No. 17-5126

IN THE

Supreme Court of the United States

MOHAMED OSMAN MOHAMUD,

Petitioner,

v.

UNITED STATES,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, CENTER FOR DEMOCRACY & TECHNOLOGY, AND NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE IN SUPPORT OF PETITIONER

ANDREW CROCKER
Counsel of Record
MARK RUMOLD
JAMIE WILLIAMS
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
andrew@eff.org

Counsel for Amici Curiae

274755

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

Cases

Cited Authorities

Page

Cited Authorities

Statutes

Page

Other Authorities

Cited Authorities

Page

Page

STATEMENT OF INTEREST[1]

Amici the Electronic Frontier Foundation, the Center for Democracy & Technology, and New America's Open Technology Institute are non-profit organizations working on issues related to civil liberties and technology. Representing the interests of technology users in the courts and through legislative and policy advocacy, amici ensure that constitutional rights keep pace with changes in law and technology. Their individual organizational statements are contained in the Appendix following this brief.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

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 Section 702 of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881a, the Government annually intercepts billions of international communications sent by hundreds of thousands of individuals, including Americans. It conducts this surveillance inside the United States with advisory approval of Article III judges, all without a warrant or anything resembling one.

---

1. As Supreme Court Rule 37.2(a) requires, amici have provided timely notice to all counsel, and all parties consent to the filing of this brief. As Supreme Court Rule 37.6 requires, amici state that this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than amici or their counsel made a monetary contribution to fund this brief's preparation or filing.

This warrantless surveillance of Americans violates the Fourth Amendment, and the advisory role imposed on the Judiciary by Section 702 violates Article III.

The Ninth Circuit's decision in this case disregarded these significant constitutional defects. Instead, the court invented a dangerous—and doctrinally unprecedented—exception to the warrant requirement. And it gave short shrift to the novel role Section 702 imposes on the Judiciary.

Section 702's constitutional infirmities have affected millions of individuals, including countless Americans, over almost a decade of surveillance conducted under the statute. Accordingly, amici urge the Court to grant certiorari in order to resolve the significant constitutional issues presented by this case.

ARGUMENT

I. Under Section 702, the Government conducts warrantless surveillance of billions of international communications, including the communications of Americans.

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 ("FAA"), 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) (internal citations omitted). Where the initial statutory regime for conducting foreign intelligence surveillance in the United States, the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, allowed for targeted surveillance with significant judicial involvement, Section 702 permits the FISC to review broad, programmatic guidelines that the Government intends to use when conducting surveillance in the future. This surveillance is carried out inside the United States with the cooperation of major American telecommunication and Internet companies.[2] Surveillance conducted under Section 702 reaches every form of modern electronic communication: telephone calls, emails, video calls, texts, and online chats, among others.[3]

---

2. The Government conducts Section 702 surveillance in one of two ways. First, it compels third-party Internet service providers, such as Google, Yahoo, and Facebook, to turn over the communications of its customers through a program commonly known as PRISM. Second, the government cooperates with telecommunication companies, like AT&T and Verizon, to intercept communications in real-time as they flow through the nation's fiber-optic Internet backbone cables. All of this surveillance occurs within the United States. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), 7, https://www.pclob.gov/library/702-report.pdf (hereafter "PCLOB Report").

3. *See* NSA Slides Explain the PRISM Data-Collection Program, Wash. Post. (Jun. 6, 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

Three aspects of Section 702 surveillance distinguish it from previous foreign intelligence surveillance practices. Section 702 surveillance is alarmingly vast. It purposefully sweeps up the communications of Americans without a warrant. And the statute mandates only programmatic judicial review, detached from the specifics of any particular surveillance application or target.

1. Section 702 surveillance is breathtaking in its scope. Annually, the Government's surveillance encompasses tens of thousands of "targets" and sweeps in billions of electronic communications, including Americans' communications.

