Case No. 18-1366

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff-Appellee,

v.

JAMSHID MUHTOROV

Defendant-Appellant.

On Appeal from the United States District Court for the District of Colorado
The Honorable John L. Kane
District Court Criminal Action No. 1:12-CR-00033-JLK-1

BRIEF OF THE BRENNAN CENTER FOR JUSTICE AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Elizabeth Goitein
THE BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
1140 Connecticut Ave. NW
Ste. 1150
Washington, DC 20036
(202) 249-7192
goiteine@brennan.law.nyu.edu

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rules 26.1 and 29(a)(4)(A) of the Federal Rules of Appellate Procedure, *amicus curiae* states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST[1]

Amicus curiae the Brennan Center for Justice at NYU School of Law[2] is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice. The Center's Liberty and National Security (LNS) Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. One of the LNS Program's main areas of research and advocacy is foreign intelligence surveillance and the effect of changes in the law and in technology on the privacy of Americans.

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(2), *amicus* represents that all parties have consented to the filing of this brief. Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), *amicus curiae* certifies that no person or entity, other than *amicus*, its members, or its counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part.

[2] *Amicus curiae* does not purport to represent the position of the NYU School of Law.

SUMMARY OF ARGUMENT

Foreign intelligence surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) raises novel Fourth Amendment issues that could have a dramatic effect on the scope of Americans' privacy. Outside of the Foreign Intelligence Surveillance Court (FISC), courts are just beginning to grapple with these questions. Unfortunately, in the few decisions to be reached thus far, a fundamental misreading of the so-called "incidental overhear" doctrine has begun to take hold. Unless corrected, this misreading threatens to create a gaping hole in the Fourth Amendment's warrant protection.[3]

The government must reasonably believe the "targets" of Section 702 to be foreigners overseas, but the surveillance inevitably pulls in large amounts of communications between foreigners and Americans. According to the government, no warrant is required to obtain these communications because foreigners have no Fourth Amendment rights, and because the capture of Americans' communications is "incidental." The FISC, and a handful of courts following its lead, have accepted this argument.

[3] The arguments in this brief are taken in significant part from a law review article published by counsel for *amicus curiae*: Elizabeth Goitein, *Another Bite Out of Katz: Foreign Intelligence Surveillance and the Incidental Overhear Doctrine*, 55 Am. Crim. L. Rev. 105 (2017).

In fact, however, the Supreme Court has made clear that the government may not infringe on Americans' privacy rights unless it has a warrant or the infringement falls within one of the established exceptions to the warrant requirement. Courts have acknowledged that surveillance of communications between foreign targets and Americans implicates Americans' privacy rights. Accordingly, for the surveillance in this case to be lawful, an established exception to the warrant requirement must apply.

The "incidental overhear" doctrine on which the government relies is not such an exception. Indeed, the doctrine arose in the context of criminal investigations in which the government *did* obtain a warrant to conduct surveillance. The Supreme Court, in those cases, held that warrants need not name every participant in a conversation in order to be sufficiently "particularized," and lower courts further held that the accidental interception of a small number of conversations that fall outside the scope of the warrant does not render the surveillance unlawful. These rulings are facially inapplicable to a case in which no warrant was obtained. If they are wrongly treated as an exception to the warrant requirement, the result will be a profound erosion of Americans' privacy in their international communications.

ARGUMENT

I. THE ADVENT OF MASS FOREIGN INTELLIGENCE SURVEILLANCE POSES NOVEL AND HIGH-STAKES FOURTH AMENDMENT QUESTIONS

Some legal and factual background is necessary to underscore both the novelty of the legal framework this Court is asked to review and the broad implications of the Court's decision.

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). *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified in scattered sections of 8, 18, 47, 50 of the United States Code). 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 FISC that the target was a "foreign power" or an "agent of a foreign power." 50 U.S.C. § 1805(a)(2)(A). While FISA defines these terms broadly, *see id.* § 1801(a)&(b), they still encompass only a small fraction of foreigners overseas (and an even smaller fraction of Americans), and their application was subject to case-by-case judicial review. *See id.* § 1805(a).

