ANOTHER BITE OUT OF *KATZ*: FOREIGN INTELLIGENCE SURVEILLANCE AND THE "INCIDENTAL OVERHEAR" DOCTRINE

Elizabeth Goitein*

INTRODUCTION

Although the "reasonable expectation of privacy" test set forth in *Katz* represented a historic expansion of the Fourth Amendment's right to privacy, it has few defenders among privacy scholars today. It is vulnerable to critique on a number of fronts: it is circular and gives courts little guidance;[1] it is not able to keep up with technology, given the lag time between the hardening of expectations and judicial review;[2] its two prongs require a subjective assessment that is easily gamed,[3] combined with an empirical analysis that courts are not well-positioned to undertake;[4] and so on.

Perhaps the most visible critique relates to one of *Katz*'s offshoots: the so-called "third-party doctrine," under which courts have held that a person loses any

---

* Co-Director, Liberty and National Security Program, Brennan Center for Justice at New York University School of Law. This article benefited greatly from conversations with Orin Kerr, Rachel Levinson-Waldman, and Patrick Toomey, and from Erica Posey's diligent research assistance.

1. *See, e.g.*, JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 60 (2000) ("Harlan's test was applauded as a victory for privacy, but it soon became clear that it was entirely circular."); Michael Abramowicz, *Constitutional Circularity*, 49 UCLA L. REV. 1, 60–61 (2001) ("Fourth Amendment doctrine, moreover, is circular, for someone can have a reasonable expectation of privacy in an area if and only if the Court has held that a search in that area would be unreasonable."); Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 ("[I]t is circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is.").

2. *See, e.g.*, Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 550–52 (2017); *see also* United States v. Jones, 565 U.S. 400, 427–31 (2012) (Alito, J., concurring) (noting that "in circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative" in part because Congress can better gauge shifting public opinion).

3. *See* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 507 (2001) (noting that "it is generally difficult to contest a defendant's claim to a subjective expectation of privacy"); *see also* Hudson v. Palmer, 468 U.S. 517, 525 n.7 (1984) ("[C]onstitutional rights are generally not defined by the subjective intent of those asserting the rights. The problems inherent in such a standard are self-evident.").

4. *See, e.g.*, ROBERT M. BLOOM, SEARCHES, SEIZURES, AND WARRANTS: A REFERENCE GUIDE TO THE UNITED STATES CONSTITUTION 46 (2003) ("How do we know what society is prepared to accept as reasonable? Because there is no straightforward answer to this question, 'reasonable' has largely come to mean what a majority of the Supreme Court Justices says is reasonable . . . ."); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1522 (2010) ("The Court rarely takes any steps to determine what society deems reasonable. Clearly, the justices have no special ability to sense the collective desires and values of all citizens of the United States. They instead are just stating their own preferences and opinions, whether they are consistent with society's or not.").

reasonable expectation of privacy in information voluntarily disclosed to a third party.[5] Critics argue that this doctrine falsely equates privacy—which encompasses, or should encompass, the limited disclosure of information to trusted associates of one's choosing—with secrecy.[6] They note that it is particularly untenable in an era in which we must routinely disclose communications, as well as information about those communications (known as "metadata"), to Internet service providers, mobile phone companies, and other intermediaries.[7]

The third-party doctrine is indeed deeply flawed and in need of rethinking. That rethinking, however, is well underway. Both on the legislative front and in the courts, an overhaul of the doctrine—one that, at a minimum, recognizes privacy in the content of electronic communications, if not the metadata—appears inevitable, even if it is coming decades later than it should have.[8] On the other hand, there is an area in which both legislative policy and the Fourth Amendment case law are moving in the direction of providing *less* protection for the privacy of electronic communications: foreign intelligence surveillance.

Part I of this article presents the factual background for this legal development. Mass warrantless surveillance of foreign targets' communications with Americans is a relatively recent phenomenon, stemming from changes in statutory law and technology. In particular, the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act), which created Section 702 of FISA, eliminated the requirement that the government obtain an individualized court order when wiretapping communications between foreign targets and Americans from inside the United States.[9] At the same time, technological advances have eroded practical constraints on collection, storage, and analysis.[10]

Part II of the article surveys the case law on the constitutionality of surveillance undertaken pursuant to Section 702. Until recently, only the Foreign Intelligence Surveillance Court ("FISA Court") was able to review the law's constitutionality because the Department of Justice failed to notify criminal defendants when using evidence derived from Section 702 surveillance. The Department changed its notification policy in 2013, however, and since then, federal courts in three circuits have had the opportunity to weigh in on the issue.[11] All of them concluded that the challenged surveillance was lawful.[12] Most based their rulings, in part, on a line of decades-old cases holding that a warrant to wiretap telephone calls need not name

---

5. *See* Smith v. Maryland, 442 U.S. 735, 743–45 (1979); United States v. Miller, 425 U.S. 435, 442–43 (1976).
6. *See infra* Part III.A.
7. *See id.*
8. *See id.*
9. *See infra* Part I.
10. *See id.*
11. *See* Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance—Again?*, JUST SEC. (Dec. 11, 2015 9:01 AM), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again.
12. *See infra* Part II.A–C.

every person whose communications will be intercepted.[13] From these cases, the courts derived the so-called "incidental overhear" rule: Those in contact with a surveillance target can claim no greater rights or protections than the target herself.[14] Because the targets of surveillance under Section 702 are foreigners without Fourth Amendment rights, the courts concluded that no warrant is required to obtain the communications of Americans in contact with them.

Part III critiques these decisions. It starts with the basic premise that the government must obtain a warrant to invade an American's reasonable expectation of privacy, unless the search falls within an established exception to the warrant requirement. It then posits that Americans have a reasonable expectation of privacy in their communications with foreigners overseas—a proposition that the courts reviewing the constitutionality of Section 702 surveillance appeared to accept. Finally, Part III examines the "incidental overhear" cases and demonstrates that they did not establish an exception to the warrant requirement. Instead, they held that a warrant need specify only the phone line to be tapped and the conversations to be seized. Communications that meet these specifications fall *within the warrant*—not within an exception to the warrant requirement—and may be seized, even if the communicants are not named targets. By misunderstanding and misapplying this case law, the recent decisions on Section 702 surveillance threaten to take an enormous bite out of the constitutional protection for private communications recognized in *Katz*.

I. BACKGROUND: THE ADVENT OF MASS FOREIGN INTELLIGENCE SURVEILLANCE

In past decades, there were significant legal and technological constraints on the collection of Americans' communications with foreign targets for the purpose of obtaining foreign intelligence. The primary legal constraint was the Foreign Intelligence Surveillance Act of 1978 (FISA).[15] Under this law, if the government wished to wiretap communications between foreigners and Americans from inside the United States, it had to show probable cause to the FISA Court that the target was a "foreign power" or an "agent of a foreign power."[16] While FISA defines these terms broadly,[17] they still encompass only a small fraction of foreigners overseas (and an even smaller fraction of Americans), and their application was

---

13. *See* United States v. Kahn, 415 U.S. 143, 150–55 (1974); United States v. Donovan, 429 U.S. 413, 423–28 (1977).

14. *See* United States v. Mohamud, 843 F.3d 420, 439–41 (9th Cir. 2016); United States v. Hasbajrami, No. 11-CR-623 (JG), 2016 WL 1029500, at *8–9, (E.D.N.Y. Mar. 8, 2016); United States v. Mohamud, No. 3:10–CR-00475–KI-1, 2014 WL 2866749, at *15, (D. Or. June 24, 2014).

15. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 [hereinafter Foreign Intelligence Surveillance Act of 1978] (codified in scattered sections of 8, 18, 47, 50 of the United States Code).

16. 50 U.S.C. § 1805(a)(2)(A) (2012).

17. *See id.* § 1801(a)–(b). The definition of "agent of a foreign power," however, is narrower when applied to U.S. persons, and all of the qualifying activities in the narrower definition involve illegal conduct. *Id.* § 1801(b)(2).

subject to case-by-case judicial review.[18]

The substantive and procedural limits set forth in FISA did not apply when the government engaged in overseas wiretapping of communications between foreigners and Americans, unless the government was intentionally targeting a particular, known American.[19] Overseas surveillance is generally not subject to judicial review[20] and is governed almost entirely by Executive Order 12333, which prohibits intentional targeting of U.S. persons but otherwise imposes few restrictions on collection.[21] Nonetheless, until at least the waning years of the 20th century, the limits of technology served as a practical barrier to mass surveillance.[22] International communication was difficult and expensive[23] and, therefore, relatively rare.[24] In addition, the technological constraints on acquisition, storage, and analytical capabilities rendered mass or indiscriminate surveillance unworkable, forcing a more targeted approach.

The world today looks entirely different. Advances in communications technology have made international communication easy and inexpensive, and globalization has made it necessary.[25] The result is an explosion in international communication. The FCC reported 84.7 billion minutes spent on international telephone calls by Americans in 2014[26]—an average of nearly four and a half hours per person,[27] not including minutes spent on Internet-based video and voice communications systems like Skype. Worldwide, over 205 billion emails were sent daily in

---

18. *See id.* § 1805(a).

19. Whether an electronic communication is subject to FISA depends on a combination of the method of transmission and the location of the communicants and/or the acquisition. These requirements are set forth in the statutory definition of "electronic surveillance." *See id.* §1801(f).

20. In 2008, Congress added a provision to FISA that requires individualized FISA Court orders when the government targets American citizens or residents who are outside the United States. *See id.* §§ 1881b & 1881c.

21. Exec. Order No. 12,333, 3 C.F.R.§ 200 (1981), *reprinted as amended in* 50 U.S.C. app. § 401 (2008).

22. A version of this discussion appears in ELIZABETH GOITEIN & FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, WHAT WENT WRONG WITH THE FISA COURT 19–21 (2015), https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf.

23. *See, e.g.*, JEAN-YVES HUWART & LOIC VERDIER, ORG. FOR ECON. CO-OPERATION AND DEV., ECONOMIC GLOBALISATION: ORIGINS AND CONSEQUENCES 35–36 (2013) (noting that "[i]n 1930, a three-minute telephone call between New York and London cost USD 250. In the 2000s, it is less than 23 cents").

24. In 1980, the average American spent about twelve minutes a year on international calls, compared with four and a half hours in 2014. *Compare* LINDA BLAKE & JIM LANDE, INDUS. ANALYSIS DIV., FED. COMMC'NS COMM'N, TRENDS IN THE U.S. INTERNATIONAL TELECOMMUNICATIONS INDUSTRY tbl. 4 (1998) (showing 2.7 billion total international call minutes in the U.S. in 1980) *with* STACEY ASHTON & LINDA BLAKE, TELECOMMC'NS AND ANALYSIS DIV., FED. COMMC'NS COMM'N, 2014 INTERNATIONAL TELECOMMUNICATIONS TRAFFIC AND REVENUE DATA 1 (2016), https://web.archive.org/web/20160703134329/http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0701/DOC-340121A1.pdf (showing 84.7 billion total international call minutes in the U.S. in 2014).

25. *See* GOITEIN & PATEL, *supra* note 22, at 20 (noting that the percentage of foreign-born individuals in the U.S. population today has doubled since FISA was enacted, while the number of Americans living abroad is four times higher. Similarly, the number of Americans traveling and studying abroad each year has increased several fold in recent decades).

26. ASHTON & BLAKE, *supra* note 24, at 1.

27. This number was derived by dividing the number of minutes reported by the FCC, *see supra* note 24, by the population of the United States in 2014, which was 318.7 million. *See* SANDRA L. COLBY & JENNIFER M. ORTMAN,

2015.[28] Moreover, the limits on the government's technological capability to acquire, store, and process these communications have become negligible. Under one program code-named "MYSTIC," for instance, the NSA reportedly collects *all* of the phone calls that transit into and out of certain countries and stores them for a 30-day period to permit querying.[29]

In the midst of this technological revolution, Congress dramatically weakened the legal protections afforded by FISA. Under Section 702 of FISA, created by the FISA Amendments Act of 2008[30] (which replaced the similar Protect America Act of 2007[31]), the government is no longer required to obtain individualized authorization from the FISA Court when conducting domestic wiretapping of foreign targets' communications with Americans.[32] Moreover, there is no requirement that the target be a foreign power or agent of a foreign power. The government may target any foreigner overseas and obtain all of that person's communications, as long as a significant purpose of the surveillance is to acquire foreign intelligence.[33]

These changes have enabled mass surveillance of communications between foreigners and Americans. The exact number of such communications acquired is unknown, but a 2011 FISA Court opinion noted that the government obtains 250 million Internet communications each year based on domestic foreign intelligence surveillance alone.[34] Given the prevalence of international communication, this intake could well include of Americans' communications; that number could be even higher in the context of overseas surveillance, which is subject to fewer legal constraints.

This state of affairs begs a constitutional question that ordinary federal courts are just beginning to grapple with: what protections does the Fourth Amendment afford to Americans whose communications with foreign targets are "incidentally" swept up in the millions?

II. RECENT COURT DECISIONS ON FISA SECTION 702 SURVEILLANCE

Foreign intelligence surveillance under Executive Order 12333 is not subject to judicial review, and until 2013, only the FISA Court was able to review surveil-

---

U.S. CENSUS BUREAU, P25-1143, PROJECTIONS OF THE SIZE AND COMPOSITION OF THE U.S. POPULATION: 2014 TO 2060 (2015); https://www.census.gov/content/dam/Census/library/publications/2015/demo/p25-1143.pdf.

28. THE RADICATI GRP., EMAIL MARKET, 2015-2019 4 tbl. 2 (2015), http://www.radicati.com/wp/wp-content/uploads/2015/07/Email-Market-2015-2019-Executive-Summary.pdf.

29. Ryan Devereaux et al., *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, INTERCEPT (May 19, 2014, 12:37 PM), https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/; *see also* Bob Sorokanich, *Report: The NSA Is Recording Nearly Every Call Made in Afghanistan*, GIZMODO (May 23, 2014, 10:06 AM), http://gizmodo.com/report-nsa-is-recording-every-call-in-the-bahamas-incl-1578572197/1580608721.

30. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2435 (2008) at § 101(a)(2) (codified as amended at 50 U.S.C. § 1881a).

31. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007) (expired 2008).

32. 50 U.S.C. § 1881a (2012).

33. *Id.*

34. [REDACTED], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).

lance under FISA Section 702.[35] Regular courts were denied any role because the government shirked its statutory duty to notify criminal defendants when using evidence obtained or derived from Section 702 surveillance.[36] After the Justice Department changed its notification policies in 2013, however, defendants were able to raise challenges.[37] As a result, courts in three circuits have now examined Section 702 surveillance.[38]

In all three cases, the government either acknowledged or assumed that Americans have privacy interests in their communications with foreigners overseas. It presented two arguments for why warrants were nonetheless unnecessary. First, it argued that the Fourth Amendment does not protect foreigners overseas, and therefore no warrant is required to collect their communications—even if the Americans with whom they communicate are thereby "incidentally" subject to surveillance.[39] Alternatively, the government argued that the communications are covered by the "foreign intelligence exception" to the warrant requirement,[40] as that exception has been interpreted and applied by the FISA Court.[41]

---

35. *See* Toomey, *supra* note 11.