The latitude afforded by the statute drives this sweeping breadth. Section 702 permits the Attorney General and the Director of National Intelligence to authorize "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. *See id.*; 50 U.S.C. § 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

4. Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities for Calendar Year 2016* (Apr. 2017), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016.

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]

Although a "substantial number of persons" are targeted under Section 702,[8] the number of "targets" belies the true scope of the surveillance. A review of a "large cache of intercepted conversations" analyzed by the *Washington Post* 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."[9] The material reviewed by the *Post* consisted of 160,000 intercepted e-mail and instant message conversations, 7,900 documents—including "medical records sent from one family member to another,

---

5. Although the government has not released the number of targets from 2011, internal NSA documents show that approximately 35,000 "unique selectors" were surveilled under PRISM in 2011. *See* Glenn Greenwald, *No Place to Hide*, at 111 (2014), http://glenngreenwald.net/pdf/NoPlaceToHide-Documents-Compressed.pdf (documents referenced in book).

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

7. *See* PCLOB Report at 116 (noting the "current number is much higher" than the 2011 count).

8. PCLOB Report at 33.

9. Barton Gellman, Julie Tate, and Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post (Jul. 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

resumes from job hunters and academic transcripts of schoolchildren"—and more than 5,000 private photos.[10] In all, the cache revealed the "daily lives of more than 10,000 account holders who were not targeted [but were] catalogued and recorded nevertheless."[11] The *Post* estimated that, at the Government's rate of "targeting," annual collection under Section 702 would encompass more than 900,000 user accounts.[12]

The volume of communications intercepted is far too great for the Government to review—let alone use—every communication it obtains. Many are never viewed by human eyes and simply reside in vast databases of intercepted communications.[13] The Government thus casts its international surveillance net widely, collecting far more information than it can ever process or use.

2. This vast surveillance apparatus inevitably—and intentionally—sweeps in the communications of Americans. 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

10. *Id.*

11. *Id.*

12. *Id.*

13. PCLOB Report at 128–29.

protection."[14] Indeed, this is one of the principal aims of the surveillance.[15]

Although nominally targeted at those overseas,[16] each time a U.S. person communicates with any one of the Government's self-selected targets—targets that 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 to count, or even estimate, the "substantial quantity" of U.S. persons' communications it collects under Section 702.[17] By all accounts, however, the volume is significant.

Not only are Americans' communications collected in substantial quantities under Section 702, they

---

14. Memorandum Opinion, [*Redacted*], (FISC Aug. 30, 2013), ("August 30 FISC Order") at 24, https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2003%2006.13.17%20--%20REDACTED.PDF.

15. *See* FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary, 109th Cong. at 9 (2006), http://1.usa.gov/1kbgHm3 (statement of NSA Director Michael Hayden).

16. While Section 702 indisputably allows for the collection of Americans' communications, the statute prohibits the *intentionally* targeting specific U.S. persons for surveillance under the statute. *See* 50 U.S.C. § 1881c(a)(2).

17. Dustin Volz, *White House, Intel Chiefs Want to Make Digital Spying Law Permanent*, Reuters (Jun. 7, 2017), https://www.reuters.com/article/us-usa-intelligence-idUSKBN18Y21E.

are also retained and used in later investigations—including domestic criminal investigations unrelated to the foreign intelligence purpose for which they were ostensibly collected. Collected communications are stored in databases, generally for a period of three to five years.[18] The Government then searches these vast databases of collected communications—at times, using Americans' email addresses or other identifiers to target particular Americans. These "secondary" (or "backdoor") searches allow the Government to target and read the communications of Americans without obtaining a warrant or any specific judicial authorization.[19]

3. The FISC plays a singular but limited role in overseeing this surveillance—one fundamentally unlike courts' roles in approving search warrants or authorizing surveillance under FISA or Title III, 18 U.S.C. §§ 2510-22.

