lawfully collected in Section 702 surveillance, database queries may yield U.S. person communications.[13]

Privacy advocates have recommended imposing probable cause warrant requirements on such queries.[14] Currently, queries must be conducted to return foreign intelligence information[15] or evidence of a

---

9. *E.g.*, *Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act*, HUM. RTS. WATCH (Sept. 14, 2017, 1:54 PM), https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance [https://perma.cc/TC9B-Z64S] (discussing how Section 702 "violates the human right to privacy" and is inconsistent with basic human rights law); Derek Hawkins, *The Cybersecurity 202: Privacy Advocates Are Back in Court Fighting NSA Surveillance. It's an Uphill Battle.*, WASH. POST: POWERPOST (Sept. 4, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/04/the-cybersecurity-202-privacy-advocates-are-back-in-court-fighting-nsa-surveillance-it-s-an-uphill-battle/5b8d69f21b326b3f31919f29/?noredirect=on [https://perma.cc/U4WM-KWK6] (explaining the ongoing legal challenges to Section 702 surveillance brought by U.S. privacy groups).

10. *See* Letter from Forty-Seven Organizations to Bob Goodlatte, Chairman, and John Conyers, Ranking Member, U.S. House of Representatives (Oct. 13, 2017), https://www.fcnl.org/documents/465 [https://perma.cc/F32T-9YL5] (urging Congress to reform Section 702 and addressing concerns over querying).

11. *Id.* (discussing the use of U.S. person queries as an "exception" to the warrant requirement that threatens the privacy rights of "innocent Americans").

12. *See infra* Section I.B.2.b. for a discussion of incidental collection of U.S. person communications.

13. *See* NAT'L SEC. AGENCY, 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 4–5, 9–12 (2017) [hereinafter NSA MINIMIZATION PROCEDURES].

14. *See* USA Liberty Act of 2017, H.R. 3989, 115th Cong. (2017). This proposed bill would have required the government to obtain a probable cause order before querying Section 702 databases to retrieve content data. *Id.*

15. Foreign intelligence information is defined in 50 U.S.C. § 1801(e)(1) (2018) as "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against" potential or actual attacks or clandestine intelligence activities by foreign powers or their agents, weapons of mass destruction proliferation by foreign powers or their agents, sabotage, and international terrorism. It also includes information with respect to foreign powers, territories, or

crime, but no court order requirement exists for most searches.[16] Accordingly, privacy advocates are concerned that U.S. person queries evade the Fourth Amendment by allowing the government access to U.S. person communications that would otherwise require a warrant, earning the queries the title "backdoor searches."[17] In part, the concern arises from the FBI's ability to query data for criminal investigations, blurring the line between national security and domestic law enforcement.[18] While the most recent reauthorization imposes a court order requirement on the FBI in certain circumstances, the requirement does not go far enough to fully address privacy concerns.[19]

The IC suggests that a warrant requirement would hamper the speed and efficiency of surveillance operations and run counter to national security by delaying or potentially prohibiting access to intelligence identifying impending threats.[20] Additionally, queries do not result in any new intelligence collection but allow access only to communications that have already been collected lawfully under Section 702 surveillance procedures subject to significant internal and external oversight.[21] The FBI has responded that it is "extremely unlikely that an agent or analyst who is conducting an assessment of a non-national security crime would get a responsive result from the query against the Section 702-acquired data."[22] Nonetheless, the Fourth Amendment implications of U.S. person queries merit a focused analysis.

This Comment argues that querying is a separate search for Fourth Amendment purposes and is thus subject to Fourth Amendment

---

agents thereof, that is related to the "national defense or the security of the United States" or "the conduct of the foreign affairs of the United States." *Id.* § 1801(e)(2).

16. *See* FED. BUREAU OF INVESTIGATION, MINIMIZATION PROCEDURES USED BY THE FED. 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 19 (2016) [hereinafter FBI MINIMIZATION PROCEDURES]; NSA MINIMIZATION PROCEDURES, *supra* note 13, at 4–5.

17. *E.g.*, *Backdoor Search*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/pages/backdoor-search [https://perma.cc/MML5-BUD9] (noting that "the civil liberties community" refers to queries as the "'backdoor search' loophole in Section 702" surveillance).

18. *Id.* (noting concern that, under Section 702, "domestic law enforcement officials can, without a warrant, access Americans' communications that they would otherwise need a warrant to access").

19. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 101, 132 Stat. 3, 4–5 (2018).

20. *See* David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act* 5–6 (2007) (Brookings Inst., Georgetown Univ. Law Ctr. & Hoover Inst., Working Paper), https://www.brookings.edu/wp-content/uploads/2016/06/1115_nationalsecurity_kris.pdf [https://perma.cc/R4V3-LLMR] (discussing the government's concern with the restrictions imposed by the inefficiencies of the traditional FISA framework).

21. Wray, *supra* note 8 (explaining that the government is performing queries of information it has "already lawfully obtained").

22. PCLOB REPORT, *supra* note 7, at 8, 59–60.

reasonableness standards. However, given (1) the minimization procedures in place to protect the acquisition, retention, use, and dissemination of U.S. person information; (2) the statutorily required oversight; and (3) the foreign intelligence purpose of the surveillance, the queries are nonetheless reasonable. With some delineation between queries conducted for foreign intelligence purposes versus criminal investigative purposes, privacy rights may be adequately balanced with the government's compelling interests in national security and foreign intelligence.

Part I provides an overview of Section 702 surveillance procedures. In particular, Part I explains how the government collects intelligence under the statute and the procedures designed to limit intrusions on U.S. persons' privacy. Part II describes relevant Fourth Amendment law, including how courts define searches and seizures and interpret the reasonableness of Fourth Amendment searches in the context of modern technology. Part III concludes that U.S. person queries are constitutional Fourth Amendment searches. Generally, a warrant should not be required to conduct queries using U.S. person identifiers. Notwithstanding an exception for U.S. person queries performed for criminal investigations, minimization procedures and statutorily required oversight make reasonable an otherwise intrusive search.

I. POLITICAL AND STATUTORY FOUNDATIONS FOR SECTION 702 SURVEILLANCE

In 2008, Congress amended the Foreign Intelligence Surveillance Act of 1978 (FISA) with the passage of the FAA. Congress included a new provision in the FAA, known as Section 702.[23] Section 702 authorizes the IC to collect the electronic communications of targeted non-U.S. persons located outside the United States for foreign intelligence purposes.[24] Section 702 is a complex surveillance program involving the collection of multiple types of communications, obtained through numerous methods, for multiple purposes by multiple intelligence agencies. While Section 702 does not permit the IC to target U.S. persons in or outside of the United States, it does permit the incidental collection of U.S. persons' communications.[25] Such incidental collection is subject to procedural rules governing the use, retention, and dissemination of those

23. FISA Amendments Act § 702 (codified at 50 U.S.C. § 1881a (2018)).

24. *See id.*

25. PCLOB REPORT, *supra* note 7, at 6–9.

communications.[26] Each intelligence agency has its own rules governing the handling and use of the acquired data.[27] This Part provides context for the concerns surrounding querying Section 702 data, including: (1) the transition from "traditional FISA" to Section 702, (2) the operation of intelligence collection authorized under the statute, and (3) the development of Fourth Amendment law pertinent to electronic surveillance.

A. The Surveillance Expansion in the Transition from "Traditional FISA" to Section 702

FISA was originally enacted in 1978 to establish a court-sanctioned process allowing the U.S. Attorney General (AG) to conduct electronic surveillance on both U.S. and non-U.S. persons for foreign intelligence purposes.[28] This Act—now known as "traditional FISA"—required an individualized court order for each specific target the government intended to surveil.[29] Over time, Congress expanded the government's authority to conduct foreign intelligence surveillance within the FISA framework.[30] Perhaps the most notable addition is Section 702.

Section 702 has its roots in the surveillance program authorized by President Bush in the aftermath of the 9/11 attacks.[31] In response to the attacks, the intelligence and law enforcement communities acknowledged their limitations in failing to prevent 9/11.[32] Importantly, they recognized the existence of the "wall" between the two communities preventing information sharing.[33] To facilitate better homeland security and allow the government to "connect the dots," the pre-9/11 wall was removed, in part,

---

26. *Id.*

27. *Id.* at 2, 86.

28. *Id.* at 80; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, THE FISA AMENDMENTS ACT: Q&A 1–2 (2017), https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf [https://perma.cc/U737-525P].

29. PCLOB REPORT, *supra* note 7, at 80; *see* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 136, 154 (2015).

30. PCLOB REPORT, *supra* note 7, at 80.

31. *Id.* at 5.

32. *See generally* RICHARD A. BEST, JR., CONG. RESEARCH SERV., THE INTELLIGENCE COMMUNITY AND 9/11: CONGRESSIONAL HEARINGS AND THE STATUS OF THE INVESTIGATION (2003), https://fas.org/irp/crs/RL31650.pdf [https://perma.cc/A9EV-R7VP] (explaining the congressional hearings and public testimony regarding the IC and law enforcement responses to 9/11).

33. *Id.* at 8–9 (noting that a former inspector general of the Defense Department and other IC and law enforcement officials described the "walls derived from the provisions of the Foreign Intelligence Surveillance Act" as "unworkable and counterproductive set of bureaucratic hurdles").

with the Terrorist Surveillance Program (TSP).[34] TSP permitted the government to intercept contents of international communications outside of the traditional FISA process when the government believed that at least one party to a communication was a member of al-Qaeda or was supporting a related terrorist organization.[35] The Bush Administration cited FISA's lack of flexibility in identifying potential terrorist threats as justification for the new program.[36]

Under traditional FISA, acquisition of stored email from a U.S. provider's server within the country is considered "electronic surveillance."[37] As such, FISA's warrant requirement extended to non-U.S. persons having no connection to the United States except opening an email account with a U.S. provider. Thus, FISA's warrant requirement may have protected foreigners outside the United States who were considered potential threats. According to the Bush Administration, such a requirement inhibited the "speed and agility required" for early identification of potential terrorist threats.[38]

After information about TSP became public and the Administration faced increasing pressure regarding the legality of the program, the government sought and obtained authorization from the Foreign Intelligence Surveillance Court (FISC)[39] to transfer TSP collection to the

---

34. U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 1–3, 10–13 (2006) [hereinafter LEGAL AUTHORITIES NSA] (situating the executive's legal authority for TSP within the commander-in-chief's Article II powers and the Authorization for the Use of Military Force (AUMF)).

35. *Id.*; *see* OFFICES OF THE INSPECTORS GEN. OF THE DEP'T OF DEF., DEP'T OF JUSTICE, CENT. INTELLIGENCE AGENCY, NAT'L SEC. AGENCY & OFF. OF THE DIR. OF NAT'L INTELLIGENCE, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, REPORT NO. 2009-0013-A (2009), https://oig.justice.gov/special/s0907.pdf [https://perma.cc/VV6B-WGXB]; Press Release, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), https://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051219-1.html [https://perma.cc/8HNJ-4ERK].

36. Donohue, *supra* note 29, at 127. The Administration also initially claimed that TSP was fully consistent with FISA—primarily to avoid any difficult constitutional questions regarding FISA that would arise if the TSP violated the statute (namely whether traditional FISA unconstitutionally limits the president's Article II powers). LEGAL AUTHORITIES NSA, *supra* note 34, at 2–3.

37. 50 U.S.C. § 1801(f)(4) (2018).

38. U.S. DEP'T OF JUSTICE, LEGAL AUTHORITY FOR THE RECENTLY DISCLOSED NSA ACTIVITIES 3, https://www.justice.gov/sites/default/files/ag/legacy/2007/01/11/surveillance11.pdf [https://perma.cc/KC72-AFPR].

39. The FISC was established by traditional FISA and is composed of eleven federal district court judges sitting in a secure courtroom in a federal courthouse in Washington, D.C. *About the Foreign Intelligence Surveillance Court*, U.S. FOREIGN INTELLIGENCE SURVEILLANCE CT., http://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court [https://perma.cc/A8HR-MFVQ]. The FISC reviews U.S. government applications for "approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes" and most hearings

FISA framework.[40] In January 2007, the FISC authorized the government to conduct electronic surveillance of telephone and internet communications into and out of the United States under FISA when: (1) the government had probable cause to believe that at least one of the communicants was a member or agent of al-Qaeda or an affiliated terrorist organization, and (2) the government reasonably believed at least one of those communicants was located outside the United States.[41] In May 2007, when the government sought renewal of the program, the FISC reauthorized the surveillance but modified the program to require the *court*, as opposed to the government, to make probable cause determinations regarding the foreign targets.[42] In requiring court approval of individual targets, the FISC effectively rejected the key innovation of the Administration's surveillance program—i.e., the enhanced "speed and agility" permitted by requiring only executive-branch approvals.[43]

Separate from TSP collection, a second intelligence collection effort was underway within the traditional FISA framework.[44] This effort required individualized court orders to compel private communications companies to assist the government in collecting the communications of targeted persons located outside the United States.[45] Noting concerns with

---

and opinions issued by the court are classified. *Id.* For more information, see David Kris, *How the FISA Court Really Works*, LAWFARE (Sept. 2, 2018, 5:29 PM), https://www.lawfareblog.com/how-fisa-court-really-works [https://perma.cc/96VL-GBYJ].

40. 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 [https://perma.cc/KQ6A-KGHR]. The New York Times disclosed TSP to the public after delaying publication for one year because the Bush administration cited concerns that disclosure would threaten national security. *Id.*; *see* PCLOB REPORT, *supra* note 7, at 5; Donohue, *supra* note 29, at 8; Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006, 10:38 AM), https://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm (last visited Jan. 28, 2019); Josh Meyer & Joseph Menn, *U.S. Spying Is Much Wider, Some Suspect*, L.A. TIMES (Dec. 25, 2005), http://articles.latimes.com/2005/dec/25/nation/na-spy25 [https://perma.cc/TMP2-8TZR] (discussing TSP's broad intelligence collection authority and the potential threat to individual privacy).

41. Brief for the Respondents in Opposition at 1–2, ACLU v. Nat'l Sec. Agency, 552 U.S. 1179 (2008) (No. 07-648) (mem.) *denying cert. from* 493 F.3d 644 (6th Cir. 2007); Classified Certification of the Attorney General of the United States at ¶ 37, *In re* Nat'l Sec. Agency Telecomms. Records Litig., 633 F. Supp. 2d 949 (N.D. Cal. 2009) (MDL Dkt. No. 06-1791-VRW).

42. PCLOB REPORT, *supra* note 7, at 7, 116.

43. Brief for the Respondents in Opposition, *supra* note 41, at 2; Eric Lichtblau, James Risen, and Mark Mazzetti, *Reported Drop in Surveillance Spurred a Law*, N.Y. TIMES (Aug. 11, 2007), https://www.nytimes.com/2007/08/11/washington/11nsa.html [https://perma.cc/BKE9-M6FW] (discussing interactions with Congressional officials on FISA requirements, including a reported "intelligence gap").