36. *See id.* ("From 2008 to 2013, DOJ did not give a single criminal defendant notice of Section 702 surveillance—even though Congress expressly required notice when it authorized the warrantless surveillance of Americans' communications.").

37. *See id.* ("DOJ then resolved to change its notice policy. According to then-Attorney General Eric Holder, DOJ undertook a review of prosecutions in an effort to identify those where notice should have been given all along. Between October 2013 and April 2014, a total of five defendants received notice of Section 702 surveillance.").

38. *See* United States v. Mohamud, 843 F.3d 420, 437–44 (9th Cir. 2016) (reviewing the use of evidence collected pursuant to Section 702); United States v. Hasbajrami, No. 11-CR-623 (JG), 2016 WL 1029500, at *3–14 (E.D.N.Y. Mar. 8, 2016) (same); United States v. Muhtorov, 187 F. Supp. 3d 1240, 1250–58 (D. Colo. 2015) (same); United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *7–26 (D. Or. June 24, 2014) (same).

39. *See, e.g.*, Answering Brief of Plaintiff-Appellee, *Mohamud*, 843 F.3d 420 (9th Cir. 2016) (No. 14-30217), 2015 WL 8988426, at *100–08 [hereinafter *Mohamud* Appellee Answering Brief]; Government's Memorandum in Support of Its Motion for an *Ex Parte*, *in Camera* Review to Determine the Legality of Collection Pursuant to the Foreign Intelligence Surveillance Act and in Opposition to Defendant's Motions to Suppress Evidence Obtained or Derived from Section 702 of the FISA Amendments Act and to Compel Discovery of FISA Applications, Orders and Related Materials and Materials Related to the Section 702 Collection at 37–43, *Hasbajrami*, No. 11-CR-623 (JG), 2014 WL 12682145 (E.D.N.Y, Dec. 23, 2014) [hereinafter *Hasbajrami* Government's Memorandum]; Government's Unclassified Memorandum in Opposition to Defendants' Motion to Suppress Evidence Obtained or Derived From Surveillance Under the FISA Amendments Act and Motion for Discovery at 36–40, *Muhtorov*, No. 12-CR-00033-JLK (D. Colo. May 9, 2014), https://www.clearinghouse.net/chDocs/public/NS-CO-0001-0005.pdf [*Muhtorov* Government's Unclassified Memorandum]; Government's Unclassified Response to Defendant's Alternative Motion for Suppression of Evidence and a New Trial at 27–31, *Mohamud*, No. 3:10-CR-00475-KI, 2014 WL 4792313 (D. Or. May 3, 2014) [hereinafter *Mohamud* Motion to Suppress].

40. *See Mohamud* Appellee Answering Brief, *supra* note 39, at *110–18; *Hasbajrami* Government's Memorandum, *supra* note 39, at 44–53; *Muhtorov* Government's Unclassified Memorandum, *supra* note 39, at 41–51; *Mohamud* Motion to Suppress, *supra* note 39, at 32–40.

41. Although the Supreme Court has never directly recognized a foreign intelligence exception to the warrant requirement, several lower courts did so in cases that arose before FISA went into effect. *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 912–16 (4th Cir. 1980); United States v. Buck, 548 F.2d 871, 875–76 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593, 604–05 (3d Cir. 1974); United States v. Brown, 484 F.2d 418,

The government further maintained that this warrantless surveillance passes muster under the Fourth Amendment's "reasonableness" requirement.[42] In the absence of a warrant requirement, searches generally are deemed reasonable if the government's interests in conducting the search outweigh the privacy interests at stake.[43] The government asserted that its interest in protecting national security by gathering foreign intelligence is of the highest order.[44] On the other side of the equation, it argued, Americans have a diminished privacy interest in communications that foreign targets have received,[45] and that interest is adequately protected by various safeguards in the program—including so-called "minimization" procedures that place some limits[46] on the use and retention of Americans' incidentally

425–27 (5th Cir. 1973). The FISA Court, however, has adopted a much broader view of the exception, in part because the other cases involved surveillance targets who were U.S. citizens, while targets of Section 702 surveillance must reasonably be believed to be foreigners overseas. Accordingly, while other courts held that the exception applies only if the target of surveillance is a foreign power or agent of a foreign power, the FISA Court has held that it applies as long as the target has been assessed by NSA "to possess and/or to be likely to communicate foreign intelligence information concerning a foreign power . . . ." *In re* DNI/AG Certification [redacted], No. 702(i)-08-01, at *35 (Sept. 4, 2008), https://www.clearinghouse.net/chDocs/public/NS-DC-0058-0007.pdf. Moreover, while other courts limited the exception to cases in which acquiring foreign intelligence was the primary purpose of surveillance, the FISA Court has concluded that the exception applies if "the acquisitions are conducted for national security purposes, i.e., 'with a *significant* purpose . . . to obtain foreign intelligence information.'" *Id.* (emphasis added).

42. *See Mohamud* Appellee Answering Brief, *supra* note 39, at *118–39; *Hasbajrami* Government's Memorandum, *supra* note 39, at 53–80; *Muhtorov* Government's Unclassified Memorandum, *supra* note 39, at 52–76; *Mohamud* Motion to Suppress, *supra* note 39, at 41–64.

43. *See, e.g.*, Maryland v. King, 133 S. Ct. 1958, 1970 (2013); Wyoming v. Houghton, 526 U.S. 295, 299–300 (1999); Delaware v. Prouse, 440 U.S. 648, 654 (1979).

44. *See Mohamud* Appellee Answering Brief, *supra* note 39, at *120–23; *Hasbajrami* Government's Memorandum, *supra* note 39, at 58–61; *Muhtorov* Government's Unclassified Memorandum, *supra* note 39, at 55–57; *Mohamud* Motion to Suppress, *supra* note 39, at 45–47.

45. *See Mohamud* Appellee Answering Brief, *supra* note 39, at *123; *Hasbajrami* Government's Memorandum, *supra* note 39, at 61–64; *Muhtorov* Government's Unclassified Memorandum, *supra* note 39, at 58–61; *Mohamud* Motion to Suppress, *supra* note 39, at 47–50.

46. For instance, subject to a number of exceptions, agencies should retain unreviewed Section 702 data for only five years after the expiration of the certification authorizing collection. If the agencies disseminate reports that include U.S. person information obtained through Section 702 surveillance, they should obscure the person's identity unless it is evidence of a crime or necessary to understand foreign intelligence. *See* LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED §§ 3(c)(1), 6(b) (2016), https://www.dni.gov/files/documents/icotr/51117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf; LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED §§ III(G)(1)(a), V(A)–(B) (2016), https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf; LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED §§ 2, 5, 7(d) (2016), https://www.dni.gov/files/documents/icotr/51117/2016_CIA_Section_702_Minimization_Procedures_Se_26_2016.pdf; LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE

collected information.[47]

A. United States v. Mohamud

In the first case to be decided, *United States v. Mohamud*, the district court held that no warrant was required to collect communications between foreign targets and Americans.[48] It adopted the FISA Court's view that "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."[49] Because "[t]he § 702 acquisition targeting a non-U.S. person overseas is constitutionally permissible, so, under the general rule, the incidental collection of defendant's communications with the extraterritorial target would be lawful."[50] The court also embraced the FISA Court's sweeping view of the foreign intelligence exception and held that it provided an alternative justification for proceeding without a warrant.[51]