The substantive and procedural limits set forth in FISA did not apply when the government conducted foreign intelligence surveillance overseas, unless the government intentionally targeted a particular, known American to acquire wire or radio communications or sought to obtain wholly domestic radio communications. *See id.* § 1801(f). Overseas surveillance that does not target Americans is generally not subject to judicial review and is governed almost entirely by Executive Order 12333, which prohibits intentional targeting of U.S. persons but otherwise imposes few restrictions on collection. *See* Exec. Order No. 12,333, 3 C.F.R. § 200 (1981), *reprinted as amended in* 50 U.S.C. app. § 401. Nonetheless, until at least the waning years of the 20th century, the limits of technology served as a practical barrier to mass surveillance. *See* Elizabeth Goitein & Faiza Patel, *What Went Wrong with the FISA Court*, Brennan Ctr. for Justice, 19–21 (2015). International communication was difficult and expensive, *see, e.g.*, Jean-Yves Huwart & Loïc Verdier, *Economic Globalisation: Origins and Consequences*, Org. for Econ. Co-operation and Dev., 35–36 (2013) (noting that "[i]n 1930, a three-minute telephone call between New York and London cost USD 250") and, therefore, relatively rare. *See* Linda Blake & Jim Lande, *Trends in the U.S. International Telecommunications Industry*, Indus. Analysis Div., Fed. Commc'ns. Comm'n, tbl. 4 (1998). 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. The result is an explosion in international communication. The FCC reported 84.7 billion minutes spent on international telephone calls by Americans in 2014—an average of nearly four and a half hours per person, not including minutes spent on Internet-based video and voice communications systems like Skype. *See* Stacey Ashton & Linda Blake, *2014 International Telecommunications Traffic and Revenue Data*, Telecommc'ns and Analysis Div., Fed. Commc'ns. Comm'n, 1 (2016). The number of emails sent daily is projected to exceed 300 billion in 2020. *See Email Statistics Report, 2019-2023*, Radicati Grp., 3 tbl. 2 (2019). 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. *See* 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); *see also* Bob

Sorokanich, *Report: The NSA Is Recording Nearly Every Call Made in Afghanistan*, Gizmodo (May 23, 2014, 10:06 AM).

In the midst of this technological revolution, Congress significantly weakened the legal protections afforded by FISA. Under Section 702 of FISA, created by the 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)—which replaced the similar Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (expired 2008)—the government is no longer required to obtain individualized authorization from the FISC when conducting domestic wiretapping of foreign targets' communications with Americans. *See* 50 U.S.C. § 1881a. 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, extremely broadly defined. *See id*; 50 U.S.C. § 1801(e).

These changes have enabled mass surveillance of communications between foreigners and Americans. The exact number of such communications acquired is unknown, but a 2011 FISC opinion noted that the government was obtaining 250 million Internet communications each year based on domestic foreign intelligence surveillance alone, *see* [REDACTED], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011) (unpublished), and as Appellant points out in his opening brief, that

number is likely several times higher today. *See* Appellant's Opening Br. at 21. Given the prevalence of international communication, it is inevitable that this includes millions, if not tens of millions, of Americans' communications; that number could well be higher in the context of overseas surveillance, which is relatively unregulated.

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. THE "INCIDENTAL OVERHEAR" DOCTRINE DOES NOT JUSITFY WARRANTLESS SURVEILLANCE UNDER SECTION 702

Only a handful of federal courts (and only one Circuit Court) have addressed this question. To date, most have adopted the government's so-called "incidental overhear" argument. In doing so, they risk writing a fundamental misinterpretation of longstanding Fourth Amendment doctrine into the law, with the result that a large and growing swathe of Americans' communications will be stripped of the protection afforded by the warrant requirement.

The gist of the argument is 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. *See* Gov't's Unclassified Mem. in

Opp'n to Defs.' Mot. to Suppress Evidence Obtained or Derived from Surveillance Under the FISA Amendments Act and Mot. for Disc. 36–38, May 9, 2014, *United States v. Muhtorov*, 187 F. Supp. 3d 1240 (D. Colo. 2018) (No. 12-CR-00033-JLK) [hereinafter *Muhtorov* Government's Unclassified Memorandum]. The FISC has embraced this theory, asserting that "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful." *See In re* Directives [Redacted] Pursuant to Section 105B of FISA, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008). In recent decisions, other courts followed the FISC's lead. *See United States v. Mohamud*, No. 3:10–CR–00475–KI–1, 2014 WL 2866749 (D. Or. June 24, 2014) (unpublished) ("[Because the] § 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."); *see also United States v. Mohamud*, 843 F.3d 420, 439-41 (9th Cir. 2016); *United States v. Al-Jayab*, No. 16-CR-00181 at 43-45 (N.D. Ill. June 28, 2018), https://bit.ly/35f9pKT; *United States v. Hasbajrami*, No. 11-CR-623 (JG), 2016 WL 1029500, at *7–9 (E.D.N.Y. Mar. 8, 2016) (unpublished).