44. PCLOB REPORT, *supra* note 7, at 18.

45. *See id.*

both programs, the government stated that it and the FISC were expending "considerable resources" to obtain probable cause court orders.[46] As a result, the acquisition of foreign intelligence necessary to further U.S. national security interests was often delayed or prohibited.[47]

Accordingly, in April 2007, the Bush Administration submitted a proposal to Congress to modify FISA.[48] In response, Congress passed the Protect America Act of 2007 (PAA)[49]—the precursor to Section 702. The PAA combined the authority for both TSP and the separate collection effort involving individualized FISC orders into a single legislative authorization.[50] When the PAA expired in February 2008, Congress replaced it with Section 702 of the FAA.[51] Congress most recently reauthorized Section 702 in January 2018.[52]

Section 702 was widely debated both at its initial passage in 2008 and during its reauthorization in 2018.[53] Section 702 differs in significant ways from traditional FISA. Fundamentally, Section 702 is a large-scale foreign intelligence surveillance program while traditional FISA is a targeted surveillance program. Unlike traditional FISA, Section 702 does not require individualized court orders because it does not permit targeting of U.S. persons.[54] Nonetheless, traditional FISA's protections reduce the likelihood of improper surveillance and collection of U.S. person communications.[55] Additionally, Section 702 eliminates the requirements imposed by traditional FISA that surveillance targets be foreign powers

---

46. *The Foreign Intelligence Surveillance Act: Hearing Before the H. Comm. on the Judiciary*, 110th Cong. 5 (2008) (Statement of Kenneth L. Wainstein, Assistant Attorney General, National Security Division, Department of Justice).

47. *See id.* at 5–6, 18.

48. *See* S. Rep. No. 110-209, at 2, 5 (2007); Donohue, *supra* note 29, at 13.

49. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552.

50. PCLOB REPORT, *supra* note 7, at 19.

51. *See id.*

52. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 101, 132 Stat. 3, 4–5 (2018).

53. *See, e.g.*, Senate Debate on FISA Reauthorization, 115th Cong. (Jan. 16, 2018), https://www.c-span.org/video/?439676-3/senate-debate-fisa-reauthorization [https://perma.cc/87YU-H9NR] (footage of the Senate debate over FISA reauthorization, expressing concerns over the use of Section 702 in domestic surveillance); Press Release, Senator Mike Lee, Sens. Lee, Leahy Release Joint Statement on Upcoming Debate on Section 702 Legislation (Jan. 11, 2018), https://www.lee.senate.gov/public/index.cfm/2018/1/sens-lee-leahy-joint-statement-on-house-passage-of-fisa-reauthorization [https://perma.cc/P32N-MNFV] (calling for alternatives to Section 702 noting that the reauthorization bill "falls short in providing critical protections for Americans").

54. 50 U.S.C. § 1881a (2018).

55. *Id.*

or agents of foreign powers.[56] Compared to Section 702, traditional FISA's protections limit the scope and amount of communications collected.[57] However, traditional FISA required significant legal protection—even for targets with no connection to the United States—and technological advances made it difficult to administer.[58] Conversely, Section 702 reduces these protections and does not require the same level of authorizations.[59]

Under Section 702, the range of people whom the government may target is much broader than traditional FISA.[60] Section 702 surveillance is not limited to foreign powers and agents of a foreign power but extends to any foreign person located abroad who is "reasonably believed" to communicate specified kinds of foreign intelligence information.[61] That person, however, need not be engaging in any international terrorism or criminal activity—it is enough that the government believes a person may possess information about such activity.[62] By way of comparison, approximately 129,080 targets were surveilled under Section 702 in 2017 while significantly less—1,337—were surveilled under traditional FISA in the same year.[63] Even so, Section 702 collection is anything but unrestricted—targeting and minimization procedures, and many layers of internal and external oversight, govern the program for statutory and constitutional compliance. Nonetheless, the increased scope and expansive collection authorized under Section 702 combined with technological advances allowing the acquisition and retention of vast

---

56. *Id.* § 1804(a)(3); *id.* § 1801(b)(2)(A)–(E) (defining agents of foreign power to include any person who, on behalf of a foreign power, "knowingly engages in clandestine intelligence gathering activities" that "involve or may involve" criminal conduct, "sabotage or international terrorism," entering the U.S. under "under a false or fraudulent identity," or aiding and abetting any of the aforementioned).

57. PCLOB REPORT, *supra* note 7, at 115–16.

58. David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, 3 (Hoover Inst. Working Grp. on Nat'l Sec., Tech., & Law, Paper No. 1601, 2016), https://www.hoover.org/sites/default/files/research/docs/kris_trendspredictions_final_v4_digital.pdf [https://perma.cc/6VV8-NKZ8] ("In particular, the rise of web-based e-mail and other developments made it more difficult to determine the location of parties to an intercepted communication" and traditional FISA is "dependent on knowledge of those locations").

59. *See* 50 U.S.C. § 1881a.

60. PCLOB REPORT, *supra* note 7, at 115.

61. 50 U.S.C. § 1881a.

62. *See id.*; PCLOB REPORT, *supra* note 7, at 115.

63. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: CALENDAR YEAR 2017, at 8, 14 (2018), https://www.dni.gov/files/documents/icotr/2018-ASTR——CY2017——FINAL-for-Release-5.4.18.pdf [https://perma.cc/6SBV-FBRZ].

amounts of data raise important Fourth Amendment concerns for U.S. person communications swept up in the process.[64] These shifts are critical to the constitutionality analysis of U.S. person queries.

B. How Section 702 Collection and Surveillance Works

To understand the concerns over database queries, one must understand fundamentally how Section 702 collection functions. Section 702 permits the government to target "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[65] A person may be targeted for collection if the person is likely to possess, receive, or communicate foreign intelligence.[66] Broadly speaking, Section 702 permits the AG and the Director of National Intelligence (DNI) to compel the assistance of U.S.-based electronic communication service providers (ECSPs) to acquire a variety of communications for foreign intelligence purposes.[67]

Section 702 collection is subject to considerable oversight and regulation.[68] While multiple intelligence agencies have authority under Section 702, this Comment focuses specifically on the differences between NSA and FBI procedures to elucidate the relevant privacy concerns.[69] The following sections explain the procedures used to collect and protect data under Section 702.

---

64. *See generally* PCLOB REPORT, *supra* note 7 (reviewing and analyzing Section 702 for statutory and constitutional compliance, paying particular attention to Fourth Amendment privacy concerns and making policy recommendations to mitigate privacy intrusions in the context of querying).

65. Procedures for Targeting Certain Persons Outside the United States Other than United States Persons, FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2438 (codified at 50 U.S.C. § 1881a); *see* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 28, at 9.

66. *See* PCLOB REPORT, *supra* note 7, at 22. For the statutory definition of foreign intelligence, see *supra* note 15.

67. PCLOB REPORT, *supra* note 7, at 20. Under traditional FISA, court orders were required to compel providers to assist the government in acquisition and collection, but under Section 702, the AG and DNI have authority to issue directives to ECSPs requiring their assistance. 50 U.S.C. § 1881a(i)(1). If the ECSPs fail to comply, the AG may file a petition with the FISC to compel their compliance. *Id.* § 1881a(i)(5)(A).

68. *See, e.g.*, FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, tit. I, 132 Stat. 3, 4 (2018) (explaining the statutorily required safeguards, accountability, and oversight).

69. The CIA and National Counterterrorism Center (NCTC) also have authority to conduct intelligence collection activities under Section 702 and minimization procedures to govern their activities. *See generally* CENT. INTELLIGENCE AGENCY, 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 (2016) [hereinafter CIA MINIMIZATION PROCEDURES].

1. Targeting and Minimization Procedures Protect U.S. Person Information

As the only agency that can initiate data collection, the NSA regulates all data acquisition occurring under Section 702 with its targeting procedures.[70] After acquisition, each agency's minimization procedures regulate the retention, dissemination, and use of the data.[71] Each agency acquiring or accessing Section 702 intelligence must develop and comply with its respective minimization procedures.[72] As of the latest annual report in April 2018, the NSA is authorized to collect intelligence on 129,080 foreign targets.[73] This section will define targeting procedures that govern data acquisition and other minimization procedures used to reduce the collection of U.S. person information.

a. Surveillance Targets Must Not Be U.S. Persons

Under Section 702, intelligence agencies "target" persons[74] for intelligence collection by "tasking" specific "selectors."[75] A selector must be a unique communications facility, such as a telephone number or email address associated with a target, and cannot be a keyword or name, such as "bomb" or "al-Baghdadi."[76] The user of a tasked selector is the Section 702 "target."[77] Targets of collection may not include U.S. persons or "any person known at the time of acquisition to be located in the United States."[78]

The NSA's targeting procedures require analysts to make two assessments when identifying potential targets: (1) the "foreignness" requirement and (2) a determination that the person possesses or is likely

---

70. 50 U.S.C. § 1881a; PCLOB REPORT, *supra* note 7.

71. PCLOB REPORT, *supra* note 7, at 6–7.

72. *See generally* CIA MINIMIZATION PROCEDURES, *supra* note 69; FBI MINIMIZATION PROCEDURES, *supra* note 16; NSA MINIMIZATION PROCEDURES, *supra* note 13.

73. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 63, at 14.

74. "Person" is defined broadly in the statute and may include a foreign government, terrorist group, other entity or association, a corporation, or foreign power, in addition to individuals. PCLOB REPORT, *supra* note 7, at 20–21 (discussing 50 U.S.C. §§ 1801(a), 1801(m)).

75. PCLOB REPORT, *supra* note 7, at 32.

76. *Id.* at 33; NAT'L SEC. AGENCY, NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 4 (2014) [hereinafter NSA'S IMPLEMENTATION OF FISA], https://fas.org/irp/nsa/clpo-702.pdf [https://perma.cc/9WUP-7F62].

77. *Id.* at 32–33.

78. 50 U.S.C. § 1881a(b)(1).

to possess approved foreign intelligence information.[79] The "foreignness" assessment requires analysts to assess and determine that each potential target is a non-U.S. person located outside the United States.[80] This test is "not a 51% to 49% 'foreignness' test"[81]—the analyst must resolve any ambiguities regarding location or status of a target as a U.S. person before making the foreignness determination.[82] In addition to the foreignness requirement, the analyst must determine that tasking a specific selector will likely lead to the acquisition of foreign intelligence information that falls within one of the categories identified by the government in its annual certification approved by the FISC.[83] Unlike traditional FISA, the FISC does not review the individual persons who will be surveillance targets; rather, under Section 702, it reviews categories of intelligence about which targets must be likely to communicate.[84] Upon making those determinations, the analyst assesses "how, when, with whom, and where the target communicates" to ascertain a specific selector to be tasked.[85] Two senior analysts must review the analyst's determination to ensure that the tasking request meets the NSA's targeting procedure requirements.[86]

After review, the AG and DNI issue directives to ECSPs and companies that maintain communications networks to compel their assistance in acquiring intelligence.[87] ECSPs must assist the IC in collecting communications to and from authorized targets for a period of up to one year.[88] Even after the intelligence collection begins, the NSA

---

79. NSA'S IMPLEMENTATION OF FISA, *supra* note 76, at 43; PCLOB REPORT, *supra* note 7, at 23. Additionally, the statute expressly prohibits "reverse targeting," or using the targeting of a foreigner abroad to collect intelligence on a "particular, known person" inside the United States. 50 U.S.C. § 1881a(b)(2).

80. NSA'S IMPLEMENTATION OF FISA, *supra* note 76, at 43; PCLOB REPORT, *supra* note 7, at 23.

81. NSA'S IMPLEMENTATION OF FISA, *supra* note 76, at 4.

82. *Id.*; PCLOB REPORT, *supra* note 7, at 43.

83. *See* PCLOB REPORT, *supra* note 7, at 45. The scope of categories in these executive certifications has not been declassified, but officials in the IC have stated that the certifications concern international terrorism and acquisition of weapons of mass destruction, among others. NAT'L SEC. AGENCY, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 4–6 (2017) [hereinafter NSA TARGETING PROCEDURES 2016]; PCLOB REPORT, *supra* note 7, at 25.

84. PCLOB REPORT, *supra* note 7, at 24–27.

85. NSA'S IMPLEMENTATION OF FISA, *supra* note 76, at 4.

86. PCLOB REPORT, *supra* note 7, at 46. These tasking requests are also subject to external oversight by the Department of Justice (DOJ) and the Office of the DNI. The DOJ and the Office of the DNI review the tasking and targeting decisions to ensure statutory compliance. *Id.* at 70–72.

87. *Id.* at 32.

88. 50 U.S.C. § 1881a(a) (2018).

has post-tasking requirements.[89] NSA analysts routinely review samples of Section 702 acquired communications to verify that tasked selectors remain associated with foreign intelligence and the target remains abroad.[90] Analysts also reevaluate each selector annually to determine whether it continues to meet the requirements—foreignness and foreign intelligence purpose—specified in NSA targeting procedures.[91] Upon determining that a selector is a U.S. person or located in the United States, the NSA sends a request to the ECSP acquiring intelligence to detask, or halt collection, on the relevant selector.[92]

b. Minimization Procedures Are Designed to Balance Privacy with National Security

After acquisition, and before an agency moves data to a permanent retention database, trained personnel must review data to ensure it is limited only to requested information and meets the agency's standards for retention.[93] If personnel find U.S. person information in collected data, such data must be "necessary to understand foreign intelligence information, . . . assess its importance," or provide evidence of a crime to be permanently retained.[94] Information that has been reviewed by an analyst and determined to meet this standard is considered "minimized."[95]

89. PCLOB REPORT, *supra* note 7, at 48.

90. *Id.*

91. *Id.*

92. Any data acquired from a selector while that selector is in the United States (or after determination that the target is a U.S. person) must be purged. PCLOB REPORT, *supra* note 7, at 61. Additionally, errors must generally be reported to the DNI, the Department of Justice, Congress, and sometimes the FISC. 50 U.S.C. § 1881f(b)(1)(G); PCLOB REPORT, *supra* note 7, at 66–68; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, FACT SHEET: SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) (2017), https://www.dni.gov/files/documents/icotr/Overview_Fact_Sheet-702-Joint-Assessment13-14-15-11017.pdf [https://perma.cc/C55Y-HSX9].

93. PCLOB REPORT, *supra* note 7, at 60–62.

94. FBI MINIMIZATION PROCEDURES, *supra* note 16, at 22; NSA MINIMIZATION PROCEDURES, *supra* note 13, at 12–13.

95. If the analyst determines through this review that the tasked selector will not yield the requested information (e.g., that johndoe@isp.com is not going to be used to communicate about international terrorism), the government will send a de-tasking request to the communications provider to halt collection for that specific selector. PCLOB REPORT, *supra* note 7, at 34, 61–63.

