15-2684 (L), 17-2669 (CON)

IN THE

United States Court of Appeals

FOR THE

Second Circuit

UNITED STATES OF AMERICA,
Appellee,

– v.–

AGRON HASBAJRAMI,
Defendant-Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993
mark@eff.org

Patrick Toomey
Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street—18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Attorneys for Amici Curiae American Civil Liberties Union and Electronic Frontier Foundation

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, amici curiae state that no party to this brief is a publicly held corporation, issues stock, or has a parent corporation.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nonprofit, nonpartisan organization with more than 1.6 million members dedicated to the principles of liberty and equality embodied in the Constitution. The ACLU has appeared before the courts in many cases involving the Fourth Amendment, including cases concerning foreign-intelligence surveillance. *See, e.g.*, *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013); *Wikimedia Found. v. NSA*, 857 F.3d 193 (4th Cir. 2017).

The Electronic Frontier Foundation ("EFF") is a civil liberties organization working to protect innovation, free speech, and privacy in the online world. With over 38,000 members, EFF represents the interests of technology users in court cases involving the application of law in the digital age. *See, e.g.*, *Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2011); *In re NSA Telecomm. Records Litig.*, 671 F.3d 881 (9th Cir. 2011).

[1] All parties consent to the filing of this brief. No party or party's counsel authored this brief or contributed money to fund the preparation or submission of this brief. No person other than amici, their members, and their counsel contributed money to fund the preparation or submission of this brief.

INTRODUCTION

This case concerns a regime of electronic surveillance unprecedented in our nation's history and unlike anything this Court has countenanced in the past. Relying on a statutory authority known as Section 702, 50 U.S.C. § 1881a, the government intercepts billions of international communications sent by hundreds of thousands of individuals, including Americans. The government stores these communications in massive databases, retains them for years, and searches them repeatedly for information about Americans—including, as a matter of course, in domestic criminal investigations wholly unrelated to national security. This surveillance takes place inside the United States and with only limited involvement by the Article III judges on the Foreign Intelligence Surveillance Court. All of this surveillance is conducted without a warrant or anything resembling one.

This regime of warrantless surveillance violates the Fourth Amendment.

Section 702 surveillance, including the surveillance of Mr. Hasbajrami here, lacks safeguards for Americans that the Constitution requires. Indeed, there is a profound mismatch between the government's justification for this warrantless surveillance and the way it actually uses the wealth of private emails and phone calls it obtains. Under Section 702, the government claims to target foreigners abroad who lack Fourth Amendment rights. Yet this surveillance routinely sweeps up Americans whose communications are indisputably entitled to constitutional

protection. Rather than discarding Americans' communications or tightly restricting their use—given the absence of any warrant to search through them—the government exploits this enormous loophole. It pools communications collected under Section 702 in databases available to FBI agents around the country, who deliberately search for the communications of Americans that the government acquired without a warrant. Even if the Constitution permits the government to target foreigners abroad without a warrant, it does not permit this end-run around Americans' Fourth Amendment rights.

There is a narrow way for this Court to resolve the challenge before it: by finding that the procedures that governed the surveillance of Mr. Hasbajrami were constitutionally unreasonable, and thus violated the Fourth Amendment, because they permitted agents to freely use and search for the communications of Americans obtained without a warrant. Because the procedures failed to require individualized judicial approval of any kind—even after the fact, and even when the government sought to use or query the communications of a *known* U.S. person—the Court can and should find them defective.

BACKGROUND

Relying on Section 702, the government conducts warrantless surveillance of vast quantities of international communications entering and leaving the United States—including communications sent and received by Americans.

Section 702, codified by the FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, revolutionized, and dramatically expanded, the government's foreign-intelligence surveillance authorities. The statute "creat[ed] a new framework" under which the government could obtain authorization from the Foreign Intelligence Surveillance Court ("FISC") to conduct surveillance "targeting the communications of non-U.S. persons located abroad." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 404 (2013).

The original statutory regime for conducting foreign-intelligence surveillance in the United States, the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq*., authorized surveillance only upon an application to the FISC for individualized approval of a surveillance target, and only after the FISC found probable cause that the target was a foreign power or foreign agent.

Under Section 702, by contrast, surveillance occurs without any finding of probable cause or showing of individualized suspicion. The government need not demonstrate that the people it seeks to surveil are agents of foreign powers, engaged in criminal activity, or connected even remotely with terrorism. Instead, the FISC's role consists principally of an annual review of broad, programmatic guidelines that the government uses to conduct surveillance. The government need not even inform the FISC whom it intends to target.