Understanding where these courts went wrong requires going back to certain undisputed cardinal Fourth Amendment principles. If Americans have a reasonable expectation of privacy in their communications with foreigners overseas, then a

search or seizure of those communications implicates the Fourth Amendment and must be "reasonable." *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). 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." *Katz*, 389 U.S. at 357; *see also Riley v. California*, 573 U.S. 373, 382 (2014) ("In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."); *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). These exceptions are "jealously and carefully drawn," *Jones v. United States*, 357 U.S. 493, 499 (1958), with the Court having recognized fewer than ten of them, by most counts.[4]

[4] 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 (2016).

The district court below failed at this basic step in the analysis. The court 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. *See United States v. Muhtorov*, 187 F. Supp. 3d 1240, 1253 (D. Colo. 2015) ("I find the special need/foreign intelligence exception argument somewhat academic and limiting, because the standard ultimately is one of reasonableness . . . ."). In bypassing the question of whether an exception existed and proceeding straight to whether the warrantless search was reasonable, the court'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. Americans Have a Reasonable Expectation of Privacy in Their Communications with Foreigners

Notably, not one 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 FISC has long acknowledged that the acquisition of international communications involving Americans implicates the Fourth Amendment. *See, e.g.*, [REDACTED], No. [REDACTED] 61–62 (FISA Ct. Apr. 26, 2017) (unpublished), http://bit.ly/d56exnj (stating that Section 702 surveillance "implicates interests protected by the Fourth Amendment" insofar as it captures communications to or from Americans).

Citing the so-called "third party doctrine," the government nonetheless argues that Americans' expectation of privacy evaporates entirely when their e-mails land in the recipients' inbox. *See Muhtorov* Government's Unclassified Memorandum at 59-60. The courts, however, have not accepted this extreme position. Instead, the district court found—in the context of engaging in a "reasonableness" analysis—that a sender's privacy interest in e-mails sent over the Internet is "at least somewhat diminished." *Muhtorov*, 187 F. Supp. 3d at 1255; *see also Mohamud*, 843 F.3d at 442 (finding a "diminished" privacy interest in received communications); *Al-Jayab*, No. 16-CR-00181 at 49 (same); *Hasbajrami*, 2016 WL 1029500, at *11 (same).

This finding is questionable in light of intervening case law. In *Carpenter v. United States*, the Supreme Court held that a warrant is required to obtain an individual's cell site location information (CSLI) from a wireless carrier. *See*

Carpenter v. United States, 138 S. Ct. 2206 (2018). The Court noted that such information can provide "an intimate window into a person's life, revealing not only his particular movements, but his familial, political, professional, religious, and sexual associations." *Carpenter*, 138 S. Ct. at 2217 (internal quotation marks and citation omitted). Under these circumstances, "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Id.* at 2231. The Court contrasted CSLI with the telephone numbers and bank records that were the subject of the cases establishing the third-party doctrine, noting that the latter were "not confidential communications." *Id.* at 2216 (international quotation marks and citation omitted). The logic of the Court's opinion would be easily transferrable to e-mails. Indeed, even before *Carpenter*, courts already had 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—third-party Internet Service Providers. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 282–88 (6th Cir. 2010); *In re* Applications for Search Warrants for Info. Associated with Target Email Address, Nos. 12–MJ–8119–DJW & 12–MJ–8191–DJW, 2012 WL 4383917, at *5 (D. Kan. Sep. 21, 2012) (unpublished); *United States v. Ali*, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012).

In any case, it is apparent that the finding of a diminished expectation of

privacy in sent communications was not the basis for the district court's holding that no warrant is required for Section 702 surveillance. The court made this finding—as did the other courts that have addressed this question—in the context of assessing whether the surveillance satisfied the Fourth Amendment's "reasonableness" requirement. 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.[5]

B. The "Incidental Overhear" Doctrine Is Not 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 requirement. This follows from the basic rule, articulated above, that warrantless searches and seizures are *per se* unreasonable unless an established exception applies.

[5] Moreover, even if courts were to maintain the fiction that any reasonable expectation of privacy in communications terminates once they have been received, "upstream collection" under FISA Section 702 enables collection of Americans' communications while still winging their way overseas—i.e., before receipt. *See Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Privacy & Civil Liberties Oversight Bd., 7 (2014).