As a security measure, each agency separately retains data.[96] As such, each agency must create and follow its own minimization procedures.[97] According to the statute, such procedures must be "reasonably designed" to "minimize the acquisition and retention . . . of nonpublicly available information concerning unconsenting United States persons" that may be collected during authorized intelligence collection.[98] Information that has not yet been reviewed and evaluated by government personnel is kept in repositories separate from minimized data.[99] Because unminimized data runs a higher risk of including U.S. person information, each agency's minimization procedures limit the access of such data to trained personnel, and it generally must be aged off agency systems within five years.[100] Broadly speaking, the process proceeds as follows: after acquisition, IC personnel review collected data to minimize the retention of U.S. person information; then, data will be either purged or retained based on the result of that evaluation.

2. U.S. Person Communications May Be Lawfully Incidentally Collected

Because U.S. persons and persons located inside the United States cannot be targets, Section 702 does not permit the comprehensive collection of communications from a single U.S. person. In other words, the government will not have access to all emails or telephone calls sent by any specific U.S. citizen under this program (absent mistake or abuse).[101] Even so, U.S. person information may be acquired incidentally or inadvertently during authorized intelligence collection.[102] This section first explains how the IC conducts Section 702 intelligence acquisition

---

96. *See id.* at 54, 60–63.

97. *See id.* at 50–59. The agencies each have provisions in their minimization procedures allowing them to depart from approved procedures in cases of "immediate threat to human life" (e.g., a hostage situation). NSA MINIMIZATION PROCEDURES, *supra* note 13, at 1. Any departure must be reported to the National Security Division of the Department of Justice and, subsequently, to the FISC. *Id.*; FBI MINIMIZATION PROCEDURES, *supra* note 16, at 3.

98. 50 U.S.C. § 1801(h)(1) (2018); *see* NSA MINIMIZATION PROCEDURES, *supra* note 13, at 1.

99. NSA MINIMIZATION PROCEDURES, *supra* note 13, at 53.

100. PCLOB REPORT, *supra* note 7, at 53, 55–56; *see* FBI MINIMIZATION PROCEDURES, *supra* note 16, at 22; NSA MINIMIZATION PROCEDURES, *supra* note 13, at 5.

101. 50 U.S.C. § 1881a; PCLOB REPORT, *supra* note 7, at 113–14.

102. PCLOB REPORT, *supra* note 7, at 6. Prior to the NSA halting "about" collection, communications between U.S. persons might also have been acquired when a targeted selector (e.g., the email address of a targeted suspected terrorist) appeared in the body of an email between U.S. persons. *See id.* at 113.

and then how U.S. person information may be lawfully included in that acquisition.

a. Data Acquisition Occurs via PRISM and Upstream Collection

Initially, agencies could acquire data either by downstream collection or upstream collection, both of which are defined below.[103] In April 2017, however, the NSA ceased most forms of upstream collection and limited others.[104] Thus, Section 702 data acquisition is now conducted primarily by PRISM, the code name for the NSA's downstream surveillance tool.[105] The NSA receives all communications acquired through PRISM, and the NSA, CIA, FBI, and National Counterterrorism Center (NCTC) each have access to raw PRISM-acquired data.[106] The NSA is the only agency that receives and retains unminimized data acquired through upstream collection.[107] All told, the FBI receives approximately 4.3% of the NSA's total collection.[108]

PRISM collection involves compelling the assistance of various ECSPs.[109] For example, an NSA analyst investigating lead information about John Doe—a non-U.S. person living outside the United States—discovers John Doe uses a specific email address (e.g.,

---

103. *Id.* at 33.

104. PCLOB REPORT, *supra* note 7, at 33; Press Release, NSA, NSA Stops Certain Section 702 "Upstream" Activities (Apr. 28, 2017) [hereinafter NSA Statement], https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities [https://perma.cc/Y3D8-E6B6].

105. PRISM technically stands for "Planning Tool for Resource Integration, Synchronization, and Management," but it is known by its code word, "PRISM." Benjamin Dreyfuss & Emily Dreyfuss, *What Is the NSA's PRISM Program? (FAQ)*, CNET (June 7, 2013, 11:44 AM), https://www.cnet.com/news/what-is-the-nsas-prism-program-faq/ [https://perma.cc/WUK4-5Z9P].

106. PCLOB REPORT, *supra* note 7, at 53; Jordan Brunner et al., *Foreign Intelligence Surveillance Court Approves New Targeting and Minimization Procedures: A Summary*, LAWFARE (May 15, 2017, 12:13 PM), https://www.lawfareblog.com/foreign-intelligence-surveillance-court-approves-new-targeting-and-minimization-procedures-summary [https://perma.cc/T8JP-34XN]. The CIA, FBI, and NCTC, however, do not have access to any unminimized data collected by upstream collection methods (only the NSA has this access). *See* PCLOB REPORT, *supra* note 7, at 35.

107. *See* PCLOB REPORT, *supra* note 7, at 39–40. MCTs are not entered into government databases until they have been filtered to remove domestic transactions. *Id.* at 37, 54.

108. Devlin Barrett, *FBI Director Warns Against Restricting Controversial NSA Surveillance Program*, WASH. POST (Oct. 13, 2017), https://www.washingtonpost.com/world/national-security/fbi-director-warns-against-restricting-controversial-nsa-surveillance-program/2017/10/13/a40a0b3c-b02a-11e7-a908-a3470754bbb9_story.html?utm_term=.99234b0e8edb [https://perma.cc/RN2M-ZJTN] (noting that FBI Director Christopher Wray has said "that 4.3 percent is unbelievably valuable to our mission").

109. PCLOB REPORT, *supra* note 7, at 33; *see supra* Section I.B.1.a for more information on the compelled assistance of ECSPs.

johndoe@gmail.com) to communicate with affiliates about international terrorist activities.[110] The NSA, following its targeting procedures, would "task[]" that email address for Section 702 acquisition to obtain foreign intelligence information falling within one of the pre-approved intelligence categories by the FISC (here, presumably, international terrorism).[111] The IC then sends the tasked email address to an ECSP, and the company must provide the government all communications sent to or from the email address.[112]

Before April 2017, the NSA also acquired communications through a second method—upstream collection.[113] Upstream collection occurred by intercepting communications directly from the communications "backbone" (i.e., data that is transiting between the communications networks), instead of the compelled assistance of a specific ECSP.[114] In upstream collection of internet communications, collection of internet *transactions* is possible.[115] An internet transaction may consist of a single communication—for example, an email being sent from one server to another—or multiple communications (MCTs)—for example, populating a webmail server inbox, such as a Gmail inbox.[116] The NSA's filtering mechanisms cannot distinguish between individual communications that are purely between U.S. persons and the whole MCT, allowing the possibility of collecting a communication merely "about" a tasked selector.[117] Accordingly, the FISC ordered the NSA to destroy an entire MCT upon a determination that any communication within a transaction is "not to or from persons targeted in accordance with NSA's Section 702 targeting procedures."[118]

In response, the NSA eliminated "about" collection from its acquisition methods—thus eliminating a great deal of the communications previously obtained through upstream collection and decreasing the likelihood of

110. PCLOB Report, *supra* note 7, at 34.

111. *Id.*

112. *Id.*

113. NSA MINIMIZATION PROCEDURES, *supra* note 13, at 4.

114. PCLOB REPORT, *supra* note 7, at 35.

115. An internet transaction is essentially several pieces of data traveling together "across the Internet." *Id.* at 39.

116. *Id.*; Parker Higgins, *Intelligence Agency Attorney on How "Multi-Communication Transactions" Allowed for Domestic Surveillance*, ELECTRONIC FRONTIER FOUND. (Aug. 21, 2013), https://www.eff.org/deeplinks/2013/08/intelligence-agency-attorney-explains-how-multi-communication-transactions-allowed [https://perma.cc/Y49D-V2YZ].

117. PCLOB REPORT, *supra* note 7, at 39–40.

118. [Redacted], 2011 WL 10947772, at *7–9 (FISA Ct. Nov. 30, 2011) (mem.); NSA MINIMIZATION PROCEDURES, *supra* note 13, at 4.

acquiring U.S. person communications.[119] Nevertheless, data formerly acquired upstream remains stored in Section 702 databases and, until it is aged off agency systems, analysts may still query such data. Only analysts trained in reviewing MCTs may access that repository and MCTs must age off NSA systems within two years.[120] Other intelligence agencies cannot view or query data collected upstream before the NSA applies its minimization procedures.[121] While the 2018 FAA reauthorization allows the NSA to recommence "about" collection, it may only do so after notifying Congress and receiving approval from the FISC.[122] Absent some technological development that allows the NSA to distinguish between communications involving a target and communications merely "about" a target, renewal of the program is unlikely.[123]

b. U.S. Person Information May Be Collected Incidentally or Accidentally

Incidentally collected U.S. person information—information obtained when a U.S. person is communicating with a foreign target or when a foreign target's communications contain U.S. person information—may be retained and used subject to minimization.[124] Inadvertently (or accidentally) collected U.S. person information, however, must generally be destroyed.[125]

When a person who is targeted for surveillance communicates by phone or email with another person, the second person's information is said to be "incidentally" collected.[126] In the context of U.S. person information, incidental collection occurs when a foreign target located

---

119. NSA Statement, *supra* note 104 (noting that the elimination of upstream collection also reduced relevant foreign intelligence information); Adam Klein, *The End of "About" Collection Under Section 702*, LAWFARE (May 1, 2017, 10:07 AM), https://www.lawfareblog.com/end-about-collection-under-section-702 [https://perma.cc/WP6T-5XA9].

120. NSA MINIMIZATION PROCEDURES, *supra* note 13, at 5 (requiring destruction of MCTs unless the NSA determines that at least one of the communications in the transaction meets the agency's retention standards).

121. *See generally id.* (describing the procedures governing the NSA's acquisition, retention, access, use, and dissemination of Section 702 data).

122. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 101, 132 Stat. 3 (2018).

123. George W. Croner, *Terrorists, America Is Still Listening: Section 702 Is Alive and Well*, FOREIGN POL'Y RES. INST. (Jan. 22, 2018), https://fpri.org/article/2018/01/terrorists-america-still-listening-section-702-alive-well/ [https://perma.cc/Z7MW-HTED].

124. PCLOB REPORT, *supra* note 7, at 6.

125. *Id.*

126. *Id.* at 114.

overseas communicates with a U.S. person.[127] Incidental collection can also occur when two foreign targets located abroad discuss a U.S. person in the contents of their communications (e.g., two targets being surveilled under Section 702 are emailing, and the body of the email contains a passport belonging to a U.S. person).[128] The amount of U.S. person communications acquired incidentally is unknown; however, the IC targets approximately .004% of the world's internet users for Section 702 surveillance and .001% of the world's population.[129] Therefore, the odds of acquiring any one U.S. person's communications incidentally are incredibly low.

Sometimes, U.S. person communications, or the communications of persons located in the United States, are collected accidentally.[130] Accidental collections are referred to as "inadvertent" collection.[131] For example, inadvertent collection may occur when the NSA mistakenly believes a target is a foreign citizen, or an analyst types a selector incorrectly during the targeting process.[132] Inadvertent collection can also be a result of a technological malfunction.[133] In 2013, the U.S. Department of Justice reviewed the NSA's annual data and determined that only 0.4% of NSA's targeting decisions resulted in the accidental targeting of U.S. citizens or persons located within the United States.[134] Any collection of this type is generally subject to purge.[135]

3. U.S. Person Identifiers May Be Used to Query Acquired Data

After an intelligence agency acquires data pursuant to the procedures discussed above, personnel may access the data by querying the databases in which the data is retained—both raw and minimized databases.[136] Querying is used to access data already in the government's possession more quickly and efficiently; rather than examining single, discrete

127. *See id.*

128. *See id.* at 6, 114.

129. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 6.

130. *See* PCLOB REPORT, *supra* note 7, at 116.

131. *Id.*

132. *See id.*

133. *See id.*

134. *Id.* at 44.

135. *Id.* at 6.

136. PCLOB REPORT, *supra* note 7, at 55. Queries of raw data are limited to trained personnel and are subject to stricter requirements than queries of minimized data. *Id.* at 56–57 (explaining that, for example, queries of unminimized data using U.S. person identifiers cannot be used to query MCTs and content queries using U.S. person identifiers must be pre-approved).

communications, analysts may query databases to retrieve information readily.[137] In this context, a "query" is a search of Section 702 acquired data using specific terms—such as keywords or phrases, names, email addresses, or phone numbers—to access previously collected information.[138] Such terms may be identifiers associated with U.S. persons. Agencies may use U.S. person identifiers "as the first step in evaluating and detecting potential threats to the homeland."[139] For example, the NSA may query a database with the name of a government official traveling abroad to identify threats by foreign adversaries, or the name of a U.S. citizen who is held hostage abroad to pinpoint terrorist communications indicating the location or condition of the hostage.[140]

All queries, involving U.S. persons or otherwise, must be reasonably likely to return foreign intelligence information or evidence of a crime and must be sufficiently tailored.[141] U.S. person queries are subject to additional limitations.[142] The most recent reauthorization of Section 702 requires the AG and DNI to adopt "procedures consistent with the requirements of the fourth amendment" to govern queries.[143] These procedures are subject to review by the FISC, and agencies must keep a record of U.S. person query terms used.[144] These limitations aim to reduce the probability of returning non-pertinent U.S. person information.[145]

Agencies have differing requirements for content and metadata queries. Content generally receives greater protection as it involves the substance of communications, whereas metadata, or non-content, receives lesser

137. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 6. The NSA, FBI, CIA, and NCTC each have access to databases of Section 702 data which they may query.

138. PCLOB REPORT, *supra* note 7, at 55.

139. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 6.

140. *Id.*

141. FBI MINIMIZATION PROCEDURES, *supra* note 16, at 8–9; NSA MINIMIZATION PROCEDURES, *supra* note 13, at. 4–5; Chris Inglis & Jeff Kosseff, *In Defense of FAA Section 702: An Examination of Its Justification, Operational Employment, and Legal Underpinnings* 14 (Hoover Inst. Working Grp. on Nat'l Sec., Tech., and Law, Paper No. 1604, 2016), https://www.hoover.org/sites/default/files/research/docs/ingliskosseff_defenseof702_final_v3_digital.pdf [https://perma.cc/ZK3W-ZT5U] (explaining that agencies are prohibited from using overbroad queries to conduct "fishing expeditions"). For a discussion on new FBI requirements in the 2018 reauthorization, see *infra* notes 153–160.

142. NSA MINIMIZATION PROCEDURES, *supra* note 13, at 4–5; Brunner et al., *supra* note 106.

143. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 101, 132 Stat. 3, 4–5 (2018).

144. *Id.*; *see* NSA'S IMPLEMENTATION OF FISA, *supra* note 76, at 7.

