HARVARD LAW SCHOOL
NATIONAL SECURITY JOURNAL

ONLINE ARTICLE

Updating the Fourth Amendment Analysis of U.S. Person Communication Incidentally Collected Under FISA Section 702

PETER G. MACHTIGER*

Recommended Citation

Peter G. Machtiger, *Updating the Fourth Amendment Analysis of U.S. Person Communications Incidentally Collected Under FISA Section 702*, HARV. NAT'L SEC. J. ONLINE (Feb. 7, 2021), https://harvardnsj.org/wp-content/uploads/sites/13/2021/02/Machtiger_Fourth-Amendment-Under-FISA-702.pdf

* A.B., Harvard College, 2014; J.D. Candidate, New York University School of Law, Class of 2021.

CONTENTS

INTRODUCTION

Following the terrorist attacks of September 11, 2001, the United States government rallied around its national security apparatus to improve its ability to detect and prevent future acts of terrorism. As part of this mission, the Intelligence Community was asked to "identify and target plotters in some of the most remote parts of the world and to anticipate the actions of networks that, by their very nature, cannot be easily penetrated with spies or informants."[1] Improvements in surveillance technology meant that there were "fewer and fewer technical constraints" on what the government *could* do.[2] Members of all three branches of government were therefore left to wonder what the government *should* do.[3] These government actors, in thinking about the proper scope of government surveillance, have assessed many competing factors from information overload and mission creep to trust-in-government and law enforcement legitimacy.[4]

Surveillance involving U.S. persons is the most legally complicated type of surveillance because it requires a difficult balancing of competing factors. Under the Fourth Amendment, U.S. persons have rights against unreasonable government "surveillance." However, the government also has an important countervailing interest in conducting surveillance, which may implicate U.S. persons, to protect national security. Accommodating expectations of privacy and security involves identifying an equilibrium between "the interest in liberty from government restraint or interference and the interest in public safety, in recognition of the grave threat that terrorism poses to the nation's security."[5] The bounds of Executive Branch surveillance in the realm of national security are rarely litigated in open court. Due to Article III case or controversy requirements,[6] federal courts rarely review foreign intelligence surveillance programs. Such review occurs rarely outside of the Foreign Intelligence Surveillance Court (FISC),[7] which has various duties related to the oversight of intelligence surveillance programs, including the authorization of FISA surveillance orders and the review of proposed procedures for targeting non-U.S. persons reasonably believed to be located abroad.[8] The FISC is composed of federal judges appointed by the Chief Justice of the Supreme Court to address foreign intelligence oversight.[9] Occasionally, however, cases have led judges to rule on legal challenges to government surveillance programs that implicate the civil liberties of U.S. persons; such cases provide perspectives that may "challeng[e] that of the national security experts."[10] One of the most prominent examples of a government surveillance program that has been reviewed in Article III courts is "Section 702" of the Foreign Intelligence Surveillance Act (FISA) Amendments Act (FAA).[11] Most recently, a

[1] Remarks on United States Signals Intelligence and Electronic Surveillance Programs, 2014 DAILY COMP. PRES. DOC. 2 (Jan. 17, 2014), https://www.govinfo.gov/content/pkg/DCPD-201400030/pdf/DCPD-201400030.pdf [https://perma.cc/QWH4-P8P5].
[2] *Id.*
[3] *See id.*
[4] *See* STEPHEN J. SCHULHOFER, RETHINKING THE PATRIOT ACT: KEEPING AMERICA SAFE AND FREE 27 (2005).
[5] RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 31 (2006).
[6] *See* U.S. CONST. art. III, § 2, cl. 1.
[7] *See* 50 U.S.C. § 1803.
[8] *See* DAVID KRIS & J. DOUGLAS WILSON, NAT'L SECURITY INVESTIGATIONS & PROSECUTIONS § 5.2 (3d ed. 2019).
[9] *See id.* at § 5.1.
[10] POSNER, *supra* note 5, at 5.
[11] Section 702 of the FISA Amendments Act, Pub. L. No. 110-261, 122 Stat. 2436 (codified at 50 U.S.C. § 1881a); *see* United States v. Mohamud, 843 F.3d 420 (9th Cir. 2016); United States v. Mohammad, 339 F. Supp. 3d 724 (N.D. Ohio 2018); United States v. Muhtorov, 187 F. Supp. 3d 1240 (D. Colo. 2015).

Second Circuit panel in *United States v. Hasbajrami*,[12] held that the introduction by prosecutors of evidence derived from Section 702 created a "case or controversy" sufficient for review of the program in federal court.

The *Hasbajrami* court—like all previous courts to consider the issue—upheld the constitutionality, as applied, of the warrantless use of incidentally collected U.S. person communications under Section 702.[13] In doing so, the court made only one citation[14] to *Carpenter v. United States*,[15] which has been called "one of this generation's most important Fourth Amendment opinions."[16] *Hasbajrami*'s connection to *Carpenter* may not be immediately obvious, for *Carpenter* established a warrant requirement for law enforcement access to a certain amount of a person's cell site location information (CSLI).[17] However, *Carpenter* provides a window into how the Supreme Court thinks about the constitutional implications of bulk data collection. Ignoring *Carpenter* in deciding *Hasbajrami* might make sense under a narrow reading of *Carpenter*, which focuses solely on CSLI, but dicta from *Carpenter* about applying the Fourth Amendment in the era of modern technology may support a more robust constitutional analysis of incidental collection under Section 702.[18] While *Carpenter*'s dicta are non-binding, they may provide insight into how the Supreme Court might address other forms of bulk data collection, like the collection in *Hasbajrami*, in the future.