Three aspects of Section 702 surveillance bear emphasis. Section 702 surveillance is alarmingly vast. It purposefully sweeps up the international communications of Americans without a warrant. And the statute authorizes surveillance with only limited judicial review of "targeting" and "minimization" procedures—procedures that fail to protect the privacy of Americans.

1. Section 702 surveillance is breathtaking in its scope. The government's surveillance encompasses tens of thousands of "targets" and sweeps in billions of electronic communications, including Americans' communications. With the cooperation of American telecommunication and Internet companies, the government carries out this surveillance inside the United States.[2] Section 702

[2] The government conducts Section 702 surveillance in one of two ways, commonly known as PRISM and Upstream. Under PRISM, it compels Internet service providers, such as Google and Facebook, to turn over the communications of their customers. Under Upstream, the government cooperates with telecommunication companies, like AT&T and Verizon, to intercept communications in real-time as they flow through Internet backbone cables. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702* at 7 (2014), https://perma.cc/WD5R-5GKE ("PCLOB Report").

The government asserted below that only PRISM was used to surveil Mr. Hasbajrami, *see* A.81, though it has admitted elsewhere that *both* PRISM and Upstream are used to surveil the same targets. PCLOB Hearing Tr. 57 (Mar. 19, 2014), https://perma.cc/Y57J-L4JB.

reaches every form of modern electronic communication: telephone calls, emails, video calls, texts, and online chats, among others.[3]

The latitude afforded by the statute drives this sweeping collection. Section 702 authorizes "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a). The government can target *any* foreigner abroad to obtain "foreign intelligence information"—a term broadly defined to encompass nearly any information bearing on the foreign affairs of the United States. *Id*. § 1801(e).

The government reported that, in 2016, it monitored the communications of 106,469 targets under a single FISC order.[4] In 2011, when it monitored approximately one-third that number of targets,[5] the government still collected more than 250 million communications.[6] Today, with nearly three times as many targets, the government likely collects over a billion communications under Section 702 each year.[7]

---

[3] *NSA Slides Explain the PRISM Data-Collection Program*, Wash. Post. (Jun. 6, 2013), http://wapo.st/J2gkLY.

[4] Office of the Director of National Intelligence, *2016 Statistical Transparency Report* (Apr. 2017), goo.gl/HurVE8.

[5] Glenn Greenwald, *No Place to Hide* 111 (2014), https://perma.cc/6VU2-5RNH (NSA documents showing that 35,000 "unique selectors" were surveilled under PRISM in 2011).

[6] [*Redacted*], 2011 WL 10945618, at *9 (FISC Oct. 3, 2011).

[7] PCLOB Report 116 (noting the "current number is significantly higher" than in 2011).

Although the government targets a significant number of persons under Section 702, the number of "targets" does not reflect the true scope of the surveillance. The *Washington Post*'s review of a "large cache of intercepted conversations" revealed that the vast majority of account holders subject to surveillance "were not the intended surveillance targets but were caught in a net the agency had cast for somebody else."[8] The material reviewed by the *Post* consisted of 160,000 intercepted email and instant message conversations, 7,900 documents—including "medical records sent from one family member to another, resumes from job hunters and academic transcripts of schoolchildren"—and more than 5,000 private photos.[9] The *Post* estimated that, at the government's rate of "targeting," annual collection under Section 702 would encompass more than 900,000 user accounts.[10]

The volume of communications intercepted is far too great for government analysts to individually review—let alone use—every communication collected. Thus, there is no "minimization" of Americans' emails and phone calls at the moment the communications are obtained. They are simply added to the

[8] Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post (Jul. 5, 2014), http://wapo.st/1MVootx.

[9] *Id*.

[10] *Id.*

government's massive databases of intercepted communications, to await later search, use, and analysis. PCLOB Report 128-29.

2. This sprawling surveillance apparatus inevitably—and intentionally—sweeps in the communications of Americans without a warrant. As the FISC has observed, Section 702 surveillance results in the government obtaining "substantial quantities of information concerning United States persons and persons located inside the United States who are entitled to Fourth Amendment protection."[11] Indeed, intelligence officials have stated that this is one of the principal aims of the surveillance.[12]

Each time an American communicates with any one of the government's targets—which may include journalists, academics, human rights researchers, or employees of foreign-owned corporations—the government collects and stores that communication. It is unknown precisely how many Americans are swept up in the government's surveillance web. Despite repeated requests from members of Congress, the government has refused even to estimate the number of Americans' communications it collects under Section 702. By all accounts, however, the volume is significant.

---

[11] [*Redacted*], No. [Redacted], at 24 (FISC Aug. 30, 2013) https://perma.cc/GR62-FNQC.