145. PCLOB REPORT, *supra* note 7, at 56.

protection as it is only the information about a communication.[146] For content queries, the NSA may use only pre-approved U.S. person identifiers (e.g., FISC-approved under traditional FISA).[147] NSA analysts may also get approval for a U.S. person identifier query by making a showing to the Office of the General Counsel that the identifier is reasonably likely to yield foreign intelligence information.[148] The NSA conducts significantly fewer content queries using U.S. person identifiers than metadata queries.[149] To ensure compliance, the NSA conducts periodic spot checks of queries.[150] NSA procedures prohibit analysts from querying any data collected upstream with known U.S. person identifiers; only communications collected via PRISM[151] may be queried using U.S. person query terms.[152]

The FAA reauthorization imposes a probable cause court order requirement for certain *content*, but not metadata, queries conducted by the FBI.[153] Essentially, the FBI must procure a court order prior to using a U.S. person identifier to query Section 702 data in connection with a "predicated criminal investigation" that is "not relate[d] to the national security of the United States."[154] Importantly, the FBI's investigation process begins with an assessment phase prior to the "predicated" stage of any investigation.[155] The requirement is silent on queries conducted in the assessment stage.[156] The court order requirement is limited to investigations and fails to address queries conducted absent an open

146. For example, metadata would include the number dialed on a telephone, email addresses from which communications are sent and received, and the time stamps indicating when emails are sent or received. For more information, see Orin Kerr, *Relative vs. Absolute Approaches to the Content/Metadata Line*, LAWFARE (Aug. 25, 2016, 4:18 PM), https://www.lawfareblog.com/relative-vs-absolute-approaches-contentmetadata-line [https://perma.cc/9EM2-8T2G].

147. NSA'S IMPLEMENTATION OF FISA, *supra* note 76, at 6–7.

148. PCLOB REPORT, *supra* note 7, at 57.

149. In 2017, the NSA conducted an estimated 7,512 content queries using terms concerning a known U.S. person and an estimated 16,924 metadata or non-content queries using U.S. person identifiers. These numbers count each query separately, even if the same identifier (e.g., the telephone number 800-222-2222) is used in multiple queries. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 63.

150. NSA'S IMPLEMENTATION OF FISA, *supra* note 76, at 7.

151. *See supra* Section I.B.2.a for an explanation of PRISM collection.

152. NSA'S IMPLEMENTATION OF FISA, *supra* note 76, at 6–7.

153. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 101, 132 Stat. 3, 4–5 (2018).

154. *Id.*

155. FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE 16 (2016).

156. PCLOB REPORT, *supra* note 7, at 57; *see* FISA Amendments Reauthorization Act § 101.

criminal investigation.[157] An exception to the requirement exists if the FBI determines that "there is a reasonable belief" that the query results "could assist in mitigating or eliminating a threat to life or serious bodily harm."[158] The DNI and the NSD conduct periodic reviews of FBI queries to ensure compliance with privacy protections.[159] The court order requirement does not apply to queries conducted by any other intelligence agency.[160]

II. THE FOURTH AMENDMENT AND ELECTRONIC SURVEILLANCE

The Fourth Amendment is the cornerstone of the privacy debate over U.S. person queries. Any agency collecting Section 702 intelligence must do so consistently with the Fourth Amendment.[161] The statute expressly mandates this constitutional compliance.[162] Any Fourth Amendment analysis concerning U.S. person queries must consider privacy risks associated with such collection together with the statutory provisions designed to mitigate such intrusions.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects" by prohibiting "unreasonable searches and seizures" by the government.[163] In the modern technological era, the Fourth Amendment has evolved from protecting only physical searches to encompassing limitations on electronic surveillance.[164] In early jurisprudence involving electronic surveillance, courts held that the Fourth Amendment did not protect intercepted telephonic communications because they are not material things that can be searched or seized—a.k.a. the trespass theory.[165] However, in *Katz v. United*

157. *See* FISA Amendments Reauthorization Act § 101.

158. *Id.*

159. PCLOB REPORT, *supra* note 7, at 59.

160. FISA Amendments Reauthorization Act § 101.

161. 50 U.S.C. § 1881a(b)(5) (2018).

162. *Id.* § 1881a(b)(5).

163. U.S. CONST. amend. IV ("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.").

164. *See* Katz v. United States, 389 U.S. 347, 351 (1967); Riley v. California, 573 U.S.__, 134 S. Ct. 2473, 2483–84 (2014) (describing the extent of privacy intrusions as much more significant when government actors have access to digital information, particularly in the modern era of technological advances).

165. *See* Olmstead v. United States, 277 U.S. 438, 465–66 (1928).

States,[166] the U.S. Supreme Court departed from *Olmstead v. United States*,[167] the foundational trespass theory case, and held that the Fourth Amendment protects "people, not places."[168] As such, the Court redefined a Fourth Amendment search as government conduct that violates a person's reasonable expectation of privacy.[169] Even so, a warrantless search may nonetheless be constitutional if it is reasonable—usually by falling within a recognized exception to the warrant requirement.[170] Some courts and numerous scholars have also recognized a general reasonableness approach to warrantless searches and seizures under the Fourth Amendment.[171] Fourth Amendment Warrant Clause jurisprudence is increasingly decided on a case-by-case basis with analyses that turn on policy considerations and imports of practicality.[172]

After *Katz*, the Court began to recognize Congress's role in regulating the acquisition of electronic evidence, and Congress has passed statutes in response.[173] In the ordinary law enforcement context, digital evidence acquisition is regulated by a variety of statutes, including the Wiretap Act

166. 389 U.S. 347 (1967). The *Katz* Court expressly declined to determine whether warrantless electronic surveillance would be permitted in national security cases. *Id.* at 358 n.32.

167. 277 U.S. 438 (1928), *overruled in part by* Berger v. State of N.Y., 388 U.S. 41 (1967) *and Katz*, 389 U.S. 347.

168. *Katz*, 389 U.S. at 351.

169. *See id.* at 361 (Harlan, J., concurring); Kyllo v. United States, 535 U.S. 27, 33 (2001) (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

170. *Katz*, 389 U.S. at 357.

171. *E.g.*, Groh v. Ramirez, 540 U.S. 551, 571–73 (2004) (Thomas, J., dissenting) ("[T]he Court has vacillated between imposing a categorical warrant requirement and applying a general reasonableness standard." *Id.* at 572); United States v. Knights, 534 U.S. 112, 118–19 (2001) (holding a warrantless search to be constitutional under a "general Fourth Amendment approach" of reasonableness); United States v. Muhtorov, 187 F. Supp. 3d 1240, 1254 (D. Colo. 2015) (finding "the special need/foreign intelligence exception argument somewhat academic and limiting, because the standard ultimately is one of reasonableness"); Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1612–13 (2012) (discussing the "collapse of the warrant requirement" and the rise of a general reasonableness approach); Nikolaus Williams, *The Supreme Court's Ahistorical Reasonableness Approach to the Fourth Amendment*, 89 N.Y.U. L. REV. 1522, 1524 (2014) ("Increasingly, the Court has abandoned its preference for warrants for . . . the reasonableness interpretation.").

172. *See* Corey M. Then, *Searches and Seizures of Americans Abroad: Re-Examining the Fourth Amendment's Warrant Clause and the Foreign Intelligence Exception Five Years After* United States v. Bin Laden, 55 DUKE L.J. 1059, 1072 ("[T]he so-called warrant requirement is clearly a misnomer in that it is not absolute and there is a laundry list of searches and seizures that either historically or currently do not require a warrant. . . ." (citations omitted)).

173. *See, e.g.*, Brian M. Kistner, The Fourth Amendment in the Digital World: Do You Have an Expectation of Privacy on the Internet? 20–21 (2016) (unpublished manuscript) (Seton Hall Univ. L. Sch. Student Scholarship, https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1830 &context=student_scholarship [https://perma.cc/73SL-9SSP]) (discussing Congressional response to *Katz* in passing the Wiretap Act/Title III).

(Title III).[174] Before a domestic criminal wiretap can occur, a warrant must be issued that indicates—with particularity—the phone line to be tapped, the conversation to be seized, and the crime under investigation.[175] Only after the government secures a warrant may it collect the target's communications, including the incidental communications of the receiving-end of the conversation.[176] In the foreign intelligence context, electronic evidence is regulated largely by traditional FISA, the FAA including Section 702, and Executive Order (EO) 12333.[177] These regulations are designed to allow surveillance and acquisition of digital evidence for proper law enforcement and intelligence purposes, but deny surveillance in unlawful circumstances. In the national security context, or at least insofar as "foreign powers or their agents" are involved, courts have expressly invited Congress to establish statutory guidelines for electronic surveillance.[178] As such, the relevant statutory provisions are critical in analyzing the reasonableness of searches in the context of electronic evidence.

Before examining whether government conduct is reasonable, courts must find that the conduct falls within the protections of the Fourth Amendment. As such, the below sections will address the following: (1) how courts define searches and seizures; (2) when conduct is defined as a search or seizure, how courts determine whether the conduct is reasonable under the Fourth Amendment; and (3) how the digital age affects Fourth Amendment jurisprudence, including case law squarely addressing Section 702 queries and other electronic surveillance.

---

174. Wiretap Act, 18 U.S.C. §§ 2510–2522 (2018) [hereinafter Title III]; *see also* Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2018); Pen-Register/Trap and Trace Statutes, 18 U.S.C. §§ 3121–3127 (2018).

175. 18 U.S.C. § 2518 (requiring a court order for a criminal wiretap); U.S. CONST. amend. IV (requiring warrants to be supported by evidence "particularly describing the place to be searched, and the persons or things to be seized").

176. 18 U.S.C. § 2518.

177. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), *amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4,075 (Jan. 23, 2003); Exec. Order No. 13,355, 69 Fed. Reg. 53,594 (Aug. 27, 2004); *and* Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (July 30, 2008).

178. United States v. United States Dist. Court (*Keith*), 407 U.S. 297, 322–23 (1972); *see also* United States v. Truong Dinh Hung, 629 F.2d 908, 914 (4th Cir. 1980) ("Perhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs.").

A. Digital Searches are Defined by Reasonableness and Government Access to Seized Data

Underlying the Fourth Amendment's reasonableness analysis are the definitions of a "search" and a "seizure." As the scope of the Fourth Amendment is limited to searches and seizures, government activity must qualify as a search or seizure to fall within the ambit of its protection.[179] Whether conduct constitutes a search for purposes of the Fourth Amendment goes directly to the reasonableness of the search—a search is defined as government action that violates an individual's reasonable expectation of privacy.[180] A seizure is generally defined as the taking of physical property or "some meaningful interference with an individual's possessory interests in that property."[181] An understanding of how searches and seizures have been interpreted in both physical and digital searches provides a framework for how Section 702 querying should be viewed under the Fourth Amendment.

Unlike physical searches, digital searches are usually conducted by copying some form of original data—whether it is an entire hard drive, a single file, a specific communication, etc.—and reviewing that data in a different location.[182] Note that in Section 702 terms, the "copying" occurs at the acquisition stage, and the review occurs when agency analysts query the respective database. Accordingly, courts have recognized distinct Fourth Amendment rules to respond to the unique privacy challenges of digital searches.[183]

In the context of digital searches, courts often consider the moment when data "is exposed to human observation"[184] to be the relevant point for determining whether a search occurred. For example, in *Kyllo v. United States*,[185] the Court found that the output of measurements emanating from a heat-sensing device constituted a search.[186] In *Kyllo*, the

---

179. U.S. CONST. amend. IV.

180. *See* Katz v. United States, 389 U.S. 347, 353 (1967).

181. United States v. Jacobsen, 466 U.S. 109, 113 (1984); *see also* Soldal v. Cook Cty., 506 U.S. 56, 68 (1992) (finding that "seizures of property are subject to Fourth Amendment scrutiny even though no search within the meaning of the Amendment has taken place").

182. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 540–41 (2005).

183. *See, e.g.*, Riley v. California, 573 U.S. __, 134 S. Ct. 2473, 2488 (2014) (analogizing the government's argument that computer searches are "materially indistinguishable" from physical searches to "saying a ride on horseback is materially indistinguishable from a flight to the moon" and concluding that digital-specific searches require specific Fourth Amendment rules).

184. Kerr, *supra* note 182, at 548.

185. 533 U.S. 27 (2001).

186. *Id.* at 35.

search occurred not when the radiation signal was emitted into the air, but when federal agents observed the contents of the home in the form of measurements from the thermal technology.[187] Notably, the *Kyllo* Court reasoned that the use of technological advances in the context of Fourth Amendment searches—specifically, the government's ability to search a person's home without notice to the occupants—violated the reasonable expectation of privacy test.[188] Similarly, in *Riley v. California*,[189] the Court used this same basic reasoning to find that a police officer may lawfully seize a person's cell phone; however, the officer must usually obtain a warrant before accessing, or searching, that phone's contents.[190] In these cases, the government "searched" the data not when it obtained information per se, but when authorities actually observed the data.[191]

The question of when a seizure occurs in the digital context, and particularly in electronic surveillance, is more doctrinally uncertain.[192] On the one hand, some courts have found that copying and control over original computer files constitutes a seizure under the Fourth Amendment.[193] In the context of Section 702, copying and control over digital evidence is akin to acquisition and retention. For example, in *United States v. Ganias*,[194] the Second Circuit concluded that the government's permanent retention of an individual's personal computer records constituted a seizure for Fourth Amendment purposes.[195] In finding that the government "overseized" non-relevant files, the court ruled that the government must delete all files not described by the warrant.[196] When considering a similar question in *United States v. Carey*,[197] the Tenth Circuit ruled that data unexposed by the initial search

187. *Id.*

188. *Id.*

189. 573 U.S. __, 134 S. Ct. 2473 (2014).

190. *Id.* at 2484–85.

191. *See* Kerr, *supra* note 182, at 548.

192. Orin Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 705–09 (2010); *see generally* Note, *Digital Duplications and the Fourth Amendment*, 129 HARV. L. REV. 1046 (2016).

193. *Compare* United States v. Ganias, 755 F.3d 125, 137 (2d Cir. 2014) (finding that copying computer data constituted a seizure), *and* United States v. Burgess, 576 F.3d 1078, 1088–89 (10th Cir. 2009) (assuming that copying a hard drive constituted a seizure), *with* United States v. Jefferson, 571 F. Supp. 2d 696, 704 (E.D. Va. 2008) (finding that FBI agents taking photographs or notes of what agents saw in defendant's home interfered with the homeowner's sole possession of such items and, thus, constituted a search under the Fourth Amendment).

194. 755 F.3d 125 (2d Cir. 2014), *aff'd on reh'g en banc*, 824 F.3d 199 (2d Cir. 2016).

195. *Id.* at 137.

196. Orin Kerr, *Executing Warrants for Digital Evidence*, 48 TEXAS TECH L. REV. 1, 9 (2015); *Ganias*, 755 F.3d at 137–40.