As the FISC itself has noted, its review under Section 702 is "narrowly circumscribed."[20] Unlike traditional FISA surveillance, the Government is not required to demonstrate probable cause that the target is a foreign power or an agent of a foreign power. *Compare* 50 U.S.C. § 1805(a)(2), *with* 50 U.S.C. § 1881a. Section 702 does not require the Government to tell the FISC the nature or location of its targets. *See* 50 U.S.C. § 1881a. Nor does it require the Government to identify to the FISC the

18. PCLOB Report at 59.

19. PCLOB Report at 55–60.

20. *See In re Proceedings Required by § 702(I) of the FISA Amendments Act of 2008*, Misc. No. 08-01, 2008 WL 9487946, at *2 (FISC Aug. 27, 2008).

particular facilities or places at which the electronic surveillance will occur. *Id.*

Rather, on an annual basis, the Government submits to the FISC the guidelines it will follow—in the form of targeting and minimization procedures, 50 U.S.C. § 1881a(d),(e)—to conduct surveillance for up to one year. *Id*. These procedures form only the general framework of the surveillance program—*i.e.*, the rules executive branch employees will employ when making future surveillance targeting and retention decisions—and are wholly divorced from any specific application or target. *See id.* The FISC reviews these "procedures and guidelines" for compliance with the statute and the Fourth Amendment. 50 U.S.C. § 1881a(g)(2)(iv).

Section 702 thus transformed the FISC "into a 'metaarbiter,' approving generally applicable targeting and minimization procedures" to apply in future surveillance decisions, a far cry from Tile I of FISA "and the recommendations of the Church Committee."[21]

II. The constitutionality of surveillance conducted under Section 702 is a question of exceptional importance.

Certiorari is appropriate in cases, like this one, where "important constitutional issues [are] presented." *Heffron v. Int'l Society for Krishna Consciousness*, 452 U.S. 640,

21. Walter F. Mondale, Robert A. Stein, Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 100 Minn. L. Rev. 2251, 2267, 2276 (June 2016) (emphasis in original).

646 (1981); *accord* Supreme Ct. R. 10(c). Surveillance carried out under Section 702 strikes at the heart of the Fourth Amendment's prohibition on unreasonable searches and seizures, and the FISC's limited and advisory role in the process violates Article III.

The Fourth Amendment violations worked by Section 702 against an untold number of Americans cast a pall on international communications and the "vast democratic forums of the Internet." *Packingham v. North Carolina*, 580 U.S. ___, 137 S. Ct. 1730, 1735 (2017). These violations are carried out with the imprimatur of the Judiciary, despite the FISC's statutorily limited role.

These are critical constitutional issues requiring this Court's review.

A. Section 702 surveillance violates the Fourth Amendment.

Under the Fourth Amendment, U.S. persons have a protected privacy interest in the contents of their communications, including telephone calls and emails. *See Katz v. United States*, 389 U.S. 347, 353 (1967); *United States v. United States District Court (Keith)*, 407 U.S. 297, 313 (1972); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). A warrant is therefore required to search and seize these communications, and warrantless searches are "per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Katz*, 389 U.S. at 357.

Section 702 does not require the Government to obtain a warrant based on probable cause. Nor can the

Government point to a valid exception to the warrant requirement that could justify such a sweeping program. Taken as a whole, surveillance of U.S. persons under Section 702 is unreasonable and therefore unconstitutional.

1. Surveillance under Section 702 is conducted without many of the familiar safeguards that a warrant provides.

First, Section 702 fails to interpose "the deliberate, impartial judgment of a judicial officer . . . between the citizen and the police." *Id.* (citation and internal quotation marks omitted). 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 is limited to reviewing general targeting and minimization procedures. Every decision relevant to specific surveillance targets is left to the unreviewed discretion of executive branch employees, even as these decisions determine privacy protections for countless U.S. persons.

Second, Section 702 fails to condition surveillance on the existence of probable cause. It permits the Government to conduct acquisitions without proving to a court that its surveillance targets are foreign agents, engaged in criminal activity, or connected—even remotely—with terrorism. *Compare* 50 U.S.C. § 1881a *with* 18 U.S.C. § 2518 (3) (Title III), 50 U.S.C. § 1805(a)(2) (FISA). It permits the Government to conduct acquisitions without even an administrative determination that its targets fall into any of these categories.