[12] *See FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 9 (2006), https://goo.gl/16ZJBH (statement of NSA Director Michael Hayden).

Not only are Americans' communications collected in substantial quantities under Section 702, they are also retained, searched, and used in later investigations—including in domestic criminal investigations unrelated to the foreign-intelligence purpose for which they were ostensibly collected. *See* PCLOB Report 59. The government amasses the collected communications in long-term databases, where agents routinely search through them—including by using Americans' names or email addresses to investigate particular Americans. These "backdoor searches" allow the government to target and read the communications of Americans without obtaining a warrant or any specific judicial authorization. *See id.* at 55-60. In short, these queries are designed to extract communications that the government *knows* are protected by the Fourth Amendment.

3. Section 702's "targeting" and "minimization" procedures fail to cure the dramatic invasions of privacy worked by the surveillance.

These rules, which supposedly protect the privacy of Americans swept up in the government's surveillance apparatus, are weak to start and riddled with exceptions. By default, they permit the government to keep virtually *all* communications collected under PRISM for as long as five years. During that time, agents can search and review the emails of foreigners and Americans alike without meaningful restriction. Beyond this initial five-year period, the minimization procedures explicitly permit the government to retain and disseminate Americans'

international communications for almost a dozen reasons, including when it determines that the communications contain "significant foreign intelligence information" or "evidence of a crime." *See, e.g.*, Minimization Procedures Used by the NSA in Connection with Section 702 (2016), §§ 3(b)(1), 3(c)(1), 5(1)-(2), 6(a)(2), 6(b).[13] The procedures do not require any judicial approval—or even high-level executive-branch approval—before agents can go looking for an American's private emails or phone calls. PCLOB Report 58-59 (discussing FBI procedures).

The FISC's review of the targeting and minimization procedures does not remedy their deficiencies. As the FISC itself has noted, its review under the statute is "narrowly circumscribed" and is conducted only once a year.[14] Those proceedings are typically one-sided and, by the FISC's own description, have been plagued by an "institutional lack of candor" by the government.[15]

* * *

Finally, a number of basic facts bearing on the surveillance in this case remain unknown, including the manner in which the government used and queried Mr. Hasbajrami's communications in its investigation. At a minimum, amici urge the Court to require the government to conduct a declassification review of the

[13] https://perma.cc/C6TY-ET5Z.

[14] *In re Proceedings Required by § 702(i) of FISA Amendments Act*, Misc. No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008).

[15] [*Redacted*], No. [Redacted], at 19 (FISC Apr. 26, 2017), https://perma.cc/7X2S-VAS7 ("April 26, 2017 FISC Op.").

underlying facts, as the Ninth Circuit did in *Mohamud*; and further urge the Court to allow supplemental briefing as necessary to ensure informed, adversarial litigation.[16]

ARGUMENT

Under the Fourth Amendment, Americans have a protected privacy interest in the contents of their communications, including their telephone calls and emails. *See United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 313 (1972); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). The government therefore needs a warrant to search and seize these communications. Searches conducted without a warrant are "per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967).

Section 702 does not require the government to obtain a warrant based on probable cause prior to collecting the communications of Americans, nor does it impose any comparable requirement after the fact. The government's collection and use of these communications is therefore presumptively unconstitutional. Moreover, no exception to the warrant requirement exists that could justify such a sweeping program. Finally, even if an exception to the warrant requirement

[16] *See* Order, *United States v. Mohamud*, No. 14-30217 (9th Cir. Sept. 2, 2016) (ECF 109-1).

applied, surveillance of Americans under Section 702 is unreasonable and therefore unconstitutional.

I. Section 702 permits surveillance of Americans' international communications in vast quantities and in violation of the warrant requirement.

The Fourth Amendment requires that search warrants be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The Supreme Court has interpreted these words to require three things: (1) that any warrant be issued by a neutral, disinterested magistrate; (2) that the government demonstrate probable cause to believe that the evidence sought will aid in a particular apprehension or conviction; and (3) that any warrant particularly describe the things to be seized and the places to be searched. *See Dalia v. United States*, 441 U.S. 238, 255 (1979).

Surveillance under Section 702 is conducted without any of the familiar safeguards that a warrant provides. *See* Background, *supra*. It is therefore presumptively unconstitutional. *See Katz*, 389 U.S. at 357. Moreover, contrary to the district court's reasoning, none of the warrant requirement's "jealously and carefully drawn" exceptions apply to the surveillance at issue here. *Jones v. United States*, 357 U.S. 493, 499 (1958). Regardless of whether the warrant requirement

applies to the communications of foreigners overseas, it unquestionably reaches the communications of U.S. persons on U.S. soil.

