NO. 14-30217

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF–APPELLEE,

v.

MOHAMED OSMAN MOHAMUD,

DEFENDANT–APPELLANT.

On Appeal from the United States District Court
for the District of Oregon
Case No. 3:10-cr-00475-KI-1
Honorable Garr M. King, Senior District Judge

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF OREGON, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT–APPELLANT'S PETITION FOR REHEARING OR REHEARING EN BANC

Counsel for Amici Curiae
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

Of Counsel
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

Of Counsel
Mathew W. dos Santos
AMERICAN CIVIL LIBERTIES UNION OF OREGON FOUNDATION
P.O. Box 40585
Portland, OR 97240
Phone: (503) 227-6928
MdosSantos@aclu-or.org

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.

Amici further state that 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.

Table of Contents

Table of Authorities

Cases

Statutes

Consitutional Provisions

Other Sources

Statements of Interest

This brief is filed pursuant to Ninth Circuit Rule 29-2(a) with the consent of all parties.

The American Civil Liberties Union ("ACLU") is a nonprofit, nonpartisan organization with more than one million members dedicated to the principles of liberty and equality embodied in the Constitution and this nation's laws. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other federal courts in numerous cases implicating Americans' right to privacy, including cases concerning foreign intelligence surveillance. The American Civil Liberties Union of Oregon is the Oregon affiliate of the ACLU.

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization that has worked to protect free speech and privacy rights in the digital world for 25 years. With roughly 36,000 donors, EFF represents the interests of technology users in court cases and policy debates surrounding the application of law in the digital age. EFF regularly participates as counsel or amicus in cases addressing the Fourth Amendment and electronic surveillance, including foreign intelligence surveillance.

Introduction

As the panel opinion acknowledged, under Section 702 of FISA, the government engages in warrantless surveillance of Americans on a remarkable scale—based on the theory that it is simply "targeting" foreigners who lack Fourth Amendment rights. The government makes extraordinary use of the resulting loophole: Having collected billions of communications under this authority, the government permits FBI agents and others to sift through its Section 702 databases when investigating Americans like Mr. Mohamud. At no point does the government obtain a warrant, or anything resembling a warrant, to examine the contents of these private communications—even when it is specifically searching for communications belonging to an American.

Under the Fourth Amendment, a warrantless search is per se unreasonable. But here, contrary to precedent, the panel's opinion embraced two novel rules to find the government's warrantless searches of Americans' communications lawful.

First, the panel's opinion improperly creates a new exception to the Fourth Amendment's warrant requirement. The panel relied on the "incidental overhear" rule to justify the warrantless search of Mr. Mohamud's private communications on U.S. soil, reasoning that because the government's intended "target" was not entitled to the protection of a warrant, Mr. Mohamud forfeited that protection as well. But, until now, the incidental overhear rule has never been recognized as an

exception to the warrant requirement. The Supreme Court's incidental overhear cases do not establish such an exception, and the panel's misreading of those cases would create a dangerous end-run around the warrant requirement—including in ordinary criminal investigations.

Second, the panel held that the third-party doctrine "diminished" Mr. Mohamud's expectation of privacy in his personal emails. However, this Court's precedent is clear that Americans have a reasonable expectation of privacy in the contents of their personal online communications and, accordingly, the third-party doctrine does not apply here. The panel's holding otherwise would diminish Fourth Amendment protections for essentially *all* private online communications—a result directly at odds with this Court's case law.

Finally, contrary to the available public record and the district court's opinion below, the panel inexplicably carved out of its decision one of the most problematic uses of this surveillance: the government's practice of intentionally searching its vast Section 702 databases for the communications of Americans like Mr. Mohamud. The panel's effort to sidestep this misuse of Section 702 was both factually unsupported and legally improper. The fact that the government is amassing Americans' communications, and then knowingly sifting through those protected emails in criminal investigations, bears directly on the reasonableness of the surveillance used in this case.

Given the scale of Section 702 surveillance, the panel's decision affects not just the defendant, but countless Americans who are subject to this surveillance yet have no opportunity to challenge it. More broadly, the panel's embrace of novel Fourth Amendment rules has significant implications for the privacy of Americans' communications in the digital age.

Background

In 2008, Congress substantially altered the FISA regime by enacting Section 702. Where FISA had, for three decades, generally required the government to show probable cause and obtain an individualized court order to conduct surveillance on U.S. soil, Section 702 authorizes warrantless surveillance of a wide swath of communications. *Compare* 50 U.S.C. § 1805, *with id.* § 1881a(a). The statute allows the government to seize international communications—including private communications sent or received by U.S. persons—from companies inside the United States, based on the "targeting" decisions of executive-branch employees. Section 702 permits this warrantless surveillance when two primary conditions are met: first, an analyst must reasonably believe that the "target" is a non-U.S. person located abroad; and second, a "significant purpose" of the surveillance must be to gather "foreign intelligence information"—a category that encompasses virtually any information bearing on the foreign affairs of the United States. *Id.* §§ 1881a(a), (g)(2)(v), 1801(e). As a result, under Section 702, the

government has substantial latitude to surveil non-U.S. persons abroad. It need not show that its targets are agents of foreign powers, much less that they are engaged in criminal activity or even remotely associated with terrorism.