197. 172 F.3d 1268 (10th Cir. 1999).

was beyond the scope of the warrant.[198] In *Carey*, a law enforcement agent searching a computer for evidence of drug sales discovered evidence of child pornography and subsequently abandoned the initial search to find additional evidence of child pornography. The first discovered image was reasonable, but the proceeding findings, or nonresponsive data, exceeded the scope of the lawful search.[199] In other words, when the government shifted to seeking information for a purpose other than the initial purpose of the search, the government was required to obtain a warrant. The Second Circuit reached a similar conclusion in *ACLU v. Clapper*,[200] deciding that storing metadata in a database amounts to a seizure under the Fourth Amendment.[201]

On the other hand, some courts have found that copying data does not constitute a seizure because the original data "remain[s] intact and unaltered" and the owner may still access it.[202] As such, the reasoning goes, the copying does not interfere with the owner's possessory rights to that information. In the Fourth Amendment context, these courts find that the government did not take or seize property when it copied data.[203] Importantly, each of these opinions treats the government's control over data differently than their access to that data under the Fourth Amendment. Whether or not the courts find a seizure where data was

198. *Compare* United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (holding that a law enforcement agent exceeded the scope of a search warrant for drug sales when he "abandoned" that search to look for evidence of child pornography), *with* United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002), *vacated on other grounds*, 537 U.S. 802 (2002), *aff'd*, 359 F.3d 356, 358 (5th Cir. 2004) (holding that a comprehensive computer search did not violate the Fourth Amendment where search of a portion of the computer had been justified). Note that the Court's recent opinions indicate agreement with the former approach—treating different "files" on a single computer, or purposes of evidence collection, separately—at least in the context of aggregated digital evidence insofar as a justification to search a particular file will not likely justify a comprehensive digital search. *See* Riley v. California, 573 U.S. __, 134 S. Ct. 2473 (2014) (noting concerns about the vast amount of data contained within a cell phone); United States v. Jones, 565 U.S. 400 (2012) (sharing similar concerns).

199. *Carey*, 172 F.3d at 1273. Nonresponsive data is generally defined as information that does not directly respond to, or is outside the scope of, an initial search warrant. For more information and an argument to limit government use of such data, see generally Orin Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH. L. REV. 1 (2015).

200. 785 F.3d 787 (2d. Cir. 2015).

201. ACLU v. Clapper, 785 F.3d 787, 801 (2d. Cir. 2015).

202. United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001); *see also* Arizona v. Hicks 480 U.S. 321, 323–24 (1987) (finding that copying a serial number from a stereo system did not constitute a seizure).

203. *In re* Application of the United States of Am. for a Search Warrant for Contents of Elec. Mail, 665 F. Supp. 2d 1210, 1222 (D. Or. 2009).

copied and retained, courts distinguish between copying and retention versus the government's observation of the data.[204]

By extension, the Court has not squarely addressed when precisely a seizure occurs in electronic surveillance but tends to use the conjunctive "search and seizure" when dealing with such cases. For example, in both *Berger v. New York*[205] and *Katz*, the Court refers to surveillance as a "search and seizure."[206] More recently, the Court used the disjunctive "search or seizure" to refer to police officers putting a GPS device on an individual's vehicle and receiving location data from it.[207] The Court, however, resolved the Fourth Amendment question without distinguishing between the search and seizure.[208] This seems to be, in part, because courts simply assume the existence of both a search and seizure—or explicitly refer to one or the other without analysis when the conduct is clearly a search, for example. Thus, courts avoid the somewhat technical question—particularly in the digital realm—of when exactly searches and seizures occur.[209]

In the modern era of "big data,"[210] courts have struggled to adapt Fourth Amendment jurisprudence to the high-volume collection of digital evidence. While the current law is complicated at best, two instructive takeaways remain. First, courts distinguish between copying and retention of data on the one hand, and the government's access to that data on the

---

204. *See* Riley v. California, 573 U.S. __, 134 S. Ct. 2473, 2488 (2014); Kyllo v. United States, 533 U.S. 27 (2001); *Gorshkov*, 2001 WL 1024026, at *3.

205. 388 U.S. 41 (1967).

206. *Id.* at 54, 57; Katz v. United States, 389 U.S. 347, 353 (1967).

207. United States v. Jones, 565 U.S. 400, 402 (2012).

208. *See id.* (finding that the government's conduct was a search or seizure within the meaning of the Fourth Amendment based on the information received).

209. *See, e.g.*, *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act (*In re Directives*), 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) (referring to searches and seizures in the FISA context but deciding the constitutionality of the surveillance without delineating the two); Kerr, *supra* note 192, at 705–13 (analyzing the "seizure puzzle" created in applying seizure precedent from physical property to digital evidence).

210. Roughly speaking, "big data" is a term used to describe extremely large, complex data sets and the technological ability to collect, aggregate, and process a greater volume of that data than was possible in the past. *See* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/VE5D-82NR]; *Big Data: What It Is and Why It Matters*, SAS, https://www.sas.com/en_us/insights/big-data/what-is-big-data.html [https://perma.cc/T4B9-GH3V]. Many scholars have analyzed its implications for the Fourth Amendment and beyond. *See* Margaret Hu, *Orwell's 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1856–60 (2017) (discussing the Fourth Amendment implications of big data apart from national security); Elizabeth E. Joh, *Policing by the Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2011).

other.[211] Whether or not courts ultimately decide when and how the search and seizure occurred, they place particular restrictions on searches and seizures based on the government's exposure to and observance of digital evidence.[212] Second, how the government conducts a search is relevant to its overall reasonableness. Because the reasonableness of a search defines whether a search occurred at all, the manner of a search's execution is crucial to any Fourth Amendment analysis.

B. Limited Foreign Intelligence Surveillance is Reasonable Under the Fourth Amendment

If government conduct qualifies as a search or seizure, it falls within the protections of the Fourth Amendment.[213] Generally, a warrantless Fourth Amendment search is considered unreasonable if it does not fall within a recognized exception to the warrant requirement. Even so, the discretionary application of the warrant exceptions and the far-reaching scope of those exceptions involving foreign intelligence nearly eviscerate the warrant preference in this context.[214] In fact, some courts have expressly stated that the benchmark for determining constitutionality in intelligence cases is not the warrant requirement, but reasonableness.[215] In other cases, even when a warrantless search would ordinarily be considered unreasonable, courts have found exceptions where

---

211. *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 801 (2d Cir. 2015) (distinguishing between acquisition and retention in finding that storing data in a database constitutes a seizure); United States v. Carey, 172 F.3d 1268, 1272–74 (10th Cir. 1999) (allowing the government to seize the entire hard drive but limiting the government's subsequent access to that data).

212. *See, e.g.*, Riley v. California, 573 U.S. __, 134 S. Ct. 2473, 2484–85 (2014) (requiring a warrant for a law enforcement officer to access the contents of a cell phone, even when the officer lawfully seized the phone); Kyllo v. United States, 533 U.S. 27, 35 (2001) (finding that a search occurred not where the government used heat-sensing technology, but when they observed the data emanating from that technology).

213. *See* Katz v. United States, 389 U.S. 347, 357 (1967).

214. *See* Jennifer Buffaloe, *"Special Needs" and the Fourth Amendment: An Exception Poised to Swallow the Warrant Preference Rule*, 32 HARV. C.R.-C.L. L. REV. 529, 530–31 (1997).

215. *Keith*, 407 U.S. 297, 322–23 (1972) ("Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."); United States v. Abu-Jihaad, 630 F.3d 102, 121–22 (2d Cir. 2010) (concluding that the Fourth Amendment's warrant requirement is "flexible" in light of "different purposes and practical considerations," specifically mentioning security and intelligence (quoting United States v. Duggan, 743 F.2d 59, 72 (1984)); United States v. Muhtorov, 187 F. Supp. 3d 1240, 1254 (D. Colo. 2015) (identifying the Fourth Amendment standard as "one of reasonableness" rather than the warrant requirement and using that standard to determine the constitutionality of Section 702 collection).

governmental interests in national security or public safety are involved.[216]

All searches, even those falling within a recognized warrant exception, must be reasonable in scope and manner.[217] To determine the reasonableness of a search or a seizure, courts look to the manner or method of execution and weigh individual privacy interests against the nature of the government interest.[218] A search is considered reasonable when the government's interest in the search or seizure outweighs the interference with individual privacy.[219]

In assessing those factors, courts consider *how* the government conducts a search.[220] In the law enforcement context, courts look to the way an officer conducts a search to determine the overall reasonableness of the search. In *United States v. Ramirez*,[221] a law enforcement officer broke the defendant's garage window to enter his home to execute a search warrant.[222] The U.S. Supreme Court considered the broken window

---

216. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974); United States v. Brown, 484 F.2d 418, 425–26 (5th Cir. 1973).

217. *E.g.*, Maryland v. King, 569 U.S. 435, 448 (2013) ("Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution."); *In re Directives*, 551 F.3d 1004, 1012–15 (Foreign Int. Surv. Ct. Rev. 2008) (upholding PAA surveillance under a foreign intelligence exception but finding that "governmental action intruding on individual privacy interests must comport with the Fourth Amendment's reasonableness requirement" (citing United States v. Place, 462 U.S. 696 (1983)).

218. *E.g.*, Riley v. California, 573 U.S. __, 134 S. Ct. 2473, 2473 (2014); *King*, 569 U.S. at 448; Illinois v. Lidster, 540 U.S. 419, 427 (2004).

219. *See, e.g.*, *Riley*, 134 S. Ct. at 2478 (noting that "the Court generally determines whether to exempt a given type of search from the warrant requirement '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'" (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))); *Lidster*, 540 U.S. at 421 (holding that police searches were "reasonable, hence, constitutional" where public interests outweighed a minimal liberty interference); United States v. Jacobsen, 466 U.S. 109, 125 (1984) (finding that searches were reasonable where law enforcement interests were substantial and the interference in private property was minimal); *In re Directives*, 551 F.3d at 1012–15 (finding surveillance under the PAA reasonable because the government's interests in national security outweighed the individual privacy interests); *In re* Sealed Case, 310 F.3d 717, 742–43, 746 (Foreign Int. Surv. Ct. Rev. 2002) (deciding that FISA surveillance is reasonable because government interests in obtaining foreign intelligence information outweighed the liberty interests involved).

220. *See, e.g.*, United States v. Ramirez, 523 U.S. 65, 71 (1998) ("Excessive or unnecessary destruction of property in the course of a search may violate the Fourth Amendment, even though the entry itself is lawful and the fruits of the search are not subject to suppression."); United States v. Place, 462 U.S. 696, 709–10 (1983) (finding no search within the meaning of the Fourth Amendment where a canine sniff was "limited both in the manner in which the information [was] obtained and in the content of the information revealed").

221. 523 U.S. 65 (1998).

222. *Id.* at 65.

in deciding whether the search violated the Fourth Amendment, noting that a search may violate the Fourth Amendment if the government excessively or unnecessarily destroys property "even though the entry itself is lawful."[223] More succinctly, reasonably executing a search supports a finding that a search is reasonable under the Fourth Amendment.

In the foreign intelligence context, courts often determine the reasonableness of intelligence collection based, in part, on what happens *after* collection.[224] For example, the FISC and the FISA Court of Review (FISCR) have recognized that the reasonableness of Section 702 collection depends on the acquisition and post-collection use of the intelligence.[225] Essentially, minimization procedures that protect U.S. person information post-collection weigh in favor of the reasonableness of the entire collection program under the Fourth Amendment.[226]

In *United States v. United States District Court*,[227] better known as the *Keith* case, the Court strongly suggested, though expressly left unresolved, that foreign intelligence searches may be subject to less stringent Fourth Amendment requirements than domestic law enforcement searches.[228] Though the holding rejected a departure from the warrant requirement for domestic security surveillance, the Court solidified the distinction between foreign and domestic intelligence collection.[229] The Court indicated that, in either case, the "legitimate need of Government" may justify lessening the stringent Fourth Amendment standards.[230] Every circuit court to squarely decide the issue since has upheld warrantless surveillance for foreign intelligence purposes.[231] At least pre-FISA, the foreign intelligence exception's domestic applicability

---

223. *Id.* at 71 ("The general touchstone of reasonableness which governs Fourth Amendment analysis . . . governs the method of execution of the warrant.").

224. *See, e.g.*, [Redacted], 2011 WL 10945618, at *7–11 (Foreign Int. Surv. Ct. Rev. 2011) (determining Fourth Amendment reasonableness of FISA collection by assessing post-acquisition minimization procedures).

225. *See id.* at *11 (looking to the NSA's minimization procedures, including the retention, use, and dissemination of MCTs to determine the overall reasonableness of the program).

226. *Id.*

227. 407 U.S. 297, 316–17 (1972).

228. *Id.* at 322. For more information on the foreign intelligence exception and its use outside the pure intelligence context, see generally L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits*, 66 VAND. L. REV. 1343 (2013).

229. *Keith*, 407 U.S. at 316–17, 321–23.

230. *Id.* at 315.

231. *E.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973).

depended on whether the surveillance was done "primarily"[232] for foreign intelligence purposes and was "carefully limited to those situations in which the interests of the executive are paramount."[233] Some courts have also required the object of the surveillance to be a "foreign power, its agent or collaborators."[234] Post-FISA, the FISCR held that a distinction between a "primary" purpose and other purposes is based on a false premise and is "inherently unstable, unrealistic, and confusing,"[235] thus it declined to adopt that approach when it considered the constitutionality of electronic surveillance under traditional FISA.[236]

In this context, the warrant clause does not apply to searches abroad. Some courts hold that a foreign intelligence exception to the warrant requirement permits warrantless surveillance abroad; other courts simply say that the warrant requirement does not apply outside the United States.[237] In 2008, the FISCR held that surveillance directed against persons outside the United States for foreign intelligence purposes does not require warrants.[238] In *In re Terrorist Bombings*,[239] the Second Circuit held that foreign intelligence searches conducted abroad that involve U.S. citizens do not require warrants.[240] Generally, the foreign country's law controls for U.S. persons outside the United States and determines what is "reasonable" under the Fourth Amendment in criminal cases and EO

---

232. *Truong Dinh Hung*, 629 F.2d at 915; *see also Butenko*, 494 F.2d at 606.

233. *Truong Dinh Hung*, 629 F.2d at 915.

234. *Id.*; *see also Butenko*, 494 F.2d at 596; *Brown*, 484 F.2d at 425.

235. *In re* Sealed Case, 310 F.3d 717, 743 (Foreign Int. Surv. Ct. Rev. 2002); *see also In re Directives*, 551 F.3d 1004, 1011 (Foreign Int. Surv. Ct. Rev. 2008) (also rejecting the primary purpose distinction, finding that whether the "programmatic purpose involves some legitimate objective beyond ordinary crime control" is the appropriate consideration).

236. *In re Sealed Case*, 310 F.3d at 743.

237. *Compare In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 167 (2d Cir. 2008) (finding the Fourth Amendment's warrant requirement to be inapplicable abroad), *with In re Directives*, 551 F.3d at 1011–12 (applying the foreign intelligence exception to the Warrant Clause for searches abroad), *and* United States v. Bin Laden, 126 F. Supp. 2d 264, 274 (S.D.N.Y. 2000) (adopting the foreign intelligence exception to search Americans abroad for foreign intelligence purposes). *Cf. In re Sealed Case*, 310 F.3d at 742–46 (assuming that FISA would survive whether or not the warrant requirements were met); Reid v. Covert, 354 U.S. 1, 74 (1957) (Harlan, J., concurring) ("The proposition is, of course, not that the Constitution 'does not apply' overseas, but that there are provisions in the Constitution which do not necessarily apply in all circumstances in every foreign place.").