Both Executive Branch and congressional personnel have flagged the lack of a warrant requirement for incidentally collected U.S. person communication as a cause for concern. President Obama's Review Group on Intelligence and Communications Technologies recommended that "it should take either a law enforcement or FISA judicial order to query the database. . . . [T]here should at least be a judge involved before there is access to the contents of U.S. person communications."[19] One draft bill in Congress would have "[r]estrict[ed] law enforcement from using information obtained or derived from warrantless surveillance except when investigating the most serious crimes, like murder."[20] The *Hasbajrami* case provides the opportunity for the judiciary to address the issues as a matter of constitutionality.

---

[12] 945 F.3d 641 (2d Cir. 2019).
[13] *See id.* at 661.
[14] *See id.* at 672.
[15] 138 S. Ct. 2206 (2018).
[16] Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After Carpenter*, 128 YALE L.J. FORUM 943, 943 (Apr. 1, 2019), (first citing Orin S. Kerr, *Implementing Carpenter*, in THE DIGITAL FOURTH AMENDMENT (forthcoming) (manuscript at 1), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 [https://perma.cc/FTZ4-ZANU]; then citing Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 206 (2018); and then citing Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357 (2019)).
[17] Carpenter, 138 S. Ct. at 2222.
[18] *See id.* at 2214.
[19] Peter Swire & Richard Clarke, *Reform Section 702 to Maintain Fourth Amendment Principles*, LAWFARE (Oct. 19, 2017, 2:02 PM), https://www.lawfareblog.com/reform-section-702-maintain-fourth-amendment-principles [https://perma.cc/WF4Q-EYMK]; *see also* Geoffrey Stone & Michael Morrell, *The One Change We Need to Surveillance Law*, WASH. POST. (Oct. 9, 2017), https://www.washingtonpost.com/opinions/the-one-change-we-need-to-surveillance-law/2017/10/09/53a40df0-a9ea-11e7-850e-2bdd1236be5d_story.html [https://perma.cc/R6SN-4C6K] (arguing "[t]he government should no longer be permitted to search the data collected under Section 702 without a warrant when seeking information about U.S. citizens and legal permanent residents.").
[20] Charlie Savage, *Fight Brews Over Push to Shield Americans in Warrantless Surveillance*, N.Y. TIMES (May 6, 2017), https://www.nytimes.com/2017/05/06/us/politics/congress-surveillance-nsa-privacy.html [https://perma.cc/75U8-Q9NM].

This piece will proceed in two parts. Part I will describe the factual and legal background of *United States v. Hasbajrami* and explain some modern developments in Fourth Amendment doctrine, primarily from *Carpenter*, that are relevant to the issues in *Hasbajrami*. Part II will look closely at the reasoning of the *Hasbajrami* court and provide an alternative Fourth Amendment analysis of incidentally collected U.S. person communications under FISA Section 702.

I. CONTEXT FOR THIS CASE-STUDY: *UNITED STATES V. HASBAJRAMI*

A. Factual Background

In 2011, Agron Hasbajrami, a legal permanent resident located in the United States,[21] communicated via e-mail with an unidentified foreign citizen located abroad "who Hasbajrami believed was associated with a terrorist organization."[22] Over the course of those communications, Hasbajrami indicated interest in traveling to Pakistan to join the terrorist organization.[23] After intercepting these communications, the Federal Bureau of Investigation's Joint Terrorism Task Force began investigating Hasbajrami and arrested him on September 6, 2011, as he attempted to board a flight to Turkey out of New York.[24] He was charged with "attempting to provide material support to a terrorist organization, alleging that he intended to travel to the Federally Administered Tribal Area of Pakistan, where he expected to join a terrorist organization, receive training, and ultimately fight 'against U.S. forces and others in Afghanistan and Pakistan.'"[25]

Hasbajrami pleaded guilty to "attempting to provide material support to terrorists in violation of 18 U.S.C. § 2339A" and was sentenced to 180 months in prison.[26] While serving his sentence, Hasbajrami was informed by the government that some previously disclosed evidence obtained from traditional FISA surveillance was actually "derived from other collection pursuant to [Section 702]."[27] Hasbajrami withdrew his plea and moved to suppress "the fruits of all warrantless FAA surveillance," including:

> all evidence and information derived as a result of [Section 702] surveillance; all evidence and information obtained or derived from Title I and Title III FISA collection . . . [that was] itself also derived from other collection pursuant to [Section 702] . . . [and] [a]ny other evidence and information that the Government could not have obtained in this case through an independent source.[28]

The district court denied the motion to suppress, and Hasbajrami appealed that decision to the Second Circuit, leading to the opinion discussed here.

B. Legal Background

1. FISA Section 702

[21] *See* Hasbajrami, 945 F.3d at 658.
[22] *Id.* at 647.
[23] *See id.*
[24] *See id.* at 645.
[25] *Id.*
[26] *Id.*
[27] *Id.* at 648.
[28] *Id.* at 648–49.