Accordingly, the government must, at a minimum, obtain a warrant when it deliberately seeks to use or search for the communications of Americans like Mr. Hasbajrami. Especially in the context of electronic searches, courts and Congress have frequently required the government to obtain a warrant after its initial seizure or search. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473 (2014) (requiring government to obtain a warrant before searching cell phone lawfully seized incident to arrest); 50 U.S.C. § 1801(h)(4) (requiring government to obtain a warrant within 72 hours of intercepting U.S. person's communications); *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) (requiring government to obtain a warrant before conducting new search of lawfully seized computer hard-drive).

A. The government must obtain a warrant to use and search Americans' communications regardless of whether it is "targeting" foreigners.

The district court held that incidental collection of a U.S. person's communications during surveillance targeting non-U.S. persons abroad did not implicate the warrant clause at all. A.84. But the rule the district court cited—sometimes called the "incidental overhear" rule—has no application here.

1. The government's use of the term "incidental" conveys the impression that its collection of Americans' communications under Section 702 is a *de minimis* or unintended byproduct, common to all forms of surveillance. In reality, however, the warrantless surveillance of Americans' communications under Section 702 was both the purpose and the direct result of the statute.[17] Moreover, the *volume* of communications intercepted "incidentally" under Section 702 dwarfs that of communications intercepted incidentally under the original provisions of FISA or Title III.[18]

2. The district court relied on the "incidental overhear" rule to hold that so long as the government claims to be targeting foreigners, it may read and listen in on the private communications of Americans without a warrant. But contrary to the district court's analysis, A.84-85, the "incidental overhear" cases do not establish an exception to the warrant requirement. The formative cases establishing this rule apply it only when the government has *sought and obtained* a valid warrant. *See, e.g.*, *United States v. Kahn*, 415 U.S. 143 (1974); *United States v. Donovan*, 429 U.S. 413, 418 (1977); *United States v. Figueroa*, 757 F.2d 466, 471 (2d Cir. 1985);

---

[17] *See* PCLOB Report 82, 86-87 ("Such 'incidental' collection of communications is not accidental, nor is it inadvertent").

[18] *See, e.g.*, President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* 149 (2013), https://perma.cc/9LYQ-DVJL ("PRG Report") ("incidental interception is significantly more likely to occur when the interception takes place under section 702 than in other circumstances").

United States v. Martin, 599 F.2d 880, 884-85 (9th Cir. 1979). Far from announcing an exception to the warrant requirement, these cases honor it.[19]

Indeed, the district court, as well as the Ninth Circuit in *Mohamud*, ignored the rationale for the incidental overhear rule, which is inextricably tied to the specific nature and function of a warrant. *See* A.85; *United States v. Mohamud*, 843 F.3d 420, 439-41 (9th Cir. 2016). The warrant process requires courts to carefully circumscribe surveillance, confining it to conversations that constitute evidence of a particular crime and limiting the intrusion as to both the target and any person with whom the target communicates. Thus, when the government has established probable cause to seize certain communications—and has thereby satisfied the necessary Fourth Amendment threshold—its warrant satisfies the privacy interests of all parties to the communications, including parties who are incidentally overheard. *See Figueroa*, 757 F.2d at 471. Because of this, the incidental overhear cases simply stand for the proposition that the government need not obtain *multiple* warrants to intercept protected communications. *See Kahn*, 415 U.S. at 153. By contrast, the "complete absence of prior judicial authorization would make an [incidental] intercept unlawful." *Donovan*, 429 U.S. at 436 n.24.

[19] *See* Elizabeth Goitein, *The Ninth Circuit's Constitutional Detour in* Mohamud, Just Security (Dec. 8, 2016), https://goo.gl/G8wT3X.

The surveillance in this case—like all Section 702 surveillance—did not involve a warrant. There was no showing of probable cause; there was no individualized judicial review; and there was no attempt at particularity. That the government's "target" was not a U.S. person may be sufficient to allow the government to warrantlessly surveil *that* person. But the Fourth Amendment's protection is nowhere limited to "targets."[20] Even if the government claims to be targeting someone who lacks Fourth Amendment rights, it is not entitled to ignore the rights of a U.S. person who *is* entitled to that protection.

3. The Supreme Court's ruling in *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), does not authorize the warrantless surveillance of Americans like Mr. Hasbajrami on U.S. soil.