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 (Title III) to codify the Supreme Court's seminal ruling in *Katz*, 389 U.S. at 347. *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.); Howard J. Kaplan et al., *The History and Law of Wiretapping*, Am. Bar Ass'n, 4 (Apr. 20, 2012) ("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."). In simplified terms, Title III required the government to obtain a warrant to acquire the content of electronic communications. *See* 18 U.S.C. § 2516.

In both *Kahn* and *Donovan*, the government obtained Title III orders to conduct wiretaps. *See United States v. Donovan*, 429 U.S. 413, 418–20 (1977); *United States v. Kahn*, 415 U.S. 143, 144–45 (1974). The defendants argued that the orders were invalid because they did not name every person whose communications would be collected. *See Donovan*, 429 U.S. at 421; *Kahn*, 415 U.S. at 150. 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. *See Donovan*, 429 U.S. at 427 n.15; *Kahn*, 415 U.S. at 154–55, 157.

The theory that these 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.

Nonetheless, courts in recent Section 702 cases, following the FISC's lead, essentially treated these cases as having *indirectly* established an exception to the warrant requirement. They have characterized 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." *Hasbajrami*, 2016 WL 1029500 at *9; *see also Mohamud*, 843 F.3d at 440–41 (quoting *Hasbajrami*, 2016 WL 1029500 at *9); *Al-Jayab*, No. 16-CR-00181 at 44 (same). It follows from this principle that

there is an exception to the warrant requirement for those in contact with people—such as foreigners overseas—whose conversations may lawfully be intercepted without a warrant.[6]

A close examination of the relevant decisions shows the courts' error. In *United States v. Kahn*, the government secured a Title III order to wiretap two phones belonging to Irving Kahn. 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. 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. *See Kahn*, 415 U.S. at 145-47, 152.

Both Kahn and his wife were charged, and they moved to suppress the phone conversations. *See id.* at 148. Title III requires the government to specify "the identity of the person, *if known*, committing the offense and whose communications are to be intercepted." 18 U.S.C. § 2518(1)(b)(iv) (emphasis added). 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

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

not yet know the identity of all the probable perpetrators, it is entitled to include "others as yet unknown" in its application. *Kahn*, 415 U.S. at 151–53. 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." *Id.* at 154.

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." *Id.* at 155 n.15 (internal quotation marks and citations omitted). 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). *See id.* at 154–55, 154 n.13, 157. 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 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 . . . .

Id. at 154–55 (alteration in original).

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. *See Donovan*, 429 U.S. at 423–28. 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.

Id. at 427 n.15 (citation omitted).

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).

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 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*. *See Hasbajrami*, 2016 WL 1029500, at *9; *Muhtorov*, 187 F. Supp. 3d at 1250–53; *Mohamud*, 2014 WL 2866749, at *15; *In re* Directives [Redacted] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d at 1015. 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*, the defendant complained that the government obtained conversations not covered by the warrant. *See United States v. Schwartz*, 535 F.2d 160, 164 (2d Cir. 1976). 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." *Id.* 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 may freely acquire, without a warrant, the communications of anyone in contact with a lawfully surveilled target.

In *United States v. Martin* and *United States v. Figueroa*, the defendants' conversations took place over the phone lines designated in the warrant and the conversations related to the offenses being investigated. *See United States v. Figueroa*, 757 F.2d 466, 470–71 (2d Cir. 1985); *United States v. Martin*, 599 F.2d 880, 883–86 (9th Cir. 1979). 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.[7] These decisions

[7] 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 interpreting Section 702. In *United States v. Bin Laden*, the district

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 unconstitutionality.[8]

---

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, 281 (S.D.N.Y. 2000) (citing *Verdugo-Urquidez*, 494 U.S. at 265, 271). 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." *Bin Laden*, 126 F. Supp. 2d 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.

[8] 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." *Martin*, 599 F.2d at 889. 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. *See Figueroa*, 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).

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 courts reviewing Section 702 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 all went on to conduct a Fourth Amendment "reasonableness" analysis, and they emphasized the constitutional significance of minimization requirements. *See Mohamud*, 843 F.3d at 441-44; *Al-Jayab*, No. 16-CR-00181 at 48-56; *Hasbajrami*, 2016 WL 1029500, at *10-13; *Muhtorov*, 187 F. Supp. 3d at 1254-57; *Mohamud*, 2014 WL 2866749, at *22-23. 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. Courts have recognized, explicitly or implicitly, 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.