The provision at issue here, Section 702, was not part of the original FISA in 1978. The original FISA was passed to address several concerns, including "judicial confusion over the existence, nature and scope of a foreign intelligence exception to the Fourth Amendment's warrant requirement," "Congressional concern over perceived Executive Branch abuses of such an exception," and the "need to provide the Executive Branch with an appropriate means to investigate and counter foreign intelligence threats."[29]

Section 702 was enacted as part of the FISA Amendments Act of 2008 to provide a new framework for the government to conduct foreign intelligence surveillance of "the communications of non-U.S. persons located abroad."[30] Section 702 requires the government to submit targeting, minimizing, and querying procedures that will govern the program for approval by the FISC.[31] It does not require the government to specify with particularity the "nature and location" of any surveilled facilities or to "demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power."[32] Surveillance conducted under Section 702 is jointly authorized by the Attorney General and the Director of National Intelligence and must target non-U.S. persons outside the United States to acquire foreign intelligence information.[33]

The *Hasbajrami* court looked at Section 702 surveillance as a five-step process: (1) targeting; (2) collection; (3) minimization; (4) retention and storage; and (5) dissemination and querying.[34] Overall, this process of acquiring a communication under Section 702 must be "conducted in a manner consistent with the fourth amendment to the Constitution of the United States."[35] The surveillance generally involves compelling internet service providers to secretly provide the government with the desired communications.[36]

In 2018, an estimated 164,770 targets were subject to Section 702 surveillance.[37] In previous years, the National Security Agency (NSA) estimated that it annually acquired over 250 million Internet communications pursuant to the program.[38] It is seemingly a useful program for the Intelligence Community, according to career intelligence professionals. Former Acting Director of the CIA Michael Morrell called Section 702 "one of our nation's most effective programs to protect our national security,"[39] and former FBI Director James Comey called it "essential to the safety of this country."[40]

Buy-in from the Intelligence Community, like the above statements, is a threshold condition for an intelligence program, but buy-in from the citizens it is meant to protect matters too. Buy-in from regular citizens may even matter *more*, as public trust in government is essential to our democratic system. For an intelligence program that former intelligence leaders consider

---

[29] United States v. Rosen, 447 F. Supp. 2d 538, 542–43 (E.D. Va. 2006).
[30] United States v. Mohamud, 843 F.3d at 437.
[31] *See id.*
[32] *Id.* (citing Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1144 (2013)).
[33] *See* 50 U.S.C. § 1881a(a).
[34] *See* Hasbajrami, 945 F.3d at 651–58.
[35] 50 U.S.C. § 1881a(b)(6).
[36] *See* Hasbajrami, 945 F.3d at 651 (citing 50 U.S.C. § 1881a(i)(1)(A)).
[37] *See* OFF. OF THE DIR. OF NAT'L INTEL., STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES 13 (2019), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf [https://perma.cc/8HPD-TJJ4].
[38] *See* [Case Title Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).
[39] Stone & Morrell, *supra* note 19.
[40] Savage, *supra* note 20.

effective and essential to be maintained with legitimacy and supported by Americans, it must be scrutinized carefully when it implicates the constitutional interests of U.S. persons.

2. Incidental Collection of U.S. Person Communications

"Incidental collection" occurs when a "target"—a non-U.S. person located abroad—communicates with a U.S. person and that entire communication is acquired by an intelligence agency conducting surveillance.[41] The information communicated by the U.S. person is said to be "incidentally collected."[42] As long as there are U.S. persons communicating with non-U.S. persons located abroad, the possibility of incidental collection is inevitable.[43] The inevitability is why it is important to look at how the government handles incidentally collected communications.[44]

According to investigative reporting, in one cache of communications intercepted by the NSA, only about 10% of identified accounts belonged to intended surveillance targets while about half of the incidentally collected accounts belonged to U.S. persons.[45] This high volume of incidental collection occurs because of the way internet communications are collected; for example, if a surveillance target enters an online chat room, the identities of all of the other participants and all of the chat room communications are collected, regardless of the subject matter.[46] After communications are intercepted, NSA analysts review the information to determine whether each communication involves a target and is "reasonably believed to contain foreign intelligence information or evidence of a crime."[47] Communications meeting that criteria are retained and potentially disseminated to other agencies, while communications that do not meet that criteria are destroyed unless they otherwise meet an enumerated exception.[48]

Retained communications are maintained in databases that may later be searched to display either the content of the communications or noncontent metadata. In 2018, there were an estimated 9,637 search terms "concerning a known U.S. person used to retrieve the unminimized contents of communications obtained under Section 702," and an estimated 14,374 queries "of unminimized noncontent information" obtained under Section 702 concerning known U.S. persons.[49] A U.S. person's identity may be disseminated "unminimized" —i.e., not redacted— if it is "necessary to understand the foreign intelligence information or assess its importance," meaning that the U.S.

---

[41] Hasbajrami, 945 F.3d at 654.
[42] *Id.*
[43] *See* Robert Chesney, *Unmasking: A Primer on the Issues, Rules, and Possible Reforms*, LAWFARE (Apr. 6, 2017, 1:58 PM), https://www.lawfareblog.com/unmasking-primer-issues-rules-and-possible-reforms [https://perma.cc/XDZ6-PTWR].
[44] *See id.*
[45] *See* Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST. (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html [https://perma.cc/3HSA-J9MX].
[46] *See id.*
[47] Hasbajrami, 945 F.3d at 656 (citing 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 § 3(b)(4) (2011), https://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf. [https://perma.cc/J3H3-47JJ].
[48] *See id.*
[49] OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 37, at 14–15.

person may be involved in a crime or their identity might shed light on a potential threat to "the safety of any person or organization."[50]

As part of the FISA Amendments Reauthorization Act of 2017, which occurred after the surveillance and arrest of Hasbajrami, Congress statutorily mandated that the FBI obtain a court order when seeking to access the contents of communications "retrieved pursuant to a query made using a United States person query term that was not designed to find and extract foreign intelligence information."[51] This provided a statutory limitation to querying in cases unrelated to national security, but the statute does not affect the constitutional analysis in this case.