Third, Section 702 fails to restrict the Government's surveillance to instances described with particularity. The requirement of particularity "is especially great in the case of eavesdropping," which inevitably results in the interception of unrelated, intimate conversations. *Berger v. New York*, 388 U.S. 41, 56 (1967). Unlike Title III and FISA, however, Section 702 does not require the Government to identify to any court the individuals to be monitored; the facilities, telephone lines, email addresses, or places at which its surveillance will be directed; or "the particular conversations to be seized." *United States v. Donovan*, 429 U.S. 413, 427 n.15 (1977). Section 702 does nothing to ensure that surveillance conducted under the Act "will be carefully tailored." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

2. Nothing about Section 702 renders the warrant clause inapplicable to the Government's interception of Americans' communications.

This Court has recognized an exception to the warrant requirement for programmatic searches "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). But in *Keith*, this 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. The Court's logic applies with equal force to surveillance directed at targets with a foreign nexus—at least when that surveillance sweeps up U.S. persons' communications (as Section 702 surveillance does), and is conducted inside

the United States (as Section 702 surveillance is). The mere fact that this surveillance is conducted to acquire foreign intelligence information does not render the warrant and probable-cause requirements unworkable.

Even if a foreign intelligence exception to the warrant requirement exists—a question this Court has never decided, *see United States v. Truong*, 629 F.2d 908, 913 (4th Cir. 1980)—the exception is not broad enough to render Section 702 surveillance constitutional. Lower 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.*, *Truong*, 629 F.2d at 913; *United States v. Cavanagh*, 807 F.2d 787, 790–91 (9th Cir. 1987); *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 limited to foreign powers or agents of foreign powers, but may target any non-citizen outside the United States. And all targeting decisions are handed off to an untold number of Government intelligence 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; *see also In re Directives*, 551 F.3d 1004, 1013–16 (FISCR 2008).

3. Even if the warrant clause were inapplicable, Section 702 surveillance would still be unconstitutional because it is unreasonable.

"The ultimate touchstone of the Fourth Amendment is reasonableness," and the reasonableness requirement applies even where the warrant requirement does not. *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006). 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) (internal quotation marks omitted).

To be reasonable, electronic surveillance must be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions" of privacy. *Berger*, 388 U.S. at 58 (internal quotation marks omitted). 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) (video surveillance); *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992).

Section 702 surveillance lacks the indicia of reasonableness these statutes possess. It abandons the Warrant Clause's core requirements—individualized suspicion, prior individualized judicial review, and particularity—thereby eliminating the primary bulwarks against general surveillance that courts have relied on to uphold the constitutionality of both FISA and Title III. *See, e.g.*, *Cavanagh*, 807 F.2d at 790 (FISA); *In re Sealed Case*, 310 F.3d at 739–40 (FISA); *United States v. Turner*, 528 F.2d 143, 158–59 (9th Cir. 1975) (Title III).

The targeting and minimization procedures adopted by the Government pursuant to Section 702 exacerbate these flaws by allowing collection, retention, and dissemination of U.S. persons' international communications in vast quantities. Indeed, the minimization procedures explicitly permit the Government to retain and disseminate U.S. persons' international communications for almost a dozen reasons, including when it determines that the communications contain "significant foreign intelligence information" or "evidence of a crime" and permit retention for as long as five years—even those U.S.-person communications that do not contain *any* foreign intelligence or evidence of a crime. *See* Minimization Procedures Used by the NSA in Connection with Acquisitions of Foreign Intelligence Information ("NSA Minimization Procedures"), §§ 3(b)(1), 3(c)(1); 5(1)–(2); 6(a)(2), 6(b).[22]

The minimization procedures also permit "backdoor searches," in which the Government searches its repository of Section 702-collected communications specifically for information about U.S. citizens and residents—like Mr. Mohamud—including for evidence of criminal activity. *See* PCLOB Report at 59; NSA Minimization Procedures § 3(b)(5). These queries are an end-run around the Fourth Amendment, converting sweeping warrantless surveillance directed at foreigners into a tool for investigating Americans in ordinary criminal investigations.