Verdugo-Urquidez involved a search of physical property located in Mexico and belonging to a Mexican national, in circumstances where no U.S. court had authority to issue a warrant. *See id.* at 261-62, 274. *Verdugo-Urquidez* was solely concerned with the warrant requirement's application *abroad*. The search was conducted on *foreign* soil; the privacy interests at stake were exclusively those of a *foreign* national; and the subject of the search was, until his arrest, located *abroad*.

The search of Mr. Hasbajrami's communications has nothing in common with *Verdugo-Urquidez*.

[20] *See* Orin Kerr, *The Surprisingly Weak Reasoning of* Mohamud, Lawfare (Dec. 23, 2016), https://www.lawfareblog.com/surprisingly-weak-reasoning-mohamud.

First, the search here took place inside the United States—and, as the Supreme Court made clear, that fact matters immensely. *See id.* at 278 (Kennedy, J., concurring) ("If the search had occurred in a residence within the United States, I have little doubt that the full protections of the Fourth Amendment would apply."); *id.* at 261-62, 264, 274-75 (plurality).

Second, Mr. Hasbajrami is a U.S. person, unlike the respondent in *Verdugo-Urquidez*. Thus, even if the government is correct that the Fourth Amendment does not protect foreigners abroad, Mr. Hasbajrami's case does not involve such a claim. What matters here is that the government acquired a communication to which a U.S. person was a party—a communication for which the Fourth Amendment unquestionably applies. Nothing in *Verdugo-Urquidez* suggests that the government may bootstrap away an American's right to privacy by "targeting" the foreign end.

Finally, longstanding historical practice confirms that *Verdugo-Urquidez*'s reasoning cannot be extended to the surveillance here. The government has consistently been required to obtain a warrant to search the private letters, phone calls, and emails of Americans—including their international communications—inside the United States. *See Ex parte Jackson*, 96 U.S. 727, 733 (1877); *see also United States v. Ramsey*, 431 U.S. 606, 623-24 (1977) (citing regulations requiring a warrant to read the contents of international letters on U.S. soil); 18 U.S.C.

§ 2518 (warrant required for interception of phone calls on U.S. soil); 50 U.S.C. § 1805 (similar). No basis exists to deviate from this tradition.

B. If there is a foreign-intelligence exception to the warrant requirement, it is not broad enough to render Section 702 constitutional.

The government has argued that the warrant requirement does not apply here because Section 702 surveillance serves a foreign-intelligence purpose and therefore falls within the "special needs" doctrine. *See* Gov't Mem. 44-49 (ECF No. 97). This is incorrect. Courts recognize an exception to the warrant requirement only "in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

The mere fact that the government conducts this surveillance to acquire foreign-intelligence information does not render the warrant and probable-cause requirements unworkable. In *Keith*, the Supreme Court expressly rejected the government's argument that intelligence needs justified dispensing with the warrant requirement in domestic surveillance cases. 407 U.S. at 316-21. That logic applies with equal force to surveillance directed at targets with a foreign nexus—at least when that surveillance sweeps up Americans' communications (as Section

702 surveillance does), and is conducted inside the United States (as Section 702 surveillance is).

The Supreme Court has never recognized a foreign-intelligence exception to the warrant requirement, nor has the Second Circuit. *See In re Terrorist Bombings*, 552 F.3d 157, 172 (2d Cir. 2008). But even if such an exception exists, it is not broad enough to render Section 702 surveillance constitutional. Courts have approved narrow modifications to the probable-cause requirement when considering individualized surveillance under FISA, but only where the surveillance in question was directed at foreign powers or their agents and predicated on an individualized finding of suspicion. *See, e.g.*, *United States v. Duggan*, 743 F.2d 59, 73-74 (2d Cir. 1984), *United States v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011); *In re Sealed Case*, 310 F.3d 717, 720 (FISCR 2002).

Section 702 contains no such limitations. The surveillance is not confined to "foreign powers or agents of foreign powers reasonably believed to be located outside the United States"—a limitation the FISCR deemed critical in *In re Directives*, 551 F.3d 1004, 1012-16 (FISCR 2008). Instead, under Section 702, the government may target any non-citizen outside the United States to acquire "foreign intelligence information," broadly defined. Moreover, where prior cases required a probable-cause determination by the President or Attorney General, under Section 702, targeting decisions have been handed off to an untold number

of government analysts. No court has ever recognized a foreign-intelligence exception sweeping enough to render constitutional the surveillance at issue here. *See* PCLOB Report 90 n.411.

While foreign-intelligence gathering is unquestionably a government interest of the highest order, it does not exempt surveillance of Americans from the warrant requirement.

II. Surveillance under Section 702 violates the Fourth Amendment's reasonableness requirement because it allows and encourages the warrantless exploitation of Americans' communications.