3. Use of Incidentally Collected Communications in Criminal Prosecutions

Generally, there is no requirement to give notice to persons whose communications are incidentally collected pursuant to Section 702. Thus, courts rarely have the opportunity to provide meaningful oversight. However, the government is required by statute to give notice to the "aggrieved person" if it "intends to enter into evidence or otherwise use or disclose . . . any information obtained or derived from an electronic surveillance" in a court proceeding.[52]

Despite this requirement, no criminal defendant received notice of Section 702 surveillance until 2013, when *New York Times* reporting revealed that the Justice Department had "misrepresented" its notice policy to the Supreme Court in *Clapper v. Amnesty International*.[53] Following this revelation, the Justice Department gave notice of Section 702 surveillance in five criminal cases between October 2013 and April 2014, including in *Hasbajrami*.[54] The Justice Department has not provided any notices since making those five disclosures. This lack of notice might mean a shift in how the Justice Department interprets "derived from"; for example, as one commentator has theorized, the Justice Department might consider evidence to be "derived from" Section 702 surveillance "only when it has expressly relied on Section 702 information in a later court filing."[55] This would allow the Justice Department to evade the notice requirement even if the expressly cited evidence that is used would not have been obtained without the original Section 702 surveillance.[56]

If the Justice Department has indeed altered its interpretation of the statute to evade the notice requirement, *Hasbajrami* may be the last case in which a federal court reviews the Fourth

---

[50] Chesney, *supra* note 43 (quoting NAT'L SEC. AGENCY ET AL., UNITED STATES SIGNAL INTELLIGENCE DIRECTIVE SP0018: (U) LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES para. 7.2.c (Jan. 15, 2011), https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf [https://perma.cc/ZLY4-VMHP].

[51] Hasbajrami, 945 F.3d at 658 (citing 50 U.S.C. § 1881a(f)(2)(A)).

[52] 50 U.S.C. § 1806(c).

[53] Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance—Again?*, JUST SEC. (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again / [https://perma.cc/QY32-5T6A].

[54] *See id.*

[55] *Id.*

[56] *See id.* This interpretation of the notice requirement may be unlawful according to the reasoning of *United States v. Moalin*, 973 F.3d 977 (9th Cir. 2020), a recent case about FISA's now-expired telephony metadata program. According to the Ninth Circuit in *Moalin*, the Fourth Amendment requires notice to a criminal defendant when the prosecution intends to enter into evidence or otherwise use information obtained *or derived* from surveillance conducted under FISA or the FISA Amendments Act. 973 F.3d at 1000–01; *see also* Orin Kerr, *Did the Ninth Circuit Create a New Fourth Amendment Notice Requirement for Surveillance Practices?*, LAWFARE (Sept. 9, 2020, 7:01 AM), https://www.lawfareblog.com/did-ninth-circuit-create-new-fourth-amendment-notice-requirement-surveillance-practices [https://perma.cc/LQ2R-2QHY].

Amendment implications of the incidental collection of U.S. person communications under Section 702.

C. Modern Developments in Fourth Amendment Doctrine

Fourth Amendment doctrine has continually developed to try to address the implications of modern technology unfathomable to the Framers of the Constitution. The most recent example of this is the *Carpenter* case, which has been called "one of this generation's most important Fourth Amendment opinions" because it thoroughly analyzes how the Framers' intentions map on to the modern technological capabilities for massive data collection.[57]

The procedure at issue in *Carpenter*, by which the government could obtain historical location data collected by telecommunications companies, was authorized under the Stored Communications Act. The Supreme Court found that it was "not a permissible mechanism for accessing historical cell-site records" and held that the government was required to obtain a warrant for that information.[58] The Court made this determination by considering the following factors: the "deeply revealing nature of CSLI"; its "depth, breadth, and comprehensive reach"; and the "inescapable and automatic nature of its collection."[59] *Carpenter* could be read narrowly to apply only to the CSLI that was at issue in the case. However, the case could also plausibly be read to hold that "even if congressionally authorized, any process short of obtaining a warrant—and thus any level of suspicion less than probable cause—would be unconstitutional."[60]

It is worth examining the incidental collection of U.S. person communications under Section 702 through the lens of *Carpenter*, the Supreme Court's most recent guidance on the constitutional implications of modern data collection. The issues in each case are somewhat analogous: Section 702 surveillance is authorized by statute, like the CSLI acquisition in *Carpenter*, and allows vast quantities of historical data to be retained in databases, which is an aspect of CSLI acquisition that concerned the *Carpenter* court.[61] When the Ninth Circuit examined incidental collection under Section 702, the court called its "vast, not de minimis" volume the "most troubling aspect" of the incidental collection and noted that "[t]his quantity distinguishes § 702 collection from Title III and traditional FISA interceptions."[62]

* * *

If the Justice Department has altered its interpretation of the notice requirement for evidence derived from Section 702, then the Second Circuit cited *Carpenter* only once in what is potentially the last opportunity for a Fourth Amendment analysis of incidental collection under Section 702.[63] The following is an alternative analysis that the court could have undertaken had it fully embraced the underlying principles revealed by *Carpenter*'s dicta.

[57] Rozenshtein, *supra* note 1616, at 943.
[58] Carpenter, 138 S. Ct. at 2221.
[59] *Id.* at 2223.
[60] Rozenshtein, *supra* note 1616, at 944.
[61] *See Carpenter*, 138 S. Ct. at 2218 ("[T]he Government can now travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers . . . .").
[62] Mohamud, 843 F.3d at 440.
[63] *See* Hasbajrami, 945 F.3d at 672 (2d Cir. 2019).