22. https://www.dni.gov/files/documents/icotr/51117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf.

B. Section 702 violates Article III.

Section 702 obligates the FISC to evaluate—on a programmatic basis—the statutory and constitutional validity of the procedures the Government intends to use to conduct surveillance. 50 U.S.C. § 1881a(i). The FISC's evaluation is largely divorced from the specifics of particular surveillance techniques or targets. It is nearly entirely secret and *ex parte*. And, with only limited exceptions, it is not subject to further adversarial testing or additional judicial scrutiny. Section 702 thus transforms and distorts the role of the Article III judges serving on the FISC in an unprecedented manner. That transformation violates Article III.

The federal judicial power is limited by Article III to "Cases" and "Controversies." *Mistretta v. United States*, 488 U.S. 361, 385 (1989). "Those two words confine the business of the federal courts to questions presented in an adversary context and in a form historically viewed as capable of resolution through the judicial process." *Massachusetts v. EPA*, 549 U.S. 497, 516 (2007) (internal quotation marks omitted).

Although not strictly adversarial, the issuance of search warrants by Article III courts is commonly seen as a proper exercise of the judicial power. *See Mistretta*, 488 U.S. at 389 n. 16; *Keith*, 407 U.S. at 317–18 ; *see also* James E. Pfander & Daniel D. Birk, *Article III Judicial Power, the Adverse-Party Requirement, and Non-Contentious Jurisdiction*, 124 Yale L.J. 1346, 1462–65 (2015).

In its original formulation, the FISC's role resembled this traditional judicial function. Under Title I of FISA,

the FISC is authorized to approve individual applications to conduct foreign intelligence surveillance. These applications require the FISC to evaluate, within specific factual contexts, whether probable cause exists to believe that targets of surveillance are foreign powers or their agents, and that the facilities to be monitored will be used by these targets. *See, e.g.*, 50 U.S.C. § 1805(a). The FISC thus issues warrant-like surveillance orders to conduct foreign intelligence surveillance of particular targets—much like Article III courts do under Title III. *See generally* 18 U.S.C. § 2518.

Still, the FISC's role under FISA's Title I presented a "difficult" Article III question, even for the Department of Justice. Elizabeth Gotein & Faiza Patel, *What Went Wrong with the FISA Court* ("*What Went Wrong*"), Brennan Center for Justice, 7, (Mar. 2015) (quoting DOJ testimony).[23] Ultimately, the Department concluded that, under FISA's original procedures, the FISC would be deciding a "case or controversy" because "what is to be determined is the United States' authority to conduct electronic surveillance of a *particular target*," and "[t]he judge is required under the bill to apply standards of law to the facts of a *particular case*." *Id.* at 31 (emphasis added) (internal quotation marks omitted); *accord In re Sealed Case*, 310 F.3d at 732 n. 19.

The FISC's role under Section 702 lacks these similarities to warrant procedure and instead represents a wholesale departure from traditional Article III practice. *See* Stephen Vladeck, *The FISA Court and Article III*, 72

23. https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The _FISA_Court.pdf.

Wash. & Lee L. Rev. 1161, 1169 n. 26 (2015). The FISC's review under Section 702 is divorced entirely from the specifics of any particular surveillance targets or cases—the primary factor that, in the Justice Department's view, saved the original FISA application process.

Rather than evaluating specific facts related to specific surveillance targets, the FISC instead reviews procedures the Government intends to use when making targeting and retention decisions for *future* surveillance. This preliminary review is more akin to "rendering an advisory opinion upon a statute or a declaratory judgment upon a hypothetical case," than traditional Article III practice of authorizing warrants or specific surveillance orders. *Watson v. Buck*, 313 U.S. 387, 402 (1941); *see also What Went Wrong* at 33 ("FISA Court judges simply don't know the specific activities that the procedures may authorize in any given case.").