In assessing the reasonableness of the warrantless surveillance, the district court acknowledged that not all of the government interests reflected in the statutory definition of "foreign intelligence information" necessarily implicate the vital goal of protecting national security.[52] It found, however, that national security was at stake in Mohamud's case.[53] Moreover, because the government had obtained Mohamud's e-mails from the recipient's inbox, the court found that Mohamud's privacy interest in the e-mails was lessened, citing a Ninth Circuit pronouncement that "[a] person's reasonable expectation of privacy may be diminished in transmissions over the Internet or e-mail that have already arrived at the recipient."[54] The court also concluded that "the minimization procedures contribute to the reasonableness of § 702 under the Fourth Amendment."[55]

On appeal, a three-judge panel of the Ninth Circuit affirmed the district court's ruling—although it made clear that its holding was "[c]onfined to the particular facts of this case" and that Section 702 "potentially raises complex statutory and constitutional issues" in other applications.[56] The panel held that a foreigner

---

SURVEILLANCE ACT OF 1978, AS AMENDED §§ B(2)(a), D(1)–(2) (2016), https://www.dni.gov/files/documents/icotr/51117/2016_NCTC_Section_702_Minimizatio_Procedures_Sep_26_2016.pdf.

47. *See Mohamud* Appellee Answering Brief, *supra* note 39, at *124–37; *Hasbajrami* Government's Memorandum, *supra* note 39, at 64–77; *Muhtorov* Government's Unclassified Memorandum, *supra* note 39, at 62–73; *Mohamud* Motion to Suppress, *supra* note 39, at 50–61.

48. United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *15 (D. Or. June 24, 2014).

49. *Id.* (citing *In re* Directives [Redacted] Pursuant to Section 105B of FISA, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008)). (quotation marks omitted).

50. *Id.*

51. *Id.* at *15–18.

52. *Id.* at *22–23.

53. *Id.*

54. *Id.* at *23 (citing United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007)) (quotation marks omitted).

55. *Id.* at *23.

56. United States v. Mohamud, 843 F.3d 420, 438 (9th Cir. 2016).

overseas has "no Fourth Amendment right" and therefore no warrant is required to collect a foreign target's communications, regardless of whether Americans in contact with the target are "incidentally" monitored.[57] The court did not address the government's alternative argument that warrantless surveillance was justified by the foreign intelligence exception.[58]

The panel then assumed, without deciding, that Americans retain a Fourth Amendment interest in their communications with foreign targets, and analyzed whether the "incidental" collection of their communications satisfied the Fourth Amendment's reasonableness requirement.[59] On this point, the panel's analysis essentially echoed that of the district court. The Ninth Circuit denied the defendant's request for rehearing en banc.[60]

B. United States v. Muhtorov

In *United States v. Muhtorov*, the district court conflated the government's two arguments about why a warrant is unnecessary, viewing them—somewhat incongruously—as different components of the "foreign intelligence exception."[61] It then declined to address whether such an exception exists. Ignoring the Supreme Court's instruction that searches impinging on Americans' privacy interests are *per se* unreasonable without a warrant, the court wrote: "I find the special need/foreign intelligence exception argument somewhat academic and limiting, because the standard ultimately is one of reasonableness . . . ."[62]

The court proceeded to find that Section 702 surveillance is reasonable.[63] It held that the government's interest in "using intelligence information to detect and prevent criminal acts of terrorism, and ultimately to punish their perpetrators," outweighed the defendant's privacy interest, which was "at least somewhat diminished when [his communications were] transmitted to a third party over the internet."[64] The court also noted that "the government's use of FAA-acquired communications is carefully controlled under FISA."[65]

---

57. *Id.* at 439–41.

58. *Id.* at 441 n.25.

59. *Id.* at 441–44.

60. Order Denying Petition for Panel Rehearing and Rehearing en banc, United States v. Mohamud, 843 F.3d 420 (9th Cir. 2016) (No. 3:10-cr-00475-KI), https://www.clearinghouse.net/chDocs/public/NS-OR-0003-0020.pdf.

61. United States v. Muhtorov, 187 F. Supp. 3d 1240, 1253 (D. Colo. 2015).

62. *Id.*

63. *See id.* at 1254–57.

64. *Id.* at 1255, 1256. It is unclear whether the "third party" to which the court referred was the Internet Service Provider or the recipient of the communications.

65. *Id.* at 1256 (emphasis omitted). Although not relevant to the focus of this article, the *Muhtorov* court also addressed the defendant's argument that the government's minimization procedures were inadequate because they allowed the FBI to query data acquired under Section 702 for information about Americans. The court dismissed this argument with a three-sentence analysis, the gist of which was that "there is no reasonable expectation of privacy" in information the government has already collected. *See id.* at 1256–57. By that argument, however, the

C. United States v. Hasbajrami

In *United States v. Hasbajrami*, the district court, like the district court in *Mohamud*, held that no warrant was required to collect communications between a foreign target and the American defendant because (1) the targets of surveillance are foreigners who are not protected by the Fourth Amendment, and (2) if the surveillance of the target is lawful, so is the "incidental" surveillance of those in contact with him.[66] In a passage later cited by the Ninth Circuit *Mohamud* panel, the court stated:

> Courts have long dealt with the issue of incidental interception of non-targeted persons' communications. *Amici* correctly point out that some of those cases involve surveillance predicated on warrants, but that is because the targets at issue were U.S. citizens and the surveillance took place on United States soil. A warrant was necessary for the initial surveillance to be lawful. While those cases are thus distinguishable, the guiding principle behind them applies with equal force here: when surveillance is lawful in the first place—whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful.[67]

The court went on to say that "reasonableness" is "[t]he ultimate touchstone of the Fourth Amendment . . . and the requirement that the . . . collection at issue here be reasonable applies even when the warrant requirement does not."[68] The court's reasonableness analysis closely tracked that of the district court and appeals panel in *Mohamud*. It found that the government's interest in conducting the surveillance was "indisputably compelling"; that the defendant had "a diminished—if not nonexistent—expectation of privacy" in communications already sent; and that "the stringent safeguards" contained in Section 702's targeting and minimization requirements reinforced the finding of reasonableness.[69]

III. CLOSING THE "INCIDENTAL OVERHEAR" LOOPHOLE

The fundamental flaw in these decisions stems from the issuing courts' misreading of what the Ninth Circuit panel in *Mohamud* called the "incidental overhear

---

Fourth Amendment would require no minimization procedures whatsoever. That is clearly not the case. As the FISA Court has itself recognized, "the procedures governing retention, use, and dissemination [of 'incidentally' collected information] bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information." [REDACTED], 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011).

66. United States v. Hasbajrami, No. 11-CR-623 (JG), 2016 WL 1029500, at *7–9, (E.D.N.Y. Mar. 8, 2016).

67. *Id.* at *9 (internal citations omitted).

68. *Id.* at *10 (citations omitted).

69. *Id.* at *10–13.

approach."[70] The courts attempted to turn this approach into an exception to the warrant requirement, thus creating a hole in *Katz* that the Supreme Court has never sanctioned.