II. ALTERNATIVE ANALYSIS OF UNITED STATES V. HASBAJRAMI

The court reviewed the *Hasbajrami* case as an "as-applied challenge to the constitutionality of warrantless collection and review of his communications under Section 702."[64] The court determined that "the incidental collection in this case, and the government's use of the information thus collected, was lawful," but did not conclude as to the reasonableness of any querying involved in the case and remanded to the district court for further fact-finding on that issue.[65]

In finding the use of the incidentally collected information lawful, the Second Circuit explicitly adopted a similar approach to the Ninth Circuit—first, deciding that "a warrant is not required for such collection" and, second, deciding that "the incidental collection of Hasbajrami's e-mails was reasonable."[66] The court's analysis on both of these issues seems to follow the pre-*Carpenter* reasoning of other courts, which reached those conclusions based on a combination of only partially applicable case law concerning the extraterritorial application of the Fourth Amendment and the "incidental overhear" doctrine. This seems less convincing in a post-*Carpenter* world, where the Supreme Court has indicated that judges should consider how modern technology meshes with the intentions of the founders, especially as to the warrant requirement. The *Hasbajrami* court's strongest analysis occurs in its section separately considering querying, although it is unclear why the court treats querying so much differently than collection. These issues will now be addressed in turn.

A. Warrant Requirement

The warrant requirement in criminal law derives from the Fourth Amendment's warrant clause which states "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."[67] In the ordinary criminal context, the Supreme Court has found the Fourth Amendment's warrant clause to require three elements: (1) "warrants must be issued by neutral, disinterested magistrates"; (2) "those seeking the warrant must demonstrate to the magistrate their probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense"; (3) "warrants must particularly describe the things to be seized, as well as the place to be searched."[68] The Supreme Court has found warrantless searches "per se unreasonable under the Fourth Amendment" unless they fall within "a few specifically established and well-delineated exceptions."[69] However, the Supreme Court has been reluctant to explicitly extend these same requirements to cases involving national security.[70]

---

[64] *Id.* at 660.
[65] *Id.* at 661.
[66] *Id.* at 662.
[67] U.S. CONST. amend. IV.
[68] In re Sealed Case, 310 F.3d 717, 738 (FISA Ct. Rev. 2002) (citing Dalia v. United States, 441 U.S. 238, 255 (1979)).
[69] Katz v. United States, 389 U.S. 347, 357 (1967); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) ("[I]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.").
[70] Katz, 389 U.S. at 358 n.23 ("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."); *see also Carpenter*, 138 S. Ct. at 2220 ("[O]ur opinion does not consider other collection techniques involving foreign affairs or national security.").

The *Hasbajrami* court determined that a warrant was not required in this instance for two reasons. First, the court noted that "the Fourth Amendment does not apply extraterritorially to the surveillance of persons abroad, including United States citizens."[71] Next, the court relied on the "incidental overhear" doctrine, according to which an additional warrant is not required when, "in the course of executing a warrant or engaging in other lawful search activities, [officers] come upon evidence of other criminal activity outside the scope of the warrant or the rationale justifying the search, or the participation of individuals not the subject of the initial warrant or search."[72] Neither argument is particularly convincing in the context of Section 702 incidental collection because both doctrines arose out of specific sets of facts not analogous to the facts in this case.

1. *Extraterritoriality*

Supreme Court precedent makes clear that the Fourth Amendment warrant requirement does not apply extraterritorially to searches of non-U.S. persons. However, that rule is only pertinent to the Fourth Amendment analysis of incidental collection insofar as it legitimizes the surveillance of non-U.S. person intelligence targets located outside the United States.[73]

In addition to the aforementioned traditional extraterritoriality principle from *United States v. Verdugo-Urquidez*, the *Hasbajrami* court cited Second Circuit precedent that telephone surveillance conducted extraterritorially, even of U.S. persons, does not require a warrant.[74] As the court acknowledged, Section 702 surveillance, by its nature, only occurs *within* the territory of the United States.[75] The court addressed this point by citing *Katz* for the proposition that the location of the surveillance is not important, and thus "a foreign national resident abroad, does not acquire . . . [a Fourth Amendment-protected privacy interest] by reason of the physical location of the intercepting device."[76]

Assuming this logic to be sound, this section on extraterritoriality only establishes that the Section 702 surveillance of foreign persons located outside the United States is lawful, which is relevant only because it sets up the next section on the incidental overhear doctrine. This section, on its own, does nothing to address the Fourth Amendment-protected privacy interest of Hasbajrami, who at the time of surveillance was a U.S. person located in the United States and whose communications were collected in the United States. The fact that the surveillance target did not have Fourth Amendment rights does not mean that Hasbajrami's Fourth Amendment rights correspondingly disappear.[77]

---

[71] Hasbajrami, 945 F.3d at 662.
[72] *Id.*
[73] *See id.* (citing United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)).
[74] *Id.* at 663 (citing In re Terrorist Bombings, 552 F.3d 157, 171 (2d Cir. 2008)).
[75] *See id.* at 664.
[76] *Id.* at 665. Accepting this proposition that the location of the surveillance is not important, it is not totally clear why then the U.S. citizen in *In re Terrorist Bombings* lost the protection of the warrant requirement because he was overseas. *See* 552 F.3d 157.
[77] *See* Mohamud, 843 F.3d at 441 (assuming that the defendant "had a Fourth Amendment right in the incidentally collected communications" (citing Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 313–14 (2015) ("Communicating with a person who lacks Fourth Amendment rights should not waive the rights of the person who has those rights. The Fourth Amendment should continue to fully protect the U.S. person who communicates with those lacking Fourth Amendment rights."); also citing PRIVACY & CIVIL LIBERTIES OVERSIGHT BD. ("PCLOB"), REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 94 (July 2, 2014) ("The government has acknowledged that the Fourth

2. Incidental Overhear Doctrine

The court applied the incidental overhear doctrine to its finding that the collection of the target's communications falls outside the warrant requirement and holds that the warrantless incidental collection and use of Hasbajrami's communications are similarly lawful. But, the incidental overhear doctrine does not seem exactly appropriate in the context of Section 702 collection because: (1) the source cases involve Title III wiretaps with warrants and (2) traditional wiretaps are fundamentally different than Section 702 collection in terms of the factors identified in *Carpenter*.