238. Note that the FISA Court in *In re Sealed Case* expressly indicated that it did not hold that a foreign intelligence exception exists because it presumed that the statute in question would survive regardless of whether the warrant requirement applied, but later cases acknowledged that confirming the existence of the exception is a plausible read of the FISA Court's earlier opinion. *See In re Directives*, 551 F.3d at 1012.

239. 552 F.3d 157 (2d Cir. 2008).

240. *Id.* at 167.

12333 controls foreign intelligence surveillance.[241] The U.S. Supreme Court has also found a comparable "special needs" exception when the purpose of a search exceeds routine law enforcement and a warrant requirement would materially interfere with that purpose.[242] When the Court determines that government interests are particularly imperative, it lessens the warrant preference requirement in deference to government needs.[243] The Court engages in a "totality of the circumstances" balancing test when "special needs" apply.[244] In short, warrantless surveillance in the United States or of U.S. persons located abroad for foreign intelligence purposes has been consistently upheld subject only to Fourth Amendment reasonableness requirements.

Moreover, the third-party doctrine bears on the Fourth Amendment reasonableness requirement for electronic surveillance. The doctrine establishes that an individual does not have a reasonable expectation of privacy over information voluntarily revealed to a third-party, and therefore the Fourth Amendment does not protect such information.[245] The seminal case, *Smith v. Maryland*[246] suggests that the Fourth

241. *See generally* AMOS TOH, ET AL., BRENNAN CTR. FOR JUSTICE, OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD (clarifying the scope of EO 12,333 and its relationship to FISA); *cf. In re Terrorist Bombings*, 552 F.3d at 167 (discussing lack of precedent supporting foreign searches conducted pursuant to American warrants and the inherent difficulty of extraterritorial application of warrants issued by U.S. courts); United States v. Stokes, 726 F.3d 880, 893 (7th Cir. 2013) (holding that the Warrant Clause of the Fourth Amendment does not apply extraterritorially to searches conducted by U.S. agents).

242. *See, e.g.*, Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 653 (1995) (explaining that the exception to the warrant requirement applies "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement[s] impracticable" (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)); Terry v. Ohio, 392 U.S. 1, 33–34 (1968) (upholding stop-and-frisks to protect officer safety during investigatory stops).

243. *See, e.g.*, *Acton*, 515 U.S. at 653 (upholding high school athlete drug testing and explaining the special needs doctrine); Camara v. Mun. Court, 387 U.S. 523, 533 (1967) (noting that application of the warrant requirement "depends in part upon whether the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search"); United States v. Bin Laden, 126 F. Supp. 2d 264, 274 (S.D.N.Y. 2000) ("[I]t is clear that imposition of a warrant requirement in the context of foreign intelligence searches conducted abroad would be a significant and undue burden on the Executive.").

244. In "special needs" cases, the Court occasionally upholds warrantless searches even without individualized suspicion. *See In re* Sealed Case, 310 F.3d 717, 745 (Foreign Int. Surv. Ct. Rev. 2002) (discussing the Court's special needs exception and applying it to FISA).

245. *See* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976). *But see* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (noting that the third-party doctrine is "ill suited to the digital age" and may require reexamination to address privacy concerns).

246. 442 U.S. 735 (1979).

Amendment does not protect non-content data[247] that is given to or sent via third-party providers.[248] The Sixth Circuit held in *United States v. Warshak*,[249] however, that the Fourth Amendment does protect the *contents* of emails, even when transmitted through a third party.[250] Courts have reasoned that the third-party is merely the conduit in such cases and, therefore, the user maintains a reasonable expectation of privacy in email communications.[251] The U.S. Supreme Court has raised concerns about the future of the doctrine as applied to electronic surveillance: in *United States v. Jones*,[252] two concurring opinions suggested a willingness to limit the reach of the doctrine as applied to government monitoring in the digital age.[253]

As it stands, the Fourth Amendment does not prevent the government from accessing communications, at least non-content data, voluntarily provided to a third-party without a warrant. However, the Court recently suggested that the doctrine has critical limits. In *Carpenter v. United States*,[254] the Court declined to extend the third-party doctrine to a case involving government use of cell-site records to track an individual's movements for 127 days.[255] In doing so, Chief Justice Roberts, writing for the majority, wrote: "[T]he fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[256] The decision ultimately makes applicable the protections of the Fourth Amendment where the government accesses a user's "cell phone records that provide a comprehensive chronicle of the user's past movements," at least if those records constitute seven days or more.[257] The Court, however, narrowly defined the parameters of its opinion,

247. *See supra* note 146 and accompanying text for a primer on content vs. non-content data.

248. *Smith*, 442 U.S. at 746–47.

249. 631 F.3d 266 (6th Cir. 2010).

250. *Id.* at 285–86. *But see* United States v. Mohamud, 843 F.3d 420, 442 (9th Cir. 2016) (finding only a *diminished* expectation of privacy in email communications under the third-party doctrine when a person sent communications to a third-party and did not voluntarily reveal those communications to the government).

251. *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY Doctrine 1 (2014).

252. 565 U.S. 400 (2012).

253. *Id.* at 417 (Sotomayor, J., concurring) (signaling that eliminating the third-party doctrine altogether, for both content and metadata, may be necessary in the digital age); *id.* at 427–30 (Alito, J., concurring) (recognizing the effects of modern surveillance technologies on reasonable expectations of privacy and the insufficiencies of current jurisprudence in responding to those changes).

254. 585 U.S. __, 138 S. Ct. 2206 (2018).

255. *Id.* at 2208–09.

256. *Id.* at 2217.

257. *Id.* at 2211–12.

writing that the reasoning shall not apply to collection techniques involving national security or foreign affairs.[258]

C. High-Volume, Aggregate Data Collection is Subject to Distinct Fourth Amendment Requirements

In recent years, technological advances and the expansion of governmental electronic surveillance have prompted courts to begin adapting, albeit slowly, Fourth Amendment jurisprudence to modern technology.[259] In response to concerns arising from the large volume of data available for collection with advancing technology, courts have drawn distinctions between the analog world and the digital world—specifically between information revealed piecemeal and aggregated data.[260] Most recently, the U.S. Supreme Court expressly acknowledged technology's effect on the Fourth Amendment analysis in *Riley*.[261] In *Riley*, the Court focused on the many types of information and the sensitivity of personal data contained within cell phones, concluding that a warrantless search of the devices violates the Fourth Amendment, even when it occurs during a lawful arrest.[262] Specifically, the Court noted that the government could access addresses, prescriptions, location information, and search history all from the same device; thus, the pervasiveness of the search made it unreasonable, even incident to a lawful arrest, absent an exigent circumstance.[263] Simply put, the

258. *Id.* at 2220.

259. *See id.* at 2208–09 (2018) (applying the Fourth Amendment to cell-site data used to track a person); Riley v. California, 573 U.S. __,134 S. Ct. 2473, 2477–78 (2014) (deciding how Fourth Amendment protections apply to the contents of a cell phone); United States v. Jones, 565 U.S. 400, 401 (2012) (applying the Fourth Amendment to GPS surveillance).

260. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2216–18 (analyzing Fourth Amendment concerns specifically related to cell phone location information which can be "detailed, encyclopedic, and effortlessly compiled"); *Riley*, 134 S. Ct. at 2490 (requiring heightened Fourth Amendment protections for certain cell phone searches because data on cell phones provides "detailed information about all aspects of a person's life"); *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (framing the issue in a digital search case as "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on").

261. *Riley*, 134 S. Ct. at 2484–85.

262. *Id.* While the language in Riley does suggest increased scrutiny for expansive digital searches, the holding is limited to searches incident to arrest. *Id.* The opinion expressly states that it does "not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances." *Id.* at 2489–90 n.1. Even so, the opinion is instructive for the Court's recognition that digital data capable of revealing aggregated, invasive information might trigger Fourth Amendment protections not otherwise required. *Id.* at 2478–79.

263. *Id.* at 2494.

intrusiveness of the government's conduct itself bears on whether a search is reasonable.

The Court recognized the same privacy implications in *Jones* when it considered the reasonableness of a long-term GPS surveillance.[264] While the *Jones* Court rests its conclusion on the government's physical trespass in placing a GPS device on an individual's vehicle, the concurrence addressed the privacy implications of "aggregated" data collection.[265] In her concurrence, Justice Sotomayor expressed concern with the government's ability to connect a person's "political and religious beliefs, sexual habits, and so on" by conducting long-term surveillance.[266] In sum, precedent suggests that courts afford electronic data somewhat higher protection than tangible objects, and a violation of a person's reasonable expectation of privacy occurs when the government has access to aggregated personal information. Even so, the Court has not defined how much data is too much for the government to access, and it is unclear if it would have decided these cases differently if a nexus to foreign intelligence had existed.

In the absence of a U.S. Supreme Court decision on the matter, the District Court of Colorado and the FISC have squarely weighed in on the constitutionality of queries.[267] Both courts avoided the ultimate question about what the Fourth Amendment requires by finding that queries are not searches separate from the initial collection.[268] Both courts determined that the government's query procedures must be considered in light of the reasonableness of the entire surveillance program.[269] After deciding that the queries should not be separate Fourth Amendment searches, the district court in *United States v. Muhtorov*[270] stated that evidence obtained lawfully "may be shared with similar agencies without the need for obtaining a warrant, even if sought to be used for an entirely different purpose."[271] Thus, the district court held that the queries may be conducted without warrants.[272] The FISC similarly concluded that the queries are part of a holistically reasonable Fourth Amendment analysis

264. *Jones*, 565 U.S. at 417.

265. *Id.* at 416 (Sotomayor, J., concurring).

266. *Id.*

267. *See* [Redacted] (*FISC 2015*), 2015 ODNI 20160415, at *44–45 (Foreign Int. Surv. Ct. Rev. 2015); United States v. Muhtorov, 187 F. Supp. 3d 1240, 1256 (D. Colo. 2015).

268. *See FISC 2015*, 2015 ODNI 20160415, at *44–45; *Muhtorov*, 187 F. Supp. 3d at 1256.

269. *See FISC 2015*, 2015 ODNI 20160415, at *44–45; *Muhtorov*, 187 F. Supp. 3d at 1256.

270. 187 F. Supp. 3d 1240 (D. Colo. 2015).

271. *Id.* at 1256.

272. *See id.*

because the minimization procedures of each agency are designed to limit unreasonable privacy intrusions.[273] Moreover, the FISC was not concerned that queries may be conducted to retrieve information for purposes unrelated to that of the initial collection—it suggested that this rarely happens and even searches of unrelated material may yield critical foreign intelligence information.[274] A case currently pending before the Second Circuit may also have implications for U.S. person queries.[275] The judges addressed the use of U.S. person queries quite extensively during oral arguments, but it is unclear whether the case will turn on that point because the record is ambiguous as to when, or whether, a query occurred in the context of that case.[276]

III. U.S. PERSON QUERIES ARE CONSTITUTIONAL SEARCHES

The constitutionality analysis for Section 702 U.S. person queries is two-fold. First, a court must determine whether the query is considered a search under the Fourth Amendment—or, more precisely, whether the query is: (1) part of the overall Fourth Amendment event beginning with data acquisition; (2) a separate search entirely from the surveillance; or (3) a search while the initial collection is a seizure. Second, based on the answer to the first question, the analysis turns to the Fourth Amendment requirements placed on U.S. person queries. If the queries are searches, are they nonetheless reasonable, and therefore constitutional? And, either way, whether the queries are separate searches or part of an overall singular Fourth Amendment event, what restrictions, if any, does the Fourth Amendment place on those queries? This Part argues: (1) queries are most accurately viewed as searches under the Fourth Amendment and (2) U.S. person queries are reasonable searches based on the minimization safeguards in place, the limited U.S. person information collected, and the foreign intelligence nexus of acquired data.

Current Fourth Amendment precedent is behind the curve on electronic evidence, and the relevant doctrine is complicated at best. Courts have struggled to adapt the Fourth Amendment to modern surveillance technologies and, as such, a clear answer does not exist. That said, courts

---

273. *See FISC 2015*, 2015 ODNI 20160415, at *44–45.

274. *Id.*

275. *See* Oral Argument, United States v. Hasbajrami, No. 11-CR-623 (2d Cir. 2016), https://www.lawfareblog.com/full-oral-argument-audio-united-states-v-hasbajrami [https://perma.cc/8CF3-RWX2] (oral arguments before the Second Circuit).

276. *Id.*

have consistently upheld warrantless foreign intelligence surveillance.[277] Accordingly, U.S. person queries are constitutional searches under the foreign intelligence exception to the warrant requirement. Queries are reasonable searches given the magnitude of the national security interests at stake, the piecemeal data available under Section 702 on U.S. persons, and the extensive oversight afforded post-collection to Section 702 acquired data. Even so, the Fourth Amendment requires some delineation between U.S. person queries required for foreign intelligence purposes versus criminal investigative purposes—the former constitutional, the latter risking an unreasonable seizure and generally requiring a probable cause warrant.[278] To explain why, the following sections will analyze each conclusion.

A. Querying Section 702 Databases Amounts to a Fourth Amendment "Search"

To fall within the ambit of Fourth Amendment protections, an unreasonable search or seizure must have occurred.[279] As applied to Section 702 queries, the government has argued—and at least two courts have agreed—that querying is not a separate search under the Fourth Amendment; it is an element of the overall surveillance under Section 702.[280] Essentially, the minimization procedures and substantial oversight afforded to Section 702 surveillance render the search reasonable for Fourth Amendment purposes. Rather than deal with the technicality of when and how the search occurs in electronic surveillance, prior courts have avoided the question altogether by deciding that the holistic surveillance, including querying, is reasonable and thus not violative of the Fourth Amendment.[281]

In support of these arguments, the government and the courts have analogized Section 702 querying to criminal wiretaps and traditional law

277. *Muhtorov*, 187 F. Supp. 3d at 1253–57 (upholding Section 702 surveillance under a reasonableness approach rather than a warrant exception); *In re Directives*, 551 F.3d 1004, 1008, 1012 (Foreign Int. Surv. Ct. Rev. 2008) (holding that warrantless surveillance "to obtain foreign intelligence for national security purposes . . . directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States" is constitutional); *In re* Sealed Case, 310 F.3d 717, 743 (Foreign Int. Surv. Ct. Rev. 2002); *see also FISC 2015*, 2015 ODNI 20160415, at *44–45 (permitting queries as part of a reasonable search pursuant to the foreign intelligence exception to the Fourth Amendment's warrant requirement); *supra* notes 237–244 and accompanying text.

278. *See infra* notes 339–346 and accompanying text.

279. Katz v. United States, 389 U.S. 347 (1967).

280. *See FISC 2015*, 2015 ODNI 20160415, at *44–45; *Muhtorov*, 187 F. Supp. 3d at 1256.