United States v. Kahn and *United States v. Donovan* are the foundational cases in which the Supreme Court articulated the "incidental overhear" principle (although neither case used this term). These cases came about in the context of domestic criminal prosecutions that took place shortly after Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968[71] (Title III) to codify *Katz*.[72] In simplified terms, Title III requires the government to obtain a warrant to acquire the content of electronic communications.[73]

In both *Kahn* and *Donovan*, the government obtained Title III orders to conduct wiretaps.[74] The defendants argued that their own communications were acquired unlawfully because they were not identified by name in the orders.[75] As discussed further below, the Court held that the warrant was sufficiently "particularized" for Fourth Amendment purposes as long as it identified the phone line to be tapped and the conversations to be acquired, and the government followed rigorous "minimization" procedures to avoid the collection of "innocent conversations"—i.e., those not specified in the warrant.[76]

Understanding where the *Hasbajrami* and *Mohamud* courts went wrong in interpreting these cases requires going back to certain undisputed cardinal Fourth Amendment principles. If Americans have a reasonable expectation of privacy in their communications with foreigners, then a search or seizure of those communications implicates the Fourth Amendment and must be "reasonable."[77] The Supreme Court has held—and, on multiple occasions, reaffirmed—that a warrantless search is "*per se* unreasonable" unless it falls within one of "a few specifically established and well delineated exceptions."[78] These exceptions are "jealously and carefully drawn,"[79] with the Court having recognized fewer than ten of them, by

---

70. *See* United States v. Mohamud, 843 F.3d 420, 439 (9th Cir. 2016) (internal quotation marks omitted).

71. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801–802, 82 Stat. 197 (codified as amended in scattered sections of 5, 18, and 42 U.S.C.).

72. *See* Howard J. Kaplan et al., *The History and Law of Wiretapping* 4, ABA (Apr. 20, 2012), https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/29-1_history_and_law_of_wiretapping.authcheckdam.pdf ("Congress . . . regarded *Katz* and *Berger* as instructive on how to draft a constitutionally sound wiretapping law and thereafter passed the Omnibus Crime Control Act of 1968.").

73. *See* 18 U.S.C. § 2516 (2012).

74. United States v. Donovan, 429 U.S. 413, 416–20 (1977); United States v. Kahn, 415 U.S. 143, 144–47 (1974).

75. *See Donovan*, 429 U.S. at 421; *Kahn*, 415 U.S. at 150.

76. *See Donovan*, 429 U.S. at 427 n.15; *Kahn*, 415 U.S. at 154–55; *infra* Part III.B.

77. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

78. *Katz*, 389 U.S. at 357; Thompson v. Louisiana, 469 U.S. 17, 19–20 (1984) (finding a consistent reaffirmation of "our understanding that in all cases outside the exceptions to the warrant requirement the Fourth Amendment requires the interposition of a neutral and detached magistrate . . . ."); Mincey v. Arizona, 437 U.S. 385, 390 (1978) (affirming as a "cardinal principle" that warrantless searches are *per se* unreasonable).

79. Jones v. United States, 357 U.S. 493, 499 (1958).

most counts.[80]

The *Muhtorov* court failed at this basic step in the analysis. The judge assumed a Fourth Amendment interest, but claimed it was unnecessary to determine whether there was an exception to the warrant requirement, as the appropriate standard was "reasonableness" in either instance.[81] In bypassing the question of whether an exception existed and proceeding straight to whether the warrantless search was reasonable, the judge's analysis contravened the bedrock principle that warrantless searches are *per se* unreasonable absent a recognized exception.

If one returns to that principle, the first question to ask is whether the government's collection of communications between Americans and foreigners under Section 702 constitutes a "search" for Fourth Amendment purposes—i.e., whether Americans have a reasonable expectation of privacy in their communications with foreigners.

A. Is There a Reasonable Expectation of Privacy?

None of the recent Section 702 decisions held that an American's expectation of privacy in her communications—as distinct from the government's obligation to obtain a warrant before intruding on that privacy—turns on the nationality or location of the other party to the communication. Indeed, the FISA Court has repeatedly acknowledged that the acquisition of international communications involving Americans raises Fourth Amendment issues.[82] The courts reviewing Section 702 assumed as much when they performed an analysis of whether the surveillance met the Fourth Amendment's test of "reasonableness."

The government did argue, however, that the defendants' reasonable expectation of privacy evaporated when their e-mails landed in the targets' inbox.[83] The government's briefs asserted that the sender of an electronic communication "loses any cognizable Fourth Amendment rights" in that communication once it is received by the foreign target.[84] The courts did not accept this extreme position, but they found—in the context of engaging in a "reasonableness" analysis—that

---

80. Some commentators consider certain exceptions to be variations of others, so the exact count and description of the exceptions varies depending on the source. There is general agreement, however, that there are exceptions to the warrant requirement for exigent circumstances (e.g., "hot pursuit"); "Terry stops"; searches pursuant to arrest and inventory searches; "plain view"; consent; "special needs" (including administrative searches); motor vehicle searches; and border searches. *See generally Warrantless Searches and Seizures*, 45 GEO. L.J. ANN. REV. CRIM. PROC. 49–50 (2016).

81. United States v. Muhtorov, 187 F. Supp. 3d 1240, 1253–54 (D. Colo. 2015).

82. For instance, a recent FISA Court decision states that Section 702 surveillance "implicates interests protected by the Fourth Amendment" insofar as it captures communications to or from Americans. *See* [REDACTED], 61–62 (FISA Ct. Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.

83. *See Mohamud* Appellee Answering Brief, *supra* note 39, at *123; *Hasbajrami* Government's Memorandum, *supra* note 39, at 61–64; *Muhtorov* Government's Unclassified Memorandum, *supra* note 39, at 58–61; *Mohamud* Motion to Suppress, *supra* note 39, at 47–50.

84. *See e.g.*, *Hasbajrami* Government's Memorandum, *supra* note 39, at 62.

the senders' privacy interest in already-received e-mails was diminished.[85]

This finding hearkens back to pre-digital case law holding that a person's expectation of privacy in a sealed letter ends upon delivery to the recipient.[86] The rationale here is the same one that underlies the third-party doctrine: a person can have no expectation of privacy in information she voluntarily conveys to another, because the recipient is then free to disclose the information to anyone else, including the government.[87]

There is no shortage of scholarship criticizing this approach to privacy. As many have observed, it is specious to equate a voluntary disclosure to one with a voluntary to disclosure to all.[88] When Person A confides in Person B, there is certainly a risk that her trust will be misplaced; but it does not follow that an unanticipated breach of that trust represents a voluntary disclosure by Person A. And even if that were the case, the third party doctrine conflates the risk that Person B will *voluntarily* reveal confidences with the risk that the government may *compel* him to do so.

The result of this flawed logic is that privacy is functionally defined as absolute secrecy. That is not only an untenable outcome in today's digitally interconnected world; it is also a highly artificial concept of privacy.[89] Commentators have put forward alternative views that far better reflect how people actually interact. For instance, privacy may be seen as an individual's control over the extent to which she chooses to disclose her personal information.[90] Just because a person invites a

---

85. United States v. Hasbajrami, No. 11-CR-623 (JG), 2016 WL 1029500, at *10–11, (E.D.N.Y. Mar. 8, 2016); *Muhtorov*, 187 F. Supp. 3d at 1255; United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *23 (D. Or. June 24, 2014).

86. *See, e.g.*, United States v. Gordon, 168 F.3d 1222, 1228 (10th Cir. 1999); United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995).

87. *See* Smith v. Maryland, 442 U.S. 735, 743–45 (1979) (holding that a person lacks a reasonable expectation of privacy in telephone numbers dialed, as these are voluntarily conveyed to the phone company); United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that a person lacks a reasonable expectation of privacy in personal financial information held by banks).