The *Hasbajrami* court primarily cited *United States v. Donovan*,[78] as establishing the incidental overhear doctrine, which, as the court understands it, provides that:

> law enforcement agents do not need to obtain a separate warrant to collect conversations of persons as to whom probable cause did not previously exist with individuals whose oral or wire communications are being collected through a lawful wiretap or bug, where those conversations on their face contain evidence of criminal activity.[79]

The idea underpinning the incidental overhear doctrine started prior to *Donovan* in *United States v. Kahn*.[80] In both *Kahn* and *Donovan*, defendants opposed the use of their communications collected pursuant to Title III wiretap orders because they had not been named in the orders.[81] The holding of *Kahn*, echoed in *Donovan*, was that "(1) Title III does not require that a wiretap order name every person whose conversations will be the target of interception, and (2) the Fourth Amendment's particularity requirement is satisfied by specifying the facilities to be surveilled and the conversations to be seized."[82] In other words, the warrant obtained by the government identifying the phone lines to be surveilled and subject matter to be discussed was sufficient under the Fourth Amendment to collect the defendants' communications, even though they were not specifically named.[83] These cases cannot be directly applied to Section 702 collection because they involved warrants and "[a] section 702 collection order is obviously not a warrant."[84] The *Hasbajrami* court would rebut this point by reading the incidental overhear cases only to require that the initial surveillance be "lawful" whether by "a warrant, a FISC order, or some other exception to the warrant requirement."[85] It seems like a large leap to read Fourth Amendment case law involving warrants to apply equally to a case about warrantless surveillance given the sanctity

---

Amendment rights of U.S. persons are affected when their communications are acquired under Section 702 incidentally or otherwise[.]")))).

[78] 429 U.S. 413 (1977).

[79] *Hasbajrami*, 945 F.3d at 663.

[80] United States v. Kahn, 415 U.S. 143 (1974).

[81] *See* Elizabeth Goitein, *Another Bite Out of* Katz*: Foreign Intelligence Surveillance and the "Incidental Overhear" Doctrine*, 55 AM. CRIM. L. REV. 105, 115 (2018), https://www.law.georgetown.edu/american-criminal-law-review/wp-content/uploads/sites/15/2018/04/55-1-Another-Bite-out-of-Katz-Foreign-Intelligence-Surveillance-and-the-%E2%80%9CIncidental-Overhear%E2%80%9D-Doctrine.pdf [https://perma.cc/88P7-CGZU].

[82] *Id.* at 122.

[83] *Id.*

[84] Orin Kerr, *The Surprisingly Weak Reasoning of Mohamud*, LAWFARE (Dec. 23, 2016, 7:30 AM), https://www.lawfareblog.com/surprisingly-weak-reasoning-mohamud [https://perma.cc/DN5G-EPNQ].

[85] Hasbajrami, 945 F.3d at 665.

of the warrant requirement.[86] However, it is the same leap the Ninth Circuit made in *Mohamud*. To support the proposition, both courts only cite the district court opinion from *Hasbajrami*.[87] Deriving an exception to the warrant requirement this way also seems to be a far cry from the "jealously and carefully drawn" exceptions described by the Supreme Court.[88] The Supreme Court has emphasized the Fourth Amendment importance of a "neutral and detached magistrate."[89] The surveillance in both *Donovan* and *Kahn* involved such a magistrate as part of the Title III wiretap process, while the surveillance in *Hasbajrami* did not. Thus, the link between the incidental overhear doctrine and the Section 702 collection in *Hasbajrami* is not as strong as the *Hasbajrami* court suggests.

When examined through the lens of the *Carpenter* factors — the "deeply revealing nature" of the information; its "depth, breadth, and comprehensive reach"; and the "inescapable and automatic nature of its collection"[90] — Section 702 collection also seems fundamentally different from Title III wiretaps. The *Hasbajrami* court seemed to consider this only in its analysis of querying,[91] perhaps thinking of Section 702 collection as contemporaneous in the same way as wiretaps. However, Section 702 collection appears to have much more in common with Section 702 querying than it does with Title III wiretaps in terms of its comprehensive reach and the inescapable nature of its collection. In 2018, a total of 2,937 wiretaps were reported between federal and state judges.[92] Compare that to the 164,770 Section 702 targets in the same year,[93] encompassing hundreds of millions of internet communications.[94] This amount of collection would have been unfathomable even at the time of *Donovan* and *Kahn*, let alone in the eighteenth century. As the Supreme Court reiterated in *Carpenter*: "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[95] In conducting this analysis for CSLI, Chief Justice Roberts noted:

> Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so for any extended period of time was difficult and costly and therefore rarely undertaken . . . . For that reason, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.[96]