Even if the government is permitted to surveil foreigners without first obtaining a warrant, it is not entitled to completely bypass the Fourth Amendment rights of Americans like Mr. Hasbajrami. Rather, the government's reasoning would justify, at most, the warrantless acquisition of foreign-to-foreign communications, in which it says no Fourth Amendment interests are implicated. But instead the government seeks a windfall: the ability to retain, use, and deliberately query its massive Section 702 databases for the emails of known U.S. persons, without ever satisfying bedrock Fourth Amendment requirements. Regardless of whether the warrant requirement applies, "the ultimate touchstone of the Fourth Amendment is reasonableness," *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006), and the government's purposeful exploitation of Americans' communications in this manner is unreasonable. To the extent the government

claims it is unable to avoid acquiring Americans' communications in the first place, reasonableness requires that it provide comparable Fourth Amendment protection to Americans after the fact. Because Section 702 lacks any such post-seizure limitations, the surveillance of Mr. Hasbajrami was unreasonable.

A. Section 702 surveillance lacks the core safeguards that courts require when assessing the reasonableness of electronic surveillance.

Under the Fourth Amendment, reasonableness is determined by examining the "totality of the circumstances" to "assess[], on the one hand, the degree to which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006). In the context of electronic surveillance, reasonableness requires that government eavesdropping be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions" of privacy. *Berger v. New York*, 388 U.S. 41, 58 (1967); *see United States v. Bobo*, 477 F.2d 974, 980 (4th Cir. 1973).

Courts assessing the lawfulness of electronic surveillance have looked to FISA and Title III as measures of reasonableness. *See, e.g.*, *United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986). While the limitations on foreign-intelligence surveillance may differ in some respects from those applicable to law-enforcement surveillance, "the closer [the challenged] procedures are to Title III

procedures, the lesser are [the] constitutional concerns." *In re Sealed Case*, 310 F.3d at 737.

Section 702 abandons three core safeguards—individualized judicial review, a finding of probable cause, and particularity—that courts have relied on to uphold the constitutionality of both FISA and Title III. *Duggan*, 743 F.2d at 73-74 (FISA); *In re Sealed Case*, 310 F.3d at 739-40 (FISA); *United States v. Tortorello*, 480 F.2d 764, 772-73 (2d Cir. 1973) (Title III).

First, Section 702 fails to interpose "the deliberate, impartial judgment of a judicial officer . . . between the citizen and the police." *Katz*, 389 U.S. at 357. The Fourth Amendment reflects a judgment that "[t]he right of privacy [is] too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals." *McDonald v. United States*, 335 U.S. 451, 455-56 (1948). But under Section 702, the FISC's role consists principally of reviewing targeting and minimization procedures. Every decision concerning specific surveillance targets is left to the discretion of executive-branch employees, even as these decisions affect countless Americans.

Second, Section 702 fails to condition surveillance on the existence of probable cause of any kind. It permits the government to conduct surveillance without proving to a court that the people it seeks to surveil are foreign agents, engaged in criminal activity, or connected—even remotely—with terrorism. 50

U.S.C. § 1881a(a). It permits the government to conduct surveillance without even an executive-branch determination that its targets fall into any of these categories.

Third, surveillance under Section 702 is not particularized. Instead, it permits the government to collect—wholesale and on an ongoing basis—all communications to and from more than one hundred thousand targets. The requirement of particularity "is especially great in the case of eavesdropping," which inevitably results in the interception of unrelated, intimate conversations. *Berger*, 388 U.S. at 56. Unlike Title III and FISA, however, Section 702 does not require the government to identify to any court the telephone lines, email addresses, or places at which its surveillance will be directed, or "the particular conversations to be seized." *Donovan*, 429 U.S. at 427 n.15.

The consequence of Section 702's failure to include any of these limitations is that government agents may target essentially any foreigner for surveillance—and may thereby collect the emails and phone calls of all U.S. persons communicating with those foreigners.

B. Section 702 surveillance lacks sufficient post-seizure restrictions to be reasonable under the Fourth Amendment.

The constitutionality of electronic surveillance regimes depends not just on limitations on initial collection but also on the restrictions on later retention and use. Because Section 702 is extremely permissive at the outset—allowing the broad, continuous collection of billions of communications—strong post-seizure

restrictions on the use of this information are critical to the Fourth Amendment analysis. In assessing such restrictions, the government's justification for its initial search matters. Where, as here, the government justifies warrantless surveillance by asserting that its foreign targets lack Fourth Amendment rights, its subsequent use and querying of *Americans'* communications without any individualized judicial approval is unreasonable. *See In re Directives*, 551 F.3d at 1015 (finding warrantless surveillance of foreigners reasonable only after the government represented that it was not amassing databases of Americans' incidentally collected communications). *See generally Terry v. Ohio*, 392 U.S. 1, 19 (1968) ("The scope of the search must be strictly tied to and justified by the circumstances which rendered its initiation permissible.").