88. *See, e.g.*, Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 258 (2006) ("Neither the *Miller* nor the *Smith* Court explained why any disclosure is equivalent to a public disclosure, even though the logical inconsistency of this proposition is apparent."); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 42 (2007) (noting that the third-party doctrine "treats the reasonable expectation of privacy as all or nothing—if a person cannot establish that his communications are invulnerable to any access, then he may not complain if law enforcement agents access those communications without satisfying constitutional prerequisites."); Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protections*, 73 MINN. L. REV. 583, 636 (1989) ("One of the essential components of privacy . . . is not solitude but the ability to choose those with whom to share business or personal intimacies.").

89. *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 276 (2015) ("Sometimes we choose to reveal . . . information to the world, as when speaking from the proverbial soapbox or sending a tweet. At the other extreme, there may be some information we choose to take to our graves . . . . Privacy is a matter of degree, not absolutes. There is a whole lot in between the soapbox and the coffin. And that space between is the stuff of friendship and familial bonds, of business and professional relationships, and of political and religious associations.").

90. *See generally* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

friend into her house and that friend could relay what he saw to the police, the police are not thereby free to enter the house to see for themselves.[91] A related but subtly different view is that privacy itself can be shared. This concept is sometimes referred to as "shared privacy" or "privity."[92] Courts have recognized this phenomenon in the context of shared property and could in theory apply the concept to communications, as well.[93]

Indeed, the notion that the act of sharing eviscerates privacy—which makes little enough sense as applied to disclosures to third party intermediaries—is particularly inapposite as applied to the "disclosures" that constitute a conversation. Telephone calls, e-mails, and other such communications are iterative exchanges, with each expression incorporating and reflecting the one before—not a series of one-sided disclosures of information. Moreover, the artificial distinction between missives that are sent and missives that are received cannot survive the advent of real-time electronic communication. There can be little doubt that if the government's target in *Katz* had been the person on the other end of the telephone line, rather than Katz himself, that person also would have had a Fourth Amendment claim.

It is highly unlikely that the courts' doctrinal reasoning on third party disclosures will remain intact. Lower courts already have begun to recognize that a warrant is required to obtain the content of e-mails, despite the fact that they are shared with—and can be obtained from—the third-party Internet Service Provider.[94] Although not all courts have followed this lead,[95] Congress has taken steps to fill the gap. In 2017, the House of Representatives unanimously passed the E-mail Privacy Act, which would require the government to obtain a warrant to

---

91. *Cf.* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 65 (2005) ("It is clear that I do not surrender my Fourth Amendment expectation of privacy by knowingly exposing my spaces, my activities and my communications to those with whom I share a home . . . .") (internal quotation marks and citation omitted).

92. *See, e.g.*, Brenner & Clarke, *supra* note 88, at 266–79 (setting forth theory of "relation-based shared privacy"); Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1593 (1987) (arguing that "current fourth amendment jurisprudence is impoverished and distorted by neglecting the ways in which privacy embodies chosen sharing"); Andrew J. DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1109 (2006) (proposing that courts adopt a "rebuttable presumption" that a warrant is required to obtain third party records "whenever individuals show that they had an objectively reasonable expectation of privity in their personal information").

93. Indeed, the concept of shared property could usefully be applied to many other things in which multiple people may have privacy interests. *See, e.g.*, Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873 (2015) (arguing that the concept of shared property—specifically, "tenancy in the entirety"—provides a workable analytic framework for the legal protections that should be afforded a person's genetic code, which invariably is shared to some degree with the person's relatives).

94. United States v. Warshak, 631 F.3d 266, 282–88 (6th Cir. 2010); *In re* Applications for Search Warrants for Information Associated with Target Email Address, Nos. 12–MJ–8119–DJW & 12–MJ–8191–DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012).

95. *See, e.g.*, People v. Thompson, 28 N.Y.S.3d 237, 243–44 (N.Y. Sup. Ct. 2016).

collect the content of e-mails,[96] and its ultimate enactment is likely a matter of time. Courts are also moving in the direction of extending Fourth Amendment protections to communications metadata—in particular, geolocation information—despite its being shared with third parties.[97] And the Supreme Court is currently reviewing *Carpenter v. United States*, a decision of the U.S. Court of Appeals for the Sixth Circuit addressing whether the Fourth Amendment protects historical cell site location records held by mobile service providers.[98]

In any case, it is apparent that the finding of a diminished expectation of privacy in sent communications was not the basis for the courts' holding that no warrant is required for Section 702 surveillance. The courts made this finding in the context of assessing whether the surveillance satisfied the Fourth Amendment's "reasonableness" requirement.[99] That assessment would have been entirely unnecessary if no search or seizure had occurred—i.e., if there had been no intrusion on a reasonable expectation of privacy. The courts thus either acknowledged or assumed that there was such an expectation here.[100]

B. Is the "Incidental Overhear" Doctrine an Exception to the Warrant Requirement?

If Americans have a reasonable expectation of privacy in their communications with foreigners overseas, then the "incidental overhear" cases would justify dispensing with a warrant only if they established an exception to the warrant

---

96. Email Privacy Act, H.R. 387, 115th Cong. (2017); Andy Greenberg, *Passing the Email Privacy Act Has Never Been More Urgent*, WIRED (Feb. 6, 2017, 4:26 PM), https://www.wired.com/2017/02/trump-power-email-privacy-act-never-urgent/. State legislatures are also acting to fill the gap; in 2015, California's governor signed into law the California Electronic Communications Privacy Act ("CalECPA"), which requires state and local law enforcement to obtain a warrant before acquiring e-mails, location information, stored documents, and other data. *See* CAL. PENAL CODE §§ 1546–1546.4 (West 2017); Nicole A. Ozer, *California is Winning the Digital Privacy Fight*, TECHCRUNCH (Nov. 7, 2015), https://techcrunch.com/2015/11/07/california-now-has-the-strongest-digital-privacy-law-in-the-us-heres-why-that-matters/.

97. *See, e.g.*, *In re* Application of the U.S. for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006); *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., No. 06 CRIM. MISC. 01, 2006 WL 468300, at *2 (S.D.N.Y. Feb. 28, 2006); *In re* Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947, 949–50 (E.D. Wis. 2006); *In re* Application of the U.S. for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Nos. [sealed] & Production of Real Time Cell Site Info., 402 F. Supp. 2d 597, 605 (D. Md. 2005). For a thorough description of the state of the law on this issue, *see* Levinson-Waldman, *supra* note 2, at 536–39.

98. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

99. *See supra* Part II.

100. Moreover, even if courts were to maintain the fiction that senders alone have a privacy interest in communications, and that the interest remains intact only until the communication is received, "upstream collection" under FISA Section 702 enables collection of Americans' communications while still winging their way overseas—*i.e.*, before receipt. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 7 (2014), https://www.pclob.gov/library/702-Report-2.pdf.

requirement. This follows from the basic rule, articulated at the outset of this discussion, that warrantless searches and seizures are *per se* unreasonable unless an established exception applies.[101]

The theory that the "incidental overhear" cases established an exception to the warrant requirement should immediately be suspect because the decisions did not use the word "exception," let alone discuss the fact that one was being created. It is difficult to imagine that the Supreme Court would have added to the handful of "jealously and carefully drawn" exceptions to the warrant requirement without even saying so. And indeed, there was no need to find an exception, because the government had obtained a warrant in these cases.[102]

Nonetheless, the courts in *Hasbajrami* and *Mohamud*, following the FISA Court's lead, essentially treated these cases as having *indirectly* established an exception to the warrant requirement. Both courts framed the "guiding principle" of the "incidental overhear" cases as follows: "[W]hen surveillance is lawful in the first place . . . the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful."[103] It follows from this principle that there is an exception to the warrant requirement for those in contact with people—such as foreigners overseas—who may lawfully be targeted without a warrant.[104]

Advocates have argued that there are significant factual distinctions between domestic criminal wiretaps and Section 702 surveillance that make the "incidental overhear" rule inapplicable in the latter context. For instance, the volume of incidental collection is almost certainly much greater in the Section 702 context; the minimization procedures are far less rigorous; and, most fundamentally, there is no warrant for the target, which would provide some vicarious protection for those in contact with him.[105]

These observations are entirely correct. But the flaw in the courts' reasoning is more fundamental than that. The courts did not simply apply the rule in a context where it is inapt; they misread the "incidental overhear" decisions altogether and deduced a "guiding principle" that the cases never established.