---

[86] *See* Katz, 389 U.S. at 357 (calling searches without warrants "per se unreasonable" outside "a few specifically established and well-delineated exceptions").
[87] *See* Mohamud, 843 F.3d at 440-41 ("[W]hen surveillance is lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful.") (citing United States v. Hasbajrami, No. 11-CR-623 (JG), 2016 WL 1029500, at *9, (E.D.N.Y. Mar. 8, 2016)).
[88] Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971).
[89] Johnson v. United States, 333 U.S. 10, 14 (1948).
[90] Carpenter, 138 S. Ct. at 2223.
[91] *See* United States v. Hasbajrami, 945 F.3d at 672.
[92] *See* U.S. CTS., WIRETAP REPORT 2018, https://www.uscourts.gov/statistics-reports/wiretap-report-2018 [https://perma.cc/23W6-Q86A] (last updated Dec. 31, 2018).
[93] *See* OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 37, at 13.
[94] *See* [Case Title Redacted], 2011 WL 10945618, at *9.
[95] *Carpenter*, 138 S. Ct. at 2214 (citing Kyllo v. United States, 533 U.S. 27, 34 (2001)).
[96] *Id.* at 2217.

A similar pre-digital analogy for incidental collection under Section 702 might include having spies surveilling foreign targets overseas at an impossible scale, who are able to open every single piece of mail received by their targets, make copies, and send those copies back to the United States, potentially to prosecute U.S. persons. In this way, *Carpenter* is all about asking "whether a prior limit on government power has been lifted."[97] When comparing Section 702 collection to Title III wiretaps, the answer to that question is undoubtedly "yes," which inspires further doubt as to the appropriateness of applying cases like *Donovan* to the situation in *Hasbajrami*.

* * *

In sum, Hasbajrami, a U.S. person whose communications were intercepted within the United States without a warrant, could be criminally prosecuted based on those communications because of the combination of two doctrines that fail to amount to an enumerated exception to the warrant requirement. It is worth noting that the Second Circuit staked its entire reasoning on the combination of extraterritoriality and the incidental overhear doctrine, rather than on a foreign intelligence or national security exception to the warrant requirement. Other courts looking at incidental collection under Section 702 have also avoided relying on a foreign intelligence or national security exception.[98] Whether or not such an exception would be more convincing than the reasoning chosen here,[99] the common denominator in Fourth Amendment cases is a reasonableness analysis.

B. Reasonableness

Having determined that the warrant requirement does not apply, the *Hasbajrami* court conducted a reasonableness analysis, examining "the totality of the circumstances to balance . . . the degree to which [the government's action] intrudes upon an individual's privacy and . . . the degree to which it is needed for the promotion of legitimate government interests."[100] However, the court did not reckon with the fact that the Supreme Court considers warrantless searches of U.S. persons within the U.S. per se unreasonable under the Fourth Amendment, except for a few clearly delineated exceptions.[101]

The court began by acknowledging that Hasbajrami, as a U.S. person, has a reasonable expectation of privacy in the content of his e-mails, even when communicating with someone overseas.[102] This is in line with *Carpenter*, in which "all nine justices signed onto opinions that declare that the police need a warrant to read the content of email messages."[103]

---

[97] Orin S. Kerr, *Implementing Carpenter*, *in* THE DIGITAL FOURTH AMENDMENT (forthcoming) (manuscript at 8), https://papers.ssrn.com/abstract_id=3301257 [https://perma.cc/ARK7-JYSW].

[98] *See* Mohamud, 843 F.3d at 441 n.25 ("Because the incidental collection excepts this search from the Fourth Amendment's warrant requirement, we need not address any 'foreign intelligence exception.'"); *see also* Muhtorov, 187 F. Supp. 3d at 1253–54) ("I find the special need/foreign intelligence exception argument somewhat academic and limiting, because the standard ultimately is one of reasonableness.").

[99] *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 77, at 90 n.411 (distinguishing Section 702 from caselaw recognizing a foreign intelligence exception, but ultimately not taking a position on the existence or scope of such an exception).

[100] Hasbajrami, 945 F.3d at 666.

[101] *See Carpenter*, 138 S. Ct. at 2221 ("[I]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.").

[102] *See Hasbajrami*, 945 F.3d at 666.

[103] Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 357, 398 (Spring 2019) (citing *Carpenter*, 138 S. Ct. at 2222; *id.* at 2230 (Kennedy, J., dissenting); *id.* at 2269 (Gorsuch, J., dissenting)).

Notably, the court did not invoke the third-party doctrine to find some kind of diminished expectation of privacy, a mistake that other federal courts in other circuits looking at incidental collection under Section 702 have made.[104] Those courts that invoked the third-party doctrine have simultaneously considered e-mails to have full Fourth Amendment protections because they are like letters and no Fourth Amendment protections because of the third-party doctrine. The considerations average out to some diminished expectation of privacy in what Professor Orin Kerr calls "the Fourth Amendment as quantum physics."[105] By avoiding the third-party doctrine trap and simply acknowledging that e-mails are like letters, the reasoning of the *Hasbajrami* court maintains greater legitimacy.