281. *See FISC 2015*, 2015 ODNI 20160415, at *44–45; *Muhtorov*, 187 F. Supp. 3d at 1256.

enforcement searches under the plain view doctrine. The government has argued that if the U.S. person information was already lawfully collected, then queries tailor the lawfully collected communications for more efficient access.[282] However, the distinction is a critical one that courts should clarify in the world of big data. If a query is a Fourth Amendment search, then data not yet queried retains the same Fourth Amendment protection it had before it was "copied" (or otherwise acquired).[283] In other words, the government's argument is not persuasive. The data sitting in agency databases, before it is queried, has been acquired but not observed—i.e., it has been seized but not searched.

As an initial matter, the government's likening of Section 702 queries to criminal wiretaps or traditional law enforcement searches is wholly unconvincing. Even in the digital realm, the reasonable expectation of privacy test determines whether a search occurred. Since *Katz*, searches have been defined, in part, by an individual's subjective expectation of privacy.[284] Today—notwithstanding the constitutionality of the collection itself—the U.S. government would not seriously maintain that U.S. persons do not have an expectation of privacy over the contents of their private communications, email or otherwise, even when transmitted through a third-party provider.[285] Though the Court has not expressly held that individuals have a reasonable expectation of privacy in their emails, the trajectory of the third-party doctrine and Fourth Amendment jurisprudence is highly indicative that the court will move in that direction.[286] As such, the differences between criminal wiretaps and Section 702 surveillance are troublesome for the government's arguments.

---

282. Answering Brief of Plaintiff-Appellee at 131–34, United States v. Mohamud, 843 F.3d 420 (9th Cir. 2015) (No. 14-30217) [hereinafter Mohamud Government Brief].

283. Orin S. Kerr, *The Fourth Amendment and Querying the 702 Database for Evidence of Crimes*, WASH. POST: VOLOKH CONSPIRACY (Oct. 20, 2017), https://www.washingtonpost.com/news /volokh-conspiracy/wp/2017/10/20/the-fourth-amendment-and-querying-the-702-database-for-evidence-of-crimes/ [https://perma.cc/E3X4-M2MY].

284. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967) (establishing the reasonable expectation of privacy test for Fourth Amendment searches).

285. *See* United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) (holding that contents of emails are protected, even when transmitted through a third party); Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 650–61 (2017).

286. *See, e.g.*, Carpenter v. United States, 585 U.S. __, 138 S. Ct. 2206, 2216–17 (2018) (refusing to extend the third-party doctrine to cell phone location data collected by wireless carriers); United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) (suggesting that the Court may need to reassess the third-party doctrine in the digital age); *Warshak*, 631 F.3d 266 (holding that the Fourth Amendment does protect the contents of emails, even when transmitted through a third-party).

In contrast to criminal wiretaps, Section 702 surveillance does not begin with a warrant.[287] The FISC does not approve individual targets.[288] The surveillance does not require probable cause.[289] Instead, the FISC must approve only categories of foreign intelligence, and there is no requirement that the targets of surveillance be engaged in international terrorism or criminal activity—it is enough that the government believes a person may possess information about such activity for purposes of Section 702 collection.[290] And, as distinguished Fourth Amendment scholar Orin Kerr points out, targeting is a foreign intelligence statutory concept, not a Fourth Amendment one.[291] Despite the FISC's issuance of a statutorily required order and an express prohibition of targeting U.S. persons, U.S. persons retain reasonable expectations of privacy in their private communications—particularly when the search occurs within the United States.[292] This suggests that querying the databases with U.S. person identifiers to obtain U.S. person information is subject to a more stringent analysis than the government and the courts have previously found.

In the digital world, courts have distinguished acquisition from access to determine where the Fourth Amendment's protections apply. The tendency of courts to analyze the constitutionality of a search based on the government's access to data, especially in the digital realm, suggests that

---

287. 50 U.S.C. § 1881a (2018).

288. PCLOB REPORT, *supra* note 7, at 6.

289. *Id.*

290. *See id.* at 115.

291. Orin S. Kerr, *The Surprisingly Weak Reasoning of Mohamud*, LAWFARE: FISA: 702 COLLECTION (Dec. 23, 2016, 7:30 AM), www.lawfareblog.com/surprisingly-weak-reasoning-mohamud# [https://perma.cc/PX7C-VM9Q] (arguing that there is no "targeting" doctrine in Fourth Amendment law).

292. None of this is to say that the incidental collection of U.S. person information itself is unlawful; in fact, there is good reason to think that it is not. Criminal wiretap cases are distinguishable from any surveillance conducted under Section 702. In wiretap cases, the targets at issue can be U.S. citizens and the surveillance takes place on U.S. soil. Because Section 702 collection is the surveillance of non-U.S. persons located abroad, no warrant is required for the initial surveillance to be lawful. The government cannot be expected to have prior knowledge of a target's communications with a 702 target. *See* [Redacted], 2011 WL 10945618 (Foreign Int. Surv. Ct. Rev. 2011); *In re Directives*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008); United States v. Hasbajrami, No. 11-CR-623, 2016 WL 1029500, at *17 (E.D.N.Y. 2016) (discussing the difference between Section 702 surveillance and criminal wiretaps); Mohamud Government Brief, *supra* note 282, at 102–08 (explaining that incidental collection of U.S. person information is lawful where the initial acquisition of data emanating from a non-U.S. person overseas is constitutionally permissible). The government has also argued that the incidental overhear doctrine makes legal the collection of U.S. person communications in Section 702 surveillance. Oral Argument, United States v. Hasbajrami, No. 11-CR-623 (2d Cir. 2016), https://www.lawfareblog.com/full-oral-argument-audio-united-states-v-hasbajrami [https://perma.cc/8CF3-RWX2] (oral arguments before the Second Circuit).

a search occurs, not when authorities collect it, but when it is accessed or observed by humans. For instance, government agents access data when they query Section 702 databases.[293]

That leaves two approaches for querying under the Fourth Amendment: (1) either queries and acquisition are two separate searches, or (2) the initial collection is the seizure, while querying is the search. As stated above, the approach most consistent with already-existing precedent on computer searches seems to be that querying is the search, while acquisition is the seizure. In digital evidence cases outside of the surveillance context, courts have often viewed the government's copying of computer files, hard drives, etc. as a seizure.[294] For example, in *United States v. Ganias*[295] and *United States v. Comprehensive Drug Testing*,[296] the Second and Ninth Circuits, respectively, referred to copied data as seized data.[297] Additionally, the Court referred to wiretapping as a "search and seizure" in both *Katz* and *Berger*.[298] While not conclusive, this conjunctive use suggests that the Court viewed the recording or acquisition of the data as a seizure. That said, both approaches concluding that querying amounts to a search for Fourth Amendment purposes—whether that querying and collection are both searches or that querying is the search while the collection is the seizure—are plausible under current computer search precedent.[299] For purposes of this Comment, the approach a court takes to conclude that a query is a search makes little difference. To be sure, the second approach, viewing queries as separate

---

293. *See, e.g.*, Riley v. California, 573 U.S. __, 134 S. Ct. 2473, 2473–94 (2014) (holding that a law enforcement officer's digital cell phone search violated the Fourth Amendment even though the officer lawfully seized the phone); Kyllo v. United States, 533 U.S. 27, 35 (2001) (finding that the government searched the home not when it used thermal-imaging technology but when it observed the heat emanations revealing the contents of the person's home).

294. *See* United States v. Ganias, 755 F.3d 125, 141 (2d Cir. 2014), *aff'd on reh'g en banc*, 824 F.3d 199 (2d Cir. 2016); United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1168 (9th Cir. 2010).

295. 755 F.3d 125 (2d Cir. 2014).

296. 621 F.3d 1162 (9th Cir. 2010).

297. *Comprehensive Drug Testing*, 755 F.3d at 169–71; *Ganias*, 755 F.3d at 136, 141.

298. *See* Berger v. New York, 388 U.S. 41, 53–55 (1967); Katz v. United States, 389 U.S. 347, 356–59 (1967).

299. Some courts and scholars have suggested that copying data is neither a search nor a seizure, but that interpretation would be particularly problematic in this context. If the data acquisition is neither a search nor a seizure, the government could presumably collect as much data as desired without restriction. *See Hicks*, 480 U.S. 321; Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 560–61 (2005). *But see* ORIN S. KERR, *Use Restrictions and the Future of Surveillance Law*, *in* BROOKINGS INSTITUTION: GOVERNANCE STUDIES 10 (Jeffery Rosen & Benjamin Wittes eds., 2011) (discussing the difficulty of categorizing all evidence in a collection as a seizure and imposing use restrictions).

searches from the overall collection of surveillance, is most accurate and consistent with precedent in the age of modern technology. As such, under that approach, ending the analysis by viewing the overall surveillance as reasonable or by determining that warrants are not be required for foreign searches abroad, as the FISC has done, would not be enough to satisfy the Fourth Amendment requirements.

B. U.S. Person Queries Conducted for Foreign Intelligence Purposes are Reasonable Fourth Amendment Searches

Because U.S. person queries are Fourth Amendment searches, they require an independent justification to be constitutional. It does not necessarily follow, however, that analysts must obtain a warrant prior to querying a Section 702 database. If the searches fall within an exception to the warrant requirement or are otherwise reasonable, they may nonetheless be constitutional.[300] Analyzing queries under a general reasonableness standard, rather than a warrant exception, may more closely align with the courts' trajectory of leniency in foreign intelligence cases and Section 702 particularly—albeit a more stringent analysis than courts have previously used. Following the generally prevailing Fourth Amendment standard, though, queries also fall within the foreign intelligence exception to the warrant requirement.[301] Under either approach, reasonableness will be the touchstone of the constitutionality analysis.[302] U.S. person queries of Section 702 databases conducted for foreign intelligence purposes will be reasonable given the existing safeguards, extensive oversight and regulation, and paramount governmental interests in the data. That said, intelligence analysts must only conduct U.S. person queries for foreign intelligence purposes, and queries conducted for criminal investigative purposes should require a probable cause warrant.

---

300. *See supra* notes 170–171 and accompanying text.

301. *See, e.g.*, [Redacted], 2011 WL 10945618 (Foreign Int. Surv. Ct. Rev. 2011) (searches must still be reasonable, even where an exception applies); *In re Directives*, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008) (upholding warrantless surveillance under the PAA under the foreign intelligence exception to the warrant requirement). *But see supra* note 171 for evidence of the general reasonableness approach's relevance in Fourth Amendment jurisprudence.

302. *Katz*, 389 U.S. 347, 357 (1967).

1. Minimization Procedures and Limited U.S. Person Information Make U.S. Person Queries Reasonable Searches

The ability to acquire communications is meaningless absent the ability to access and use such data. Even so, the queries must still be reasonable to satisfy the requirements of the Fourth Amendment.[303] To determine reasonableness, courts weigh the government's interests against the privacy concerns of U.S. persons.[304] U.S. person queries will be reasonable searches if, under the totality of the circumstances, the government's legitimate interests outweigh the invasion of privacy.[305] Two lines of Fourth Amendment precedent suggest that the use of U.S. person queries, at least for foreign intelligence, is reasonable government conduct: (1) minimization and traditional law enforcement cases defining the reasonableness of searches on the method of their execution, and (2) recent cases discussing high-volume digital evidence.[306] Under both approaches, queries using U.S. person identifiers constitute reasonable government action under the totality of the circumstances.

First, precedent indicates that how the government conducts a search is relevant to its overall reasonableness.[307] In the context of U.S. person queries, the method of executing a search includes minimization and targeting procedures.[308] In *Ramirez*, the Court acknowledged that a search may be unreasonable simply because an officer executes a search in an unnecessarily or excessively destructive manner, even when the search would otherwise be lawful.[309] In other words, the overall reasonableness

303. *Katz*, 389 U.S. at 357.

304. *See supra* Section II.B.

305. *Id.*

306. *See, e.g.*, Riley v. California, 573 U.S. __, 134 S. Ct. 2473, 2494–95 (2014) (requiring a warrant to access a cell phone's contents because of the content's personal and voluminous nature); United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (expressing concern over personal data that is "aggregated" by the government); United States v. Ramirez, 523 U.S. 65, 71 (1998) (determining the reasonableness of a search based on how the law enforcement officer conducted the search); *In re Directives*, 551 F.3d at 1014–15 (deciding that surveillance is reasonable based, in part, on the minimization procedures in place).

307. *See, e.g.*, *Ramirez*, 523 U.S. at 71 (finding that an unreasonable execution of a search inside a person's home violated the Fourth Amendment, even though the initial entry into the home was lawful); *In re Directives*, 551 F.3d at 1012 (applying the totality of the circumstances for Fourth Amendment reasonableness when analyzing the constitutionality of the Protect America Act (PAA)).

308. *Cf.* United States v. Mohamud, 843 F.3d 420, 443 (9th Cir. 2016) (declaring that whether the minimization procedures contained with Section 702 protect privacy interests is an important part of the reasonableness inquiry); *In re Directives*, 551 F.3d at 1013–15 (looking to the "matrix of safeguards," including targeting and minimization procedures, in determining that the PAA was reasonable under the Fourth Amendment).

309. *Ramirez*, 523 U.S. at 71.

of a search is based not only on what occurs at the outset but on the execution of the search itself. Under the same reasoning, the FISC has found Section 702 surveillance to be constitutional based in part on the minimization procedures.[310] These procedures robustly safeguard U.S. person information and significantly curtail an otherwise invasive overreach. Minimization procedures reduce the amount of U.S. person communications incidentally collected, and the government cannot target a U.S. person for Section 702 surveillance.[311] The AG and the FISC review each agency's minimization and targeting procedures for sufficiency and statutory compliance.[312]

Moreover, minimization procedures related to the queries themselves are designed to reduce the retrieval of non-pertinent U.S. person information. The AG approves querying procedures, and agencies must keep records of each U.S. person identifier used to query Section 702 databases.[313] Such oversight is designed to ensure that queries are tailored to be "reasonably likely to return foreign intelligence information."[314] Analysts are prevented from using overbroad identifiers or using U.S. person identifiers to search upstream internet communications, and, generally, they must get approval before using a U.S. person identifier to query a database.[315] Overall reasonableness requires reasonable execution of a search, and minimization procedures provide the necessary safeguards to protect U.S. person information.

Second, as a result of the safeguards in place, data retrieved from a U.S. person query will not be "aggregated" to the degree that has troubled courts in recent Fourth Amendment jurisprudence.[316] At least one scholar has argued that the aggregated nature of the data places queries within the scope of the Fourth Amendment.[317] In contrast, this Comment contends that, while the Fourth Amendment regulates queries, the piecemeal method by which the government collects U.S. person information weighs

---

310. *See FISC 2015*, 2015 ODNI 20160415, at *44–45 (Foreign Int. Surv. Ct. Rev. 2015).

311. *See supra* Section I.B.1.b.

312. *See* 50 U.S.C. § 1881a(e)(2) (2018) (requiring judicial review of agency minimization procedures); *id.* § 1881a(g)(2)(A)(i) (requiring judicial approval of targeting procedures).