Although Section 702 requires the FISC to review the contours of the Government's surveillance plan, these initial plans are often quite different than the surveillance the Government actually carries out in practice. Indeed, a series of declassified FISC decisions reveal systemic violations arising from surveillance carried out under FISC orders—surveillance that differed substantially from the surveillance the FISC authorized. *See, e.g.*, [*Redacted]*, 2011 WL 10945618, at *10, *11 n. 32 (basing ruling, in part, on conjecture because the FISC could not assess "for certain" how the Government's surveillance operated); August 30 FISC Order at 11 n. 7 (describing NSA failures to comply with FISC orders, resulting in "NSA's acquisition of communications falling outside the scope of Section 702"); *see also In re Production of Tangible Things from [Redacted]*, BR 08-13 (FISC Mar.

2, 2009) at 14 (describing government's "historical record of non-compliance" with FISC's orders).[24]

This, again, demonstrates the advisory and preliminary nature of the FISC's review: the court is obligated to "pass upon the possible significance of the manifold provisions of a broad" and complicated set of procedures "in advance of efforts to apply the separate provisions." *Watson*, 313 U.S. at 402.

III. The Ninth Circuit's decision was incorrect and could have far reaching consequences for the privacy of international communications.

Contrary to precedent from this Court, the Ninth Circuit created two novel Fourth Amendment rules to uphold the Government's warrantless searches of Americans' communications. The court also inexplicably avoided one of the most problematic uses of this surveillance in its decision. The combination of these errors creates a dangerous end-run around the Fourth Amendment with broad implications not just for foreign intelligence collection but also for ordinary criminal investigations.

A. The court improperly relied on the "incidental overhear" rule to create a new exception to the warrant requirement.

Although the surveillance in this case occurred on U.S. soil and although the Government indisputably searched the private emails of an American, the Ninth

24. https://www.aclu.org/files/assets/pub_March%202%202009%20Order%20from%20FISC.pdf.

Circuit held that the Fourth Amendment's warrant requirement did not apply. The court reasoned that because the Government's surveillance "target" was not entitled to the protection of a warrant, Mr. Mohamud forfeited that protection as well. *See* Pet. App. at 38-43.

But the rationale the panel relied on—often called the "incidental overhear" rule—is not an exception to the Fourth Amendment's warrant requirement. The formative cases establishing this rule apply it only when the Government has *already sought and obtained* a valid warrant. *See, e.g.*, *United States v. Kahn*, 415 U.S. 143 (1974); *Donovan*, 429 U.S. at 418; *United States v. Figueroa*, 757 F.2d 466 (2d Cir. 1985); *United States v. Martin*, 599 F.2d 880, 884–85 (9th Cir. 1979).

The Ninth Circuit ignored the underpinning of the incidental overhear rule, which is inextricably tied to the nature and function of a warrant. The warrant process requires courts to carefully circumscribe surveillance and limit Government intrusion into the privacy of those whose communications will be intercepted. As this Court has made clear, warrants not directed at a person or target in general are too broad; warrants must describe particular pieces of evidence, such as a particular category of communications on a particular phone line. *Berger*, 388 U.S. at 59 (invalidating eavesdropping statute requiring the Government to do "no more than identify the person whose constitutionally protected area is to be invaded"). When the Government has shown probable cause to seize 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. By contrast, the "complete absence of prior judicial authorization would make an [incidental] intercept unlawful." *Donovan*, 429 U.S. at 436 n.24.

As described above, the surveillance in this case—like all Section 702 surveillance—did not involve a warrant. That the Government's "target" was not a U.S. person is of no moment. The Fourth Amendment's protection is nowhere limited to "targets." Even if the Government claims to be targeting someone else who lacks Fourth Amendment rights, it is not entitled to ignore the rights of a U.S. person who *is* entitled to that protection.