The court then described the government interest in preventing "[t]he recruitment of persons inside the United States or the placement of agents here to carry out terrorist attacks" as one "of particular importance."[106] Due to their presence on U.S. soil, the U.S. person might even pose a greater immediate threat than the foreign intelligence target with whom they are communicating. However, it is also worth remembering that Section 702 surveillance does not require any showing that the target poses some threat to the United States, just that the target is a non-U.S. person located outside the United States and that "foreign intelligence information" is reasonably expected to be acquired.[107] With such a broad targeting standard, it is equally likely that the surveillance will acquire the communications of U.S. journalists, lawyers, and ordinary citizens who are in contact with non-U.S. persons overseas. These groups are certainly entitled to Fourth Amendment protections.[108]

The court found, under the totality of the circumstances, that "the incidental collection of communications between targets foreigners abroad and United States persons . . . is thus reasonable" and that dissemination of those communications to law enforcement is reasonable when the communications raise "reasonable grounds to believe that a crime is being committed or planned in the United States."[109] Other courts have come to the same conclusion.[110]

Preventing crime is certainly a legitimate government interest, but one that the Framers anticipated when they enacted the Fourth Amendment and included a warrant requirement. Even in the context of domestic security threats in which all of the suspected dangerous individuals are located on U.S. soil, the Supreme Court has emphasized that "[t]he warrant clause of the Fourth Amendment is not dead language . . . It is not an inconvenience to be somehow weighed against the claims of police efficiency."[111] It is not obvious that this calculus should change simply because one of the suspected co-conspirators is located overseas and can thus be surveilled outside of the Fourth Amendment framework.

Perhaps a more reasonable process would involve requiring a warrant for law enforcement to access the contents of incidentally collected U.S. person communications under Section 702. This could function the same way at both the collection and querying stages: if electronic communications between a U.S. person and a non-U.S. person are intercepted by intelligence

[104] *See* Mohamud, 843 F.3d at 442; Mohammad, 339 F. Supp. 3d at 752; Muhtorov, 187 F. Supp. 3d at 1255.
[105] Kerr, *supra* note 84.
[106] *Hasbajrami*, 945 F.3d at 666–67.
[107] 50 U.S.C. § 1881a(a).
[108] United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 314 (1972) ("Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs.").
[109] *Hasbajrami*, 945 F.3d at 667.
[110] *See* United States v. Mohamud, 843 F.3d 420, 443 (9th Cir. 2016); Mohammad, 339 F. Supp. 3d at 753.
[111] *Keith*, 407 U.S. at 315.

professionals and contain evidence of a potential crime, the intelligence professionals could disseminate only the identity of the U.S. person to law enforcement. Law enforcement officials would then need to make a probable cause showing to a judge and obtain a warrant to access the contents of the communications. A judicial determination that this is a constitutional requirement—rather than relying on a statutory fix—would follow in the footsteps of *Carpenter* and provide greater respect for the Fourth Amendment interests of U.S. persons, without unduly burdening the government's law enforcement interest.

C. Querying

The *Hasbajrami* court considered the querying of previously collected Section 702 analysis separately, which is something other courts have not done.[112] In doing so, the court expressed some concern about the breadth, comprehensive reach, and automatic nature of Section 702, noting that "the program begins to look more like a dragnet, and a query more like a general warrant."[113] The court remanded to the district court for more fact-finding on the issue of querying, but seemed to seriously consider that querying should receive greater Fourth Amendment protection than it currently does.[114]

The court is right to suspect that querying needs greater Fourth Amendment protection, but it should also apply this logic to the collection stage of Section 702. The communications being queried are the same communications being reviewed at the collection stage and the broad, comprehensive, and automatic nature of the acquisition should be considered throughout.[115] In short, the court seemed to identify a meaningful gap between the nature of querying and collection where it should not.

* * *

While the court's reasoning related to the warrant requirement is unconvincing, there are seeds for hope in the section of the opinion about querying. If the full Second Circuit eventually takes this case en banc, other members of the court might pick up the concerns in the section on querying and decide to apply the logic of that section to the entire collection process, similar to the analysis laid out in this piece. Requiring a warrant before law enforcement can access the contents of incidentally collected U.S. person communications for the purposes of criminal investigation would provide the most reasonable framework under the Fourth Amendment.

CONCLUSION

Hasbajrami provides an opportunity for the judiciary to undertake a constitutional review of incidental collection under Section 702, potentially for the last time.[116] By re-hashing arguments made by other courts writing about incidental collection before *Carpenter*, the Second Circuit fails to reckon with the privacy-protective guidance from the Supreme Court in *Carpenter*. In doing so,

[112] *See* Muhtorov, 187 F. Supp. 3d at 1256; *see also* United States v. Mohamud, No. 3:10-cr-475-KI-1, 2014 WL 2866749, at *26 (D. Or. June 24, 2014).
[113] *Hasbajrami*, 945 F.3d at 670–71.
[114] *See id.* at 672.
[115] *See id.* at 669–73 (comparing querying to collection and citing the Carpenter factors).
[116] *See* Toomey, *supra* note 53.

the court not only allows the government to access U.S. person communications without a warrant in this instance, but also signals to the Executive Branch that the judiciary will not stand in the way of mass surveillance programs as long as they are conducted in the name of national security. "Courts regularly deal with the most difficult issues of our society"[117]—this is undoubtedly a difficult issue, but a thorough and convincing analysis is necessary to maintain the legitimacy of both the program and the courts. As *Hasbajrami* continues to make its way through the federal courts, judges have an opportunity to engage in an analysis that protects the Fourth Amendment rights of U.S. persons in a world of increasing data collection and surveillance. A judicial decision protecting U.S. persons from warrantless surveillance would send a strong signal to an Executive Branch seeking to push the boundaries of intelligence surveillance of U.S. persons.[118]

[117] U.S. Dist. Court (*Keith*), 407 U.S. at 320.

[118] *See* Steve Vladeck & Benjamin Wittes, *DHS Authorizes Domestic Surveillance to Protect Statues and Monuments*, LAWFARE (July 20, 2020), https://www.lawfareblog.com/dhs-authorizes-domestic-surveillance-protect-statues-and-monuments [https://perma.cc/AYH3-USPT].