313. 50 U.S.C. § 1873 (requiring the reporting of all applications submitted, orders issued, and statistics concerning terms identifying "a known United States person" used to retrieve raw data under Section 702); *id.* § 1873(b)(2)(D) (reporting requirements for the FBI).

314. NSA MINIMIZATION PROCEDURES, *supra* note 13, at 4–5.

315. CHRIS INGLIS & JEFF KOSSEFF, HOOVER INST., IN DEFENSE OF FAA SECTION 702, at 13–14 (2018); PCLOB REPORT, *supra* note 7, at 57.

316. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

317. Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 578–79 (2017).

in favor of a finding of Fourth Amendment reasonableness. In the realm of Section 702 surveillance, the numerous safeguards and procedures that protect U.S. persons' privacy and the national security interests at stake are paramount. Any information acquired about any U.S. person will necessarily be scattered—whereas, only the communications where a U.S. person is communicating with a foreign target or a U.S. person is mentioned in a foreign target's communications will be acquired and retained in Section 702 databases. At least since the FISC's ruling in 2011, the government can no longer acquire MCTs or retain MCTs already collected where U.S. person information is part of the "transaction."[318] Upon discovering that a single communication within a transaction is "not to or from a tasked selector," the entire MCT must be destroyed (and thus could no longer be retrieved via a query).[319] Accordingly, the risk of the government learning a mosaic of a person's life through Section 702 acquired data is virtually nonexistent. The data revealed by a U.S. person query will not track a U.S. person for an extended period of time, like in *Carpenter* or *Jones*, or give the government access to the entirety of a U.S. person's emails, call logs, notes, search history, and prescriptions like in *Riley*. In short, the government's intrusion by use of U.S. person queries is inherently limited.

Importantly, the government interest is also quite significant. Under a balancing test viewed in light of the totality of the circumstances, the government's interest in using U.S. person identifiers to query Section 702 databases far outweighs the marginal intrusion on privacy. Courts have defined the national security objectives of Section 702 surveillance as the "highest order of magnitude,"[320] and the NSA has described the surveillance as "irreplaceable."[321] Perhaps the most important interest is protecting against threats to the homeland—particularly by using tools like U.S. person queries. Moreover, the IC and law enforcement community have posited that hundreds of the Western recruits to terrorist organizations emanate from the United States.[322]

---

318. *See* [Redacted], 2011 WL 10947772, at *9 (Foreign Int. Surv. Ct. Rev. 2011) (requiring the NSA to limit acquisitions to communications to or from an authorized 702 target).

319. *Id*. at *10.

320. *In re Directives*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008); *see also In re* Sealed Case, 310 F.3d 717, 746 (Foreign Int. Surv. Ct. Rev. 2002).

321. Rebecca Shabad, *The Fight Brewing in Congress Over How to Reauthorize a Key Surveillance Tool*, CBS NEWS (Nov. 20, 2017), https://www.cbsnews.com/news/the-fight-brewing-in-congress-over-how-to-reauthorize-a-key-surveillance-tool/ [https://perma.cc/E9SG-TKDQ] (noting that a senior NSA analyst referred to Section 702 as the "single most important statute the NSA has").

322. Deborah S. Sills, *Strengthen Section 702: A Critical Intelligence Tool Vital to the Protection of Our Country*, 7 NAT'L SECURITY L. BRIEF 1, 2 (2016) (explaining that Section 702 is one of the

Former Director of the FBI, Christopher Wray, has explained that queries give the IC the "agility we need to stay ahead of those threats" and that any obstacles to doing so will "put the American public at greater risk."[323] Since *United States v. Truong Dinh Hung*,[324] and more recently in cases like *Keith*, courts have shown tremendous leniency when national security interests are at stake.[325] Section 702 queries are reasonable under the Fourth Amendment because the intrusion on the U.S. person's privacy is so limited and the government's interests are so paramount. Under both lines of cases discussed in this section—the cases defining the method of execution and the cases discussing the scope of digital searches—queries are reasonable under the Fourth Amendment. Thus, this Comment argues that minimization procedures effectively protect U.S. persons' personal information, and the narrow, limited nature of the government intrusion weighed against the national security interests involved renders query searches reasonable. Under a general reasonableness approach to the Fourth Amendment, this is the end of the constitutionality analysis. Under the more traditional warrant preference approach, this analysis is still necessary to render the queries reasonable, but queries must also fall within a recognized warrant exception.

2. Most U.S. Person Queries Fall Within the Foreign Intelligence Exception

U.S. person queries are constitutional as foreign intelligence searches. While the Court has not squarely recognized the existence of a foreign intelligence exception to the Warrant Clause, the Court has recognized a comparable exception where "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement

---

nation's critical tools to "anticipate and counter" terrorist threats); Peter Bergen, Albert Ford, Alyssa Sims & David Sterman, *Part II. Who are the Terrorists?*, NEW AM., https://www.newamerica.org/in-depth/terrorism-in-america/who-are-terrorists/ [https://perma.cc/5CMT-STZS] (reporting that "every jihadist who conducted a lethal attack inside the United States since 9/11 was a citizen or legal resident").

323. Christopher Wray, Dir., Fed. Bureau of Investigation, Remarks at the Heritage Foundation: Defending the Value of FISA Section 702 (Oct. 13, 2017), https://www.fbi.gov/news/speeches/defending-the-value-of-fisa-section-702 [https://perma.cc/44XN-Q4ZV].

324. 629 F.2d 908 (4th Cir. 1980).

325. *E.g.*, *Keith*, 407 U.S. 297, 322 (1972) (requiring a warrant for domestic security surveillance but recognizing the "different policy and practical considerations" for national security cases and distinguishing domestic from foreign intelligence); *Truong Dinh Hung*, 629 F.2d at 913–15 (using the *Keith* analysis to reject a uniform warrant requirement for foreign intelligence surveillance).

impracticable."[326] In foreign intelligence surveillance, as the FISCR has recognized, the government's interests are equally acute and the warrant requirement may similarly hinder the government's vital interests.[327] The Court left open the question of whether an exception to the Fourth Amendment exists permitting the government to conduct foreign intelligence surveillance in *Katz*.[328] Then, in *Keith*, the Court strongly suggested, but left unresolved, that less rigorous requirements are necessary for foreign intelligence searches in the United States.[329] Every appellate court that has addressed the issue has upheld warrantless surveillance for foreign intelligence purposes in the United States as an exception to the warrant requirement.[330]

In the case of Section 702, the initial intelligence is expressly acquired for foreign intelligence purposes and must be approved by the FISC prior to collection.[331] As such, data acquired and stored in the 702 databases are necessarily foreign intelligence related (absent abuse or mistake in targeting and minimization procedures). To be retained, data that contain information about identifiable U.S. persons must be related to foreign intelligence information or include evidence of a crime; otherwise, agencies must purge it from databases.[332] The NSA and FBI run routine post-collection checks to ensure that targets of collection remain outside the United States and are likely to continue to return foreign intelligence information.[333] Thus, the government's databases remain filled with foreign intelligence focused information. Overall, the purpose of

---

326. Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 653 (1995) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)).

327. The FISCR has analogized foreign intelligence surveillance to the Court's recognized special needs exception. *In re Directives*, 551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008) (noting 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 security interests that are at stake").

328. Katz v. United States, 389 U.S. 347, 358 n.23 (1967) ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."). Justice White's concurrence expanded on the open question: "We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable." *Id.* at 364.

329. *See Keith*, 407 U.S. at 322.

330. *See Truong Dinh Hung*, 629 F.2d at 913; 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).

331. 50 U.S.C. § 1881a (2018).

332. FBI MINIMIZATION PROCEDURES, *supra* note 16, at 22; NSA MINIMIZATION PROCEDURES, *supra* note 13, at 12–13.

333. PCLOB REPORT, *supra* note 7, at 48.

Section 702 surveillance goes well "beyond the normal need for law enforcement" in targeting foreigners abroad to protect national security.[334]

Even so, that does not necessarily mean that the queries conducted fall within the exception—currently, U.S. person queries may be conducted only for foreign intelligence purposes or evidence of a crime.[335] Since the most recent reauthorization, the FBI must obtain a court order before using U.S. person queries as part of a "predicated criminal investigation" unrelated to national security.[336] While this provision is a start, it does not go far enough to comport with the Fourth Amendment's requirements. The reauthorization only applies to the FBI, open criminal investigations at the predicated stage of the investigation, and content queries.[337]

Post-FISA, courts have rejected the idea that the "primary" purpose of a search must be foreign intelligence for the exception to apply.[338] However, in the case of Section 702 queries, the data retrieved by querying databases with U.S. person identifiers for criminal investigative purposes is likely to be exactly the type of data for which the government would ordinarily need a warrant to obtain. Moreover, whether or not the initial collection is lawful, the U.S. person communications that are incidentally obtained are not necessarily without Fourth Amendment protection—particularly where the query is considered a "search" itself.[339] Where the interests of the executive are not paramount (e.g., interests other than preserving our national security), the IC should be required to obtain warrants prior to using U.S. person identifiers to query Section 702 databases. The reauthorization provision should be extended to cover *any* use of U.S. person queries—content or metadata—by the IC for criminal investigative purposes, not solely queries at the "predicated" stage of an

---

334. *See In re Directives*, 551 F.3d 1004, 10–11 (Foreign Int. Surv. Ct. Rev. 2008) (discussing the foreign intelligence exception's applicability to FISA). *But see* Patrick Walsh, *Stepping on (or Over) the Constitution's Line: Evaluating FISA Section 702 in a World of Changing 'Reasonableness' Under the Fourth Amendment*, 18 N.Y.U. J. LEGIS. & PUB. POL'Y, 741, 789–93 (2015) (suggesting that the national security exception has narrowed in recent years and does not shield Section 702 from traditional Fourth Amendment scrutiny).

335. FBI MINIMIZATION PROCEDURES, *supra* note 16, at 8–9; NSA MINIMIZATION PROCEDURES, *supra* note 13, at 4–5; *see also supra* Section I.B.3.

336. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 101(f)(2)(A), 132 Stat. 3, 4–5 (2018) (codified at 50 U.S.C. § 1881a(f)(2)(A) (2018)).

337. *See id.*

338. *See In re Directives*, 551 F.3d at 1011; *In re* Sealed Case, 310 F.3d 717, 743 (Foreign Int. Surv. Ct. Rev. 2002).

339. *See Keith*, 407 U.S. 297, 313 (1972); Katz v. United States, 389 U.S. 347, 353 (1967); United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) ("[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." (quoting *Keith*, 407 U.S at 313).

open criminal investigation by the FBI. Moreover, the "primary" purpose language should be retained. To comport with the Fourth Amendment, U.S. person queries must be conducted only when *primarily* for foreign intelligence purposes—which would be a more rigorous requirement than the "significant purpose" test currently in place.[340]

Like computer searches that return nonresponsive data, criminal investigations of U.S. persons are not—and cannot constitutionally be—the purpose of Section 702 surveillance. In computer searches, courts often find that nonresponsive information exceeds the scope of a warrant and cannot be used as evidence in trial or to secure an additional warrant.[341] The relevant computer cases are not entirely consistent with querying—the searches are initially conducted with warrants and are concerned with the need for an additional warrant—but they are instructive. Similarly, a U.S. person query conducted primarily for criminal investigative purposes is wholly outside the scope of Section 702 surveillance, and for good reason. In other words, the government can lawfully seize the data and use it for lawfully permitted purposes, but when the government seeks to broaden its use of the seized data to pursue a criminal investigation of a U.S. person, it needs a warrant.[342] Like a criminal wiretap, accessing and using U.S. person communications as evidence of a crime requires a warrant; otherwise, the government may effectively "bootstrap away an American's right to privacy by 'targeting' the foreign end."[343]

For these reasons, U.S. person queries conducted to obtain foreign intelligence information for national security purposes are constitutional under the foreign intelligence exception and the reasonableness requirements of the Fourth Amendment. Statutory limitations address the skepticism by critics who worry that creating a foreign intelligence exception (in the context of electronic surveillance) will permit sweeping

340. *In re* Sealed Case, 310 F.3d at 743.

341. United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999) (finding that an officer's search for child pornography was beyond the scope of the initial warrant for drug sales information and required a new warrant).

342. Note, however, that I am not suggesting the inclusion of a requirement to purge nonresponsive data, under the Fourth Amendment or otherwise. There is no reason to expand the Fourth Amendment to have an element requiring the government destroy non-pertinent evidence after some period, notwithstanding the statute's own retention limitations—especially because information not thought to be useful may later amount to critical foreign intelligence information.

343. Brief of Amici Curiae ACLU and Electronic Frontier Foundation in support of Defendant-Appellant and Reversal at 17, United States v. Hasbajrami, No. 15-2684 (2d Cir. Oct. 23, 2017).

intrusion by the government under the guise of national security.[344] Minimization procedures protect U.S. person information and, at least in this arena, Congress is well-equipped to continue balancing national security concerns with privacy rights. That said, the government rarely runs queries for criminal investigative purposes that have no nexus to foreign intelligence; the FBI reported zero instances of such queries in 2017 and only one in 2016.[345] To date, the FBI has not reported any instances of the government opening a criminal investigation of a U.S. person based on an acquisition authorized under Section 702.[346] These statistics suggest that the statute itself is working as designed—to protect U.S. persons' privacy interests while allowing the government to protect our national security.

CONCLUSION

Striking a proper balance between privacy and national security is a zero-sum game. In the transition from traditional FISA to Section 702, Congress has significantly expanded foreign intelligence surveillance. This broadened authority closed the pre-9/11 intelligence gap and broke down the wall between the IC and law enforcement. However, privacy advocates strongly criticize Section 702, particularly over the use of U.S. person queries. Nevertheless, U.S. person queries are reasonable searches that fall into the foreign intelligence exception to the Fourth Amendment warrant requirement. Their reasonableness is defined by both how the queries are conducted, including minimization, and the narrow scope of U.S. person information revealed by U.S. person queries.

In struggling to adapt applicable precedent in the modern technological era, courts have acknowledged Congress's role in addressing electronic surveillance and have found that statutory limitations have been quite effective at balancing security with privacy. Value judgements and policy considerations guide Fourth Amendment decisions. In an era of increasing cyber threats, national security interests are paramount. The government's ability to efficiently and effectively access Section 702 intelligence "Saves Lives, [and] Protects the Nation and Allies."[347] Any conclusion to

344. *See supra* Section I.B for a discussion of minimization procedures that mitigate the intrusion into U.S. person privacy.

345. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, *supra* note 63.

346. *Id.*

347. CENT. SEC. SERV., NAT'L SEC. AGENCY, *"Section 702" Saves Lives, Protects the Nation and Allies* (Dec. 12, 2017), https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1627009/section-702-saves-lives-protects-the-nation-and-allies/ [https://perma.cc/L2AN-E85D].

the contrary risks returning surveillance to the pre-9/11 programs lacking the speed and agility necessary to enhance national security.