Because of the "inherent dangers" and overbreadth of electronic searches, courts have long looked to post-seizure limitations when analyzing the reasonableness of surveillance. *Berger*, 388 U.S. at 60. For example, in *Berger*, the Supreme Court faulted New York's eavesdropping statute in part because it did not limit the surveillance to particular conversations, but instead permitted the retention and use of "any and all conversations" of the state's targets; it did not meaningfully constrain the duration of surveillance; and it did not provide for after-the-fact notice to those monitored. *See Berger*, 388 U.S. at 58-60.

Lower courts have similarly relied on strict post-seizure protections in finding electronic surveillance regimes reasonable. This Court upheld the constitutionality of Title III, relying on its provision of "particularity in the application and order, judicial supervision, and other protective procedures whose absence caused the Court to condemn the electronic surveillance in *Berger* and *Katz*." *Tortorello*, 480 F.2d at 772-73, 783-84; *accord Bobo*, 477 F.2d at 979. Likewise, courts considering the reasonableness of foreign-intelligence surveillance have relied on FISA's "minimization" procedures, which regulate how the government may retain, use, and disseminate the information it obtains. *See In re Sealed Case*, 310 F.3d at 740.[21] These cases reject the government's contention that wiretapping that is "lawful" at the moment of interception is somehow immune from the Fourth Amendment's continuing requirement of reasonableness. *See also, e.g.*, *Rodriguez v. United States*, 135 S. Ct. 1609, 1614-15 (2015) (traffic stop that was lawful when initiated violated Fourth Amendment when officer's investigation expanded beyond original justification); *Ferguson v. City of*

[21] In defending Section 702, it is not enough for the government to claim that Section 702's minimization procedures are "similar" to those under traditional FISA. Under traditional FISA, minimization operates as a *second* layer of protection against the retention, use, and dissemination of information relating to U.S. persons. The first layer of protection comes from the requirement of individualized judicial authorization for each surveillance target—a feature that Section 702 conspicuously lacks.

Charleston, 532 U.S. 67, 78 (2001) (observing that reasonableness of warrantless drug tests depended on protections against later dissemination of the results).

Strong post-seizure restrictions are especially critical under Section 702 given the breadth of the collection and the absence of traditional Fourth Amendment safeguards at the outset. *See* Section II.A, *supra*. Here, they would also answer one of the government's principal objections: that it would be impractical to obtain a warrant beforehand, because it cannot know whether surveillance directed at a given foreigner will sweep up protected communications involving Americans.[22] Gov't Mem. 42-43. But that fact—even if true in some instances—does not excuse the government from obtaining individualized judicial approval when it later seeks to use communications that it knows *are* protected. At the very least, reasonableness requires the provision of safeguards for Americans after the fact.[23]

Indeed, both Congress and courts—including this Court—have often dealt with similar overbreadth or overseizure problems, especially when confronted with broad seizures of digital information. In response, they have imposed rules to

[22] This premise is itself flawed. For example, when the government intercepts telephone calls with one end in the United States, it is well aware that its surveillance captures the private conversations of Americans.

[23] *See* Peter Swire & Richard Clarke, *Reform Section 702 to Maintain Fourth Amendment Principles*, Lawfare (Oct. 19, 2017), https://goo.gl/RHqdND; Geoffrey Stone & Michael Morell, *The One Change We Need to Surveillance Law*, Wash. Post (Oct. 9, 2017), http://wapo.st/2hZ1xJx.

ensure that the government's *use* of seized data does not exceed its Fourth Amendment authority. These rules routinely require the government either to refrain from using information beyond the scope of its legal authority or to secure additional court authorization after the fact.

For instance, in the case of traditional FISA surveillance, Congress imposed strict minimization rules to ensure that *warrantless* surveillance directed exclusively at foreign powers—for example, surveillance of foreign embassies—does not intrude upon the rights of U.S. persons swept up in that surveillance. *See* 50 U.S.C. §§ 1801(h)(4), 1802(a)(1). If the government learns after that fact that it has collected an American's communications without a warrant, it is required to destroy the protected communications within 72 hours or to obtain an individualized FISC order to retain them. *Id.* § 1801(h)(4). Because this surveillance is warrantless and targeted at foreign powers, it is closely analogous to that conducted under Section 702.