This Court's analysis should 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 foreigners' own privacy interest is not constitutionally cognizable. For this reason among others,[9]

[9] A proper understanding of the "incidental overhear" cases does not end the inquiry into whether a warrant is required to collect communications between foreign targets and Americans under Section 702 of FISA. There is also the question of whether a "foreign intelligence exception" applies. A full discussion of this argument is beyond the scope of this brief; however, it is addressed briefly here because the argument for a foreign intelligence exception that would be broad enough to legitimize warrantless surveillance under Section 702 suffers from a similar flaw to that in the "incidental overhear" argument.

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, 912–916 (4th Cir. 1980); *United States v. Buck*, 548 F.2d 871, 875–76 (9th Cir. 1977); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974); *United States v. Brown*, 484 F.2d 418, 425–27 (5th Cir. 1973). As Appellant notes in his opening brief, however, the courts in these cases emphasized the need for strict limitations on the foreign intelligence exception, including a requirement that the surveillance be directed at foreign powers or their agents. *See* Appellant's Opening Br. at 35. No such requirement exists when the government conducts surveillance under Section 702.

In its briefs below, the government argued that the limits described in the "foreign intelligence exception" cases are inapposite because the "targets" in those cases were inside the U.S., while the "targets" of Section 702 surveillance are foreigners overseas. *See Muhtorov* Government's Unclassified Memorandum at 50. Once again, however, there is no basis in Fourth Amendment doctrine for the notion that when an American's privacy is breached, the reach of the warrant requirement—or the breadth of any exception to it—turns on the nationality of the "target." *See* Orin Kerr, *The Surprisingly Weak Reasoning of Mohamud*, Lawfare, Dec. 23, 2016 ("In

amicus curiae urge this Court to reverse the decision below.

Dated: October 7, 2019

By: /s/ Elizabeth Goitein
THE BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
1140 Connecticut Ave. NW
Ste. 1150
Washington, DC 20036
(202) 249-7192
goiteine@brennan.law.nyu.edu
Counsel for Amicus Curiae

Fourth Amendment law, the concept of 'targeting' doesn't exist. . . . Fourth Amendment law focuses what the government does, not what the government is thinking when it does it."). And there is certainly no principled basis for the government's invention of a watered-down foreign intelligence exception that arbitrarily splits the difference between the lack of protection available to foreigners and the robust protections our Constitution requires for Americans.

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitations of Fed. R. App. P. 29(a)(5) and Fed. R. App. P. 32(a)(7)(B) because this brief contains **6,087** words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f) and Local Rule 32.

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016 in 14-point Times New Roman.

Dated: October 7, 2019

By: /s/ Elizabeth Goitein
THE BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
1140 Connecticut Ave. NW
Ste. 1150
Washington, DC 20036
(202) 249-7192
goiteine@brennan.law.nyu.edu
Counsel for Amicus Curiae

CERTIFICATE OF DIGITAL SUBMISSION

I hereby certify that with respect to the foregoing:

1. All required privacy redactions have been made;

2. If required to file additional hard copies, that the ECF submission is an exact copy of those documents;

3. The digital submissions have been scanned for viruses with the most recent version of a commercial virus scanning program, WebRoot Secure Anywhere for Windows, and according to the program are free of viruses.

Dated: October 7, 2019

By: /s/ Elizabeth Goitein
THE BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
1140 Connecticut Ave. NW
Ste. 1150
Washington, DC 20036
(202) 249-7192
goiteine@brennan.law.nyu.edu
Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify that on October 7, 2019, I caused the foregoing Brief of *Amicus Curiae* to be electronically filed via the PACER NextGen system, which will send notification of such filing to the following:

James C. Murphy
James.Murphy3@usdoj.gov

Joseph Palmer
Joseph.Palmer@usdoj.gov

Counsel for Plaintiff-Appellee

John C. Arceci
John_Arceci@fd.org

Ashley Gorski
AGorski@aclu.org

Patrick Toomey
PToomey@aclu.org

Counsel for Defendant-Appellant

Dated: October 7, 2019

By: /s/ Elizabeth Goitein
THE BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
1140 Connecticut Ave. NW
Ste. 1150
Washington, DC 20036
(202) 249-7192
goiteine@brennan.law.nyu.edu
Counsel for Amicus Curiae