The implications of this holding reach far beyond the national security context. Americans today engage in international Internet communications on a massive scale. Even seemingly "domestic" communications may be routed around the world, unbeknownst to the sender or recipient. *See* Sharon Goldberg, *Surveillance without Borders: The "Traffic Shaping" Loophole and Why it Matters*, The Century Foundation (June 22, 2017).[25] If the court's analysis stands, the Government could intercept any international communication without a warrant—including in criminal investigations—simply by "targeting" a party who lacked Fourth Amendment rights. *See* Orin Kerr, *The Surprisingly Weak Reasoning of* Mohamud, Lawfare (Dec. 23, 2016).[26] Indeed, the Government could theoretically collect *all* international communications for any purpose, so long as it claimed to be targeting the

25. https://tcf.org/content/report/surveillance-without-borders-the-traffic-shaping-loophole-and-why-it-matters/.

26. https://www.lawfareblog.com/surprisingly-weak-reasoning-mohamud.

foreigners on the other end of those communications—thereby "incidentally" and warrantlessly collecting Americans' private communications.

B. The court misapplied the third-party doctrine in conflict with this Court's precedent.

The Ninth Circuit's holding that the so-called third-party doctrine "diminished" Mr. Mohamud's expectation of privacy, Pet. App. at 46, is also untenable and squarely at odds with this Court's precedent.

As an initial matter, the third-party doctrine does not apply to the contents of private online communications that are not deliberately shared with a third party, such as the emails at issue here. Under the third-party doctrine, when information is deliberately shared with a third party or the public, an individual's expectation of privacy in that information is typically extinguished. *See, e.g.*, *Miller v. United States*, 425 U.S. 435, 443 (1976). But this doctrine has never been extended to the *contents* of private communications, and doing so would conflict with this Court's long-standing protection of communications that are carried by intermediaries like mail carriers and telephone providers. *See Ex Parte Jackson*, 96 U.S. 727, 723 (1877); *Katz*, 389 U.S. at 353; *see also Warshak*, 631 F.3d at 286-88.

More generally, the third-party doctrine does not result in a "*reduced* expectation of privacy," as the court held. Pet. App. at 46 (emphasis added). Properly understood, the doctrine either applies—and eliminates Fourth Amendment protection—or does not apply. Relatedly, the "third party" that the court pointed to was

not a third party at all, but simply the intended recipient of Mr. Mohamud's private communications. *Compare id.*, *with United States v. Graham*, 824 F.3d 421, 433 n.12 (4th Cir. 2016) (en banc). Virtually all private communications have at least two parties. When a person sends a private email, the mere act of clicking "send" does not eliminate or reduce any privacy interest. This reasoning would restrict Fourth Amendment protections for essentially *all* private communications—a result directly in conflict with this Court's decisions in *Katz* and *Ex Parte Jackson*.

C. The court ignored the Government's widespread use of "backdoor" searches to query and examine the communications of Americans including Mr. Mohamud.

The Government's practice of amassing U.S. person communications using Section 702 and then later searching through them—"backdoor" searching—is one of the most controversial aspects of this surveillance.[27] Yet, contrary to all evidence in the public record and without elaboration, the court abruptly concluded that the issue was not before it. *See* Pet. App. at 37.

All evidence suggests the Government used a secondary search to deliberately retrieve and examine Mr. Mohamud's private emails. According to the Privacy and Civil Liberties Oversight Board, "whenever the FBI opens a new national security investigation or assessment, FBI personnel will query previously acquired

27. *See* Sen. Ron Wyden, *Wyden Releases Details of Backdoor Searches of Americans' Communications* (June 30, 2014), http://bit.ly/2mizZQ1.

information from a variety of sources, including Section 702, for information relevant to the investigation or assessment." PCLOB Report at 59. That is precisely what FBI agents appear to have done here. The FBI agent who investigated Mr. Mohamud specifically testified that he began the investigation by running Mr. Mohamud's email address through "an FBI database"—one that apparently contained FISA information.[28] Ninth Cir. E.R. 5122–23. Second, unlike the Ninth Circuit's opinion, the district court directly addressed the lawfulness of secondary searches in a discussion titled "Querying After Acquisition" that spanned four pages. *See* Pet. App. at 103–06 (describing Mr. Mohamud's challenge to the secondary search as his "most persuasive argument"). The district court stated that it was a "very close question" whether such a search of a U.S. person's communications was constitutional. This entire discussion is inexplicable if the Government never conducted such a warrantless query of Mr. Mohamud's communications.