In the case of warrantless surveillance conducted under Section 702's predecessor statute, the Protect America Act, the FISCR held the surveillance reasonable only after finding that the government was *not* amassing a searchable database of Americans' incidentally collected communications. *See In re Directives*, 551 F.3d at 1015. Similarly, the FISC prohibited the NSA from

conducting backdoor searches of its Section 702 databases for years—an after-the-fact restriction designed to protect Americans' privacy.[24]

In the case of computer hard-drive searches, where data is often intermingled, this Court has also recognized the importance of post-seizure restrictions. Even when the government lawfully seizes the *full* contents of a device pursuant to a warrant, it may only search for the particular information authorized by its original probable-cause warrant—at least not without further court authorization. *See United States v. Galpin*, 720 F.3d 436, 446-47 (2d Cir. 2013); *Sedaghaty*, 728 F.3d at 913.

In each of these instances, either courts or Congress have imposed workable solutions, in order to ensure that the government's electronic searches are properly confined. Similarly here, the mere fact that the government is "targeting" foreigners when it acquires Americans' protected communications is not a valid reason to jettison the safeguards that would otherwise be afforded by a warrant.

While post-seizure restrictions could adequately protect the rights of Americans under Section 702, the current procedures do the opposite. They allow the government to collect Americans' communications on U.S. soil without a

[24] The NSA was prohibited from conducting backdoor searches on communications acquired through PRISM until 2011, and on communications acquired through Upstream until 2017. *See* James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US citizens' Emails and Phone Calls*, Guardian (Aug. 9, 2013), https://goo.gl/DDg2zZ; April 26, 2017 FISC Op. at 28.

warrant. They allow the government to retain those communications for five years by default—and to pool them in massive centralized databases. And they allow agents to conduct queries that deliberately target Americans' communications after they are collected, including for use in ordinary criminal investigations. PCLOB Report 55-60. In short, the procedures authorize the very type of intrusion that the Fourth Amendment was designed to guard against.

C. The government has reasonable alternatives that would allow it to collect foreign intelligence while protecting Americans' communications.

The government has reasonable alternatives at its disposal. Compliance with the Fourth Amendment requires at least one of two things: that the government avoid warrantless *acquisition* of Americans' communications where it is reasonably possible to do so; or that it obtain judicial approval to *search for* or *use* Americans' communications when it has collected them warrantlessly. There is no practical reason why these limitations—which have the effect of requiring safeguards only for Americans' communications—could not be imposed here.

Indeed, a number of proposals would permit the government to continue collecting foreign-to-foreign communications while providing additional protections for communications involving Americans. During the debate that preceded Section 702, then-Senator Barack Obama co-sponsored an amendment that would have prohibited the government from (1) acquiring a communication

without a warrant if it knew "before or at the time of acquisition that the communication [was] to or from a person reasonably believed to be located in the United States," and (2) accessing Americans' communications collected under Section 702 without a warrant. *See* S.A. 3979, 110th Cong. (2008), 154 Cong. Rec. S607-08 (daily ed. Feb. 4, 2008). More recently, the President's Review Group concluded that a warrant requirement should be imposed, and the House of Representatives passed a bill that would prohibit the retention and use of Americans' communications. *See* PRG Report 28-29; H.R. 4870, 113th Cong. § 8127 (2014).

The government argued below that complying with the warrant requirement would be unworkable because "imposition of a warrant requirement for any incidental interception of U.S. person communications would effectively require a warrant for all foreign-intelligence collection." Gov't Mem. 43. Not so. The Fourth Amendment does not require the government to obtain prior judicial authorization for surveillance of foreign targets merely because those foreign targets might communicate with U.S. persons. Rather, the Fourth Amendment requires the government to take reasonable steps to avoid the warrantless interception, retention, and use of Americans' communications. Section 702 surveillance lacks even basic protections that would prevent these warrantless intrusions. As a consequence, it is unreasonable.

CONCLUSION

For the foregoing reasons, the Court should hold that the surveillance of Mr. Hasbajrami violated the Fourth Amendment.

Dated: October 23, 2017

Respectfully submitted,

/s/ Patrick Toomey

Patrick Toomey
Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993
mark@eff.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS,
AND TYPE-STYLE REQUIREMENTS

Pursuant to Fed. R. App. P. 29(a)(4)(G), I certify as follows:

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and 32(a)(7)(B) because this brief contains 6,499 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. 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 2010 in 14-point Times New Roman font.

Dated: October 23, 2017

/s/ Patrick Toomey
Patrick Toomey
Counsel for Amici Curiae