---

101. *See supra* note 78.

102. *See supra* note 73–74.

103. United States v. Mohamud, 843 F.3d 420, 440–41 (9th Cir. 2016), *appeal docketed*, No. 17-5126 (U.S. July 18, 2017) (citing United States v. Hasbajrami, No. 11-CR-623 (JG), 2016 WL 1029500, at *9 (E.D.N.Y. Mar. 8, 2016) (quotation marks omitted); *Hasbajrami*, 2016 WL 1029500, at *9.

104. Whether courts have properly interpreted Supreme Court precedent to hold that foreigners overseas have no claim to Fourth Amendment protection is highly debatable, but beyond the scope of this article. *See* GOITEIN & PATEL, *supra* note 22, at 12 n.52 (summarizing the bases for the multiple opinions in *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990)).

105. *See, e.g.*, Jameel Jaffer, *Privacy and Civil Liberties Oversight Board Public Hearing on Section 702 of the FISA Amendments Act, Mar. 19, 2014: Submission of Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union Foundation* 13–15 (Mar. 19, 2014), https://www.pclob.gov/library/20140319-Testimony-Jaffer.pdf.

Consider the Supreme Court cases that the courts reviewing Section 702 surveillance cite as support for their interpretation of the "incidental overhear" rule:[106] *United States v. Kahn* and *United States v. Donovan*. In both cases, the government had obtained a Title III order to conduct wiretaps. In *Kahn*, the government secured an order to wiretap two phones belonging to Irving Kahn.[107] The judge found probable cause to believe that Kahn and "others as yet unknown" were conducting an illegal gambling business, and authorized interception of their communications about the criminal enterprise.[108] The surveillance picked up conversations of Kahn's wife, Minnie Kahn, which revealed that she was involved in the business as well—information that the government had not previously known.[109]

Both Kahn and his wife were charged, and they moved to suppress the phone conversations.[110] Title III requires the government to specify "the identity of the person, *if known*, committing the offense and whose communications are to be intercepted."[111] On its face, as the Court held, this provision does not require the government to specify the name of everyone who is a legitimate target; if it does not yet know the identity of all the probable perpetrators, it is entitled to include "others as yet unknown" in its application.[112] The lower court, however, "seemed to believe that taking the statute at face value would result in a wiretap order amounting to a 'virtual general warrant,' since the law enforcement authorities would be authorized to intercept communications of anyone who talked on the named telephone line."[113]

The Court rejected that reasoning. It cited precedent holding that "[t]he Fourth Amendment requires a warrant to describe only the place to be searched, and the persons or things to be seized, not the persons from whom the things will be seized."[114] In the case of a wiretap, the particularity requirement is met by identifying the phone line to be tapped and the conversations to be acquired (e.g., conversations about a suspected gambling operation).[115] With these requirements met, the Court observed, the Kahns' fear that law enforcement officers could acquire the communications of "anyone who talked on the named telephone line" was unfounded:

> [N]either the statute nor the wiretap order in this case would allow the federal agents such total unfettered discretion. By its own terms, the wiretap order in

106. *Mohamud*, 843 F.3d at 439, 440–41; *Hasbajrami*, 2016 WL 1029500, at *9.
107. United States v. Kahn, 415 U.S. 143, 145–47 (1974).
108. *Id.*
109. *Id.* at 147, 152.
110. *Id.* at 147–48.
111. 18 U.S.C. § 2518(1)(b)(iv) (2012) (emphasis added).
112. *Kahn*, 415 U.S. at 151–53.
113. *Id.* at 154.
114. *Id.* at 155 n.15 (internal quotation marks and citations omitted).
115. *Id.* at 154–55, 154 n.13, 157.

> this case conferred authority to intercept only communications "concerning the above-described (gambling) offenses." Moreover, in accord with the statute the order required the agents to execute the warrant in such a manner as to minimize the interception of any innocent conversations . . . . Thus, the failure of the order to specify that Mrs. Kahn's conversations might be the subject of interception hardly left the executing agents free to seize at will every communication that came over the wire . . . .[116]

The central holding of *Kahn*, in short, was twofold: (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.

In *Donovan*, the Court further refined its interpretation of Title III's requirements. It held that, while the statute does not require the government to identify as-yet unknown targets, it does require the government to identify every *known* target—i.e., every person for whom there is probable cause to suspect criminal activity at the time the application is made.[117] This is a statutory requirement, however, not a constitutional one. The Court engaged in no separate Fourth Amendment analysis; it merely reiterated in a footnote the principle articulated in *Kahn*:

> The Fourth Amendment requires specification of "the place to be searched, and the persons or things to be seized." In the wiretap context, those requirements are satisfied by identification of the telephone line to be tapped and the particular conversations to be seized. It is not a constitutional requirement that all those likely to be overheard engaging in incriminating conversations be named.[118]

In neither of these cases did the Court hold or suggest that no warrant was necessary to collect the defendants' conversations, as long as there was a warrant for the person with whom the defendants were communicating. To the contrary, the Court observed that the warrant the government had obtained *expressly encompassed* the defendants' communications, by virtue of specifying the phone line on which they occurred and the matters being discussed. The Court then affirmed that the Fourth Amendment's particularity requirement requires no further information (although in one of the cases, the Court held that the failure to state the defendant's name violated the statute[119]).

A rule that addresses what information renders a warrant sufficiently particularized can have no application to cases in which no warrant is obtained. The principle that those in contact with a surveillance target are not entitled to any legal

---

116. *Id.* at 154–55.
117. United States v. Donovan, 429 U.S. 413, 423–28 (1977).
118. *Id.* at 427 n.15 (citation omitted).
119. *Id.* at 423–28.

process beyond what the target must receive cannot logically be derived from *Kahn* or *Donovan*.

Courts interpreting Section 702 have also relied on lower court decisions that interpreted and applied *Kahn* and *Donovan*.[120] For the most part, however, these cases do not offer any greater support for the "warrant exception" approach. For instance, in *United States v. Schwartz*—cited by the FISA Court[121]—the defendant complained that the government obtained conversations not covered by the warrant.[122] The Second Circuit saw "no error in [the district judge's] conclusion that the extent of non-pertinent matters intercepted was slight. It is virtually impossible to completely exclude all irrelevant matter from intercepted conversations."[123] In other words, a warrant must specify the conversations to be acquired, but the accidental acquisition of a small number of "innocent conversations" does not invalidate the surveillance. This is a far cry from holding that the government can warrantlessly acquire the communications of anyone in contact with a lawfully surveilled target.

In *United States v. Martin* and *United States v. Figueroa*—cited in *Mohamud* and *Hasbajrami*—the defendants' conversations took place over the phone lines designated in the warrant and the conversations related to the offenses being investigated.[124] Accordingly, they were encompassed by the warrants the government had obtained, and there was no need for the courts to address whether their communications could be warrantlessly acquired.[125] These decisions instead addressed whether probable cause must be established for every participant in the covered conversations, and whether post-*Kahn* case law had diluted the requirement to minimize interception of "innocent conversations" to the point of

---

120. *See Hasbajrami*, 2016 WL 1029500, at *9; *Mohamud*, 2014 WL 2866749, at *15.