Above all, the court's failure to address this issue is significant because, as a result, its Fourth Amendment reasonableness analysis ignores one of the critical—and most *unreasonable*—ways in which the Government uses Section 702 surveillance as a backdoor into Americans' private communications.

---

28. The FBI has stated that its FISA and Section 702 databases are commingled and thus queried simultaneously. PCLOB Report at 59.

D. The court erred by concluding that Section 702 is consistent with Article III because it resembles review of search warrants and wiretap applications.

The Ninth Circuit, in a footnote, rejected Mr. Mohamud's Article III challenge. That conclusion was premised on two errors.

First, the panel concluded that the FISC's role is "similar to the review of search warrants and wiretap applications." Pet. App. at 49, n.28. As explained previously, that is incorrect: it ignores fundamental differences between the Judiciary's role in Section 702 and in search warrant or wiretap applications. *See* Section I, *supra*.

Second, the court erred in concluding that FISC review under Section 702 is not advisory because "the FISC either approves or denies the requested application." *Id*. That FISC review yields an approval (or denial) does not answer whether the issues it considers are a justiciable "case" or "controversy." Article III's prohibition on advisory opinions would be largely illusory if parties could avoid it by requesting a court explicitly approve or deny a requested course of conduct. Instead, the nature and posture of the question presented—not necessarily the outcome of that review—is paramount. *See United States v. Fruehauf*, 365 U.S. 146, 157 (1961) (Article III forbids "advance expressions of legal judgment" on "unfocused" issues that lack "clear concreteness"). Here, the "lessons taught by the particular" are lost when the FISC offers its preliminary judgment on the legality of future surveillance. *Sabri v. United States*, 541 U.S. 600, 609 (2004). That preliminary and advisory review violates Article III.

CONCLUSION

This case presents significant and unanswered constitutional questions that affect the privacy of every American's international communications. The Court should grant the petition to definitively resolve these significant issues.

Dated: August 9, 2017 Respectfully submitted,

ANDREW CROCKER
Counsel of Record
MARK RUMOLD
JAMIE WILLIAMS
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
andrew@eff.org

Counsel for Amici Curiae

APPENDIX

APPENDIX

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the digital world. With over 37,000 active donors and dues-paying members, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age. EFF has appeared before the federal courts, including the FISC, in multiple cases involving the Fourth Amendment and foreign-intelligence surveillance. EFF serves as counsel for plaintiffs in *Jewel v. NSA*, 08-4373 (N.D. Cal.), a case challenging the National Security Agency's "upstream" surveillance technique under Section 702. EFF filed amicus briefs in the district court and before the court of appeals in this case.

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization that advocates for individual rights in Internet law and policy. CDT represents the public's interest in an open, innovative, and decentralized Internet that promotes constitutional and democratic values of free expression, access to information, privacy, and individual liberty. CDT has played a leading role in advocating for legislative reform to the FISA Amendments Act.

New America's Open Technology Institute ("OTI") is New America's program dedicated to ensuring that all communities have equitable access to digital technology and its benefits, promoting universal access to communications technologies that are both open and

secure. New America is a Washington, DC based think tank and civic enterprise committed to renewing American politics, prosperity, and purpose in the Digital Age through big ideas, bridging the gap between technology and policy, and curating broad public conversation. Since 2014, OTI has advocated for reforms to foreign intelligence surveillance laws, including to Section 702 of the Foreign Intelligence Surveillance Act. OTI has written extensively about the scope and constitutionality of Section 702 and other foreign intelligence surveillance authorities.