121. *In re* Directives [Redacted] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008).

122. *See* United States v. Schwartz, 535 F.2d 160, 164 (2d Cir. 1976).

123. *Id.*

124. United States v. Figueroa, 757 F.2d 466, 468–70 (2d Cir. 1985); United States v. Martin, 599 F.2d 880, 882–84 (9th Cir. 1979).

125. One of the cases cited by the *Hasbajrami* court involved warrantless surveillance and does contain some language (albeit in dicta) that would support the interpretation of the courts reviewing Section 702. In *United States v. Bin Laden*, the district court cited *United States v. Verdugo-Urquidez* for the proposition that foreigners overseas have no Fourth Amendment rights. United States v. Bin Laden, 126 F. Supp. 2d 264, 270 (S.D.N.Y. 2000) (citing United States v. Verdugo-Urquidez, 494 U.S. 259, 265, 271 (1990)). It then cited *Kahn* and its progeny for the proposition that "in the Title III context, incidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment." *Id.* at 280 (citations omitted). It observed that, if the warrantless surveillance of the defendant had indeed been incidental, "the combination of *Verdugo-Urquidez* and the incidental interception cases outlined above would permit the surveillance." *Id.* at 281. In reaching this conclusion, however, the district court engaged in the same fundamental misreading of the incidental overhear cases as the courts reviewing Section 702. The fact that a warrant remains valid despite the inability to exclude every "innocent conversation" has no bearing on whether a warrant is necessary to obtain an American's conversations with a foreign target.

unconstitutionality.[126]

In short, the constitutional crux of *Kahn*, *Donovan*, and their progeny is that a warrant to obtain electronic communications is sufficiently particularized if it includes the facilities to be surveilled and the conversations to be seized; and, as long as reasonable procedures are in place to avoid capturing conversations that fall outside the warrant's scope, the accidental interception of a small number of such conversations does not violate the Fourth Amendment. It is not possible to read this line of cases as establishing—directly or indirectly—an exception to the warrant requirement.

At some level, the *Hasbajrami* and *Mohamud* courts (and the FISA Court, whose lead they followed) must have been uncomfortable with the rule they derived—i.e., that surveillance of anyone in contact with a lawfully surveilled target is itself lawful. After holding that a warrant is not required to obtain Americans' communications with Section 702 targets because the targets have no Fourth Amendment rights, they went on to conduct a Fourth Amendment "reasonableness" analysis, and they emphasized the constitutional significance of minimization requirements.[127] Neither reasonableness nor minimization would be necessary if protections owed to those "incidentally" surveilled were no greater than those owed to the foreign targets.

There is no legal justification or precedent, however, for picking and choosing among the protections that flow from the acknowledgment of a Fourth Amendment interest. Once a court determines that a reasonable expectation of privacy exists and will be invaded by the government's action, a warrant is mandatory under Supreme Court jurisprudence unless an established exception applies. None of the "incidental overhear" cases suggested that they were carving out an exception to the warrant requirement; rather, they delineated the extent to which a warrant may encompass unnamed persons and pull in "innocent conversations" without running afoul of the Fourth Amendment.

CONCLUSION

The emerging case law on the constitutionality of Section 702 surveillance is taking Fourth Amendment jurisprudence down a worrisome constitutional detour.

---

126. *See generally Figueroa*, 757 F.2d 466; *Martin*, 599 F.2d 880. In *Martin*, the court held that the government need not show probable cause as to every person named as a "probable converser" in the warrant, reasoning that because "[t]here is no constitutional requirement that the persons whose conversations may be intercepted be named in the application," it followed that "the Fourth Amendment does not require that the reasons for naming all probable conversers be shown in the application." 599 F.2d at 884. In *Figueroa*, the court addressed whether post-*Kahn* case law had diluted minimization requirements to the point that Title III was unconstitutional on its face; it held that Title III remained constitutional. 757 F.2d at 471–73. It also reached essentially the same conclusion as the court in *Martin*: "[T]he government need not establish probable cause as to all participants in a conversation. If probable cause has been shown as to one such participant, the statements of the other participants may be intercepted *if pertinent to the investigation*." *Id.* at 475 (citation omitted) (emphasis added).

127. *See supra* Part II.A & C.

The courts have implicitly recognized that Americans have protected privacy interests in their communications with foreign targets. Yet they have found that the lack of Fourth Amendment protections for the targets strips Americans of their warrant protections, as well. They have reached this conclusion by misreading the "incidental overhear" cases as indirectly establishing an exception to the warrant requirement, when in fact, the communications at issue in those cases were found to fall *within* the warrants the government had obtained. Read properly, the "incidental overhear" cases have no application to the warrantless collection of Americans' communications under Section 702.

To be sure, a proper understanding of the "incidental overhear" cases does not end the inquiry into the constitutionality of Section 702 surveillance. If courts recognize that they cannot rely on these cases, they will be forced to address the question of whether there is a "foreign intelligence exception" to the warrant requirement, and if so, what is that exception's proper scope. This is a question on which there has been much commentary,[128] several pre-FISA rulings from circuit courts,[129] a dramatically different interpretation by the FISA Court,[130] and essentially no guidance from the Supreme Court.[131]

Ultimately, the resolution of this question will determine whether Section 702 is constitutional in its current form, whether it must be significantly narrowed, or whether it must be abandoned altogether (assuming that the statute is not substantially revised in relevant respects before the courts definitively resolve its constitutionality[132]). But that analysis must proceed from the premise that Americans have a reasonable expectation of privacy in their communications with foreigners, and that interest is not extinguished or lessened simply because the foreigner's own privacy interest is not constitutionally cognizable.

---

128. *See, e.g.*, GOITEIN & PATEL, *supra* note 22, at 38–39; Steve Vladeck, *More on Clapper and the Foreign Intelligence Exception*, LAWFARE (May 23, 2012 3:32 PM), https://www.lawfareblog.com/more-clapper-and-foreign-intelligence-surveillance-exception.

129. *See supra* note 39.

130. *See id*.

131. *See* United States v. U.S. Dist. Court for the E. Dist. of Mich., 407 U.S. 297 (1972) (known as the "Keith" case). In *Keith*, the Court held that a warrant was required to conduct surveillance for domestic national security purposes. The Court left open, however, the question of whether a warrant would be required if the target of surveillance were a foreign power or its agent. *See id.* at 318–22.

132. Section 702 was created by the FISA Amendments Act of 2008, which is scheduled to expire on December 31, 2017, unless reauthorized. At time of writing, members of Congress have introduced several bills that would make significant changes to Section 702 in the course of reauthorizing it. *See* USA Liberty Act of 2017, S. 2158, 115th Cong. (as introduced, Nov. 16, 2017); FISA Amendments Reauthorization Act of 2017, S. 2010, 115th Cong. (as reported by the S. Select Comm. on Intelligence, Oct. 25, 2017); USA RIGHTS Act of 2017, S. 1997, 115th Cong. (as introduced, Oct. 24, 2017); FISA Amendments Reauthorization Act of 2017, H.R. 4478, 115th Cong. (as introduced, Nov. 29, 2017); USA Liberty Act of 2017, H.R. 3989, 115th Cong. (as reported by the H. Comm. on the Judiciary, Nov. 8, 2017). Although three of the bills—the Senate and House versions of the USA Liberty Act, and the USA RIGHTS Act—would require U.S. officials to obtain warrants in order to access certain U.S. person information collected under Section 702, none of them would require a warrant to collect communications between foreign targets and people inside the United States.