No court approves the targets of this surveillance. Instead, the role of the Foreign Intelligence Surveillance Court ("FISC") consists principally of reviewing, on an annual basis, the executive branch's "targeting" and "minimization" procedures, which govern who may be targeted for surveillance by agency analysts and how communications are to be handled once intercepted. *Id.* § 1881a(i), (a).

In practice, the government relies on Section 702 to sweep up and store huge volumes of Americans' communications.[1] The government reported that in 2015, it monitored the communications of 94,368 targets under a single order issued by the FISC.[2] In 2011, Section 702 surveillance resulted in the collection of more than 250 million communications, a number that has likely grown significantly as the number of NSA targets has ballooned.[3] Every time a U.S. person communicates with any one of those targets—who may include journalists, academics, and human

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

[2] ODNI, 2015 Statistical Transparency Report at 5 (Apr. 30, 2016), http://bit.ly/1TmRuV0.

[3] *See [Redacted]*, 2011 WL 10945618, at *9-10 (FISC Oct. 3, 2011); Glenn Greenwald, *No Place to Hide* 111 (2014), http://bit.ly/24vaGYJ.

rights researchers—the government can collect, retain, and use that communication without a warrant.

Argument

I. The Court should grant rehearing or rehearing en banc to correct manifest errors in the panel's decision.

A. The panel decision 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 panel held that the Fourth Amendment's warrant requirement did not apply. The panel reasoned that because the government's surveillance "target" was not entitled to the protection of a warrant, Mr. Mohamud lost that protection as well. *See United States v. Mohamud*, 843 F.3d 420, 439-41 (9th Cir. 2016). However, the rationale the panel relied on—often called the "incidental overhear" rule—has never been recognized as an exception to the Fourth Amendment's warrant requirement.[4]

Under the Fourth Amendment, a warrantless search is "per se unreasonable," unless it is excused by one of a few carefully drawn exceptions. *Katz v. United States*, 389 U.S. 347, 357 (1967). Neither the Supreme Court nor this Court has recognized the incidental overhear rule as one of those exceptions. To the contrary,

[4] *See* Elizabeth Goitein, *The Ninth Circuit's Constitutional Detour in* Mohamud, Just Security (Dec. 8, 2016), https://www.justsecurity.org/35411/ninth-circuits-constitutional-detour-mohamud/.

the incidental overhear rule applies when the government has *already sought and obtained a warrant*—and has thus established probable cause to believe that certain communications will contain evidence of criminal activity. *See, e.g.*, *United States v. Kahn*, 415 U.S. 143 (1974).

Critically, the formative cases establishing this rule—which the panel cited as support for bypassing the warrant requirement—all involved court-issued warrants, a factor central to the reasoning of those cases. For example, in *United States v. Kahn*, the government obtained a Title III order to monitor the telephone communications of Irving Kahn and "others as yet unknown," based on a showing of probable cause that the wiretap would produce evidence of illegal gambling. *Id.* at 145-47. After agents overheard Kahn's wife, Minnie Kahn, discussing the same criminal activities on the same phone line, the Supreme Court held that the interception of her communications was lawful. Although she was incidentally overheard, her conversations fell within the original warrant permitting the government to acquire specific evidence of criminal activity. *Id.* at 154-55. The same is true of the Supreme Court's decision in *United States v. Donovan*, 429 U.S. 413 (1977), and this Court's decision in *United States v. Martin*, 599 F.2d 880 (9th Cir. 1979). In both cases, the government obtained a valid warrant to seize specific communications as evidence of criminal activity. *See also United States v. Figueroa*, 757 F.2d 466, 473 (2d Cir. 1985) (same). And that particularized

warrant was held to satisfy the Fourth Amendment rights of even those incidentally overheard. *See Martin*, 599 F.2d at 884-85.[5]

It is no accident that the cases cited by the panel were predicated on warrants. The logic of the incidental overhear rule is closely tied to the nature and function of a warrant. Through the warrant process, courts carefully circumscribe the government's surveillance and limit the intrusion into the privacy of those whose communications are intercepted. The resulting warrant is not directed at a person or target in general—that would be too broad, as the Supreme Court made clear in *Berger v. New York*, 388 U.S. 41, 59 (1967). Instead, it is directed at particular pieces of evidence, such as a specific category of communications on a particular phone line. *See id.* Because the government has shown probable cause to seize those 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 Donovan*, 429 U.S. at 436 n.24 (holding that while a warrant is not made unconstitutional by "failure to identify every individual who could be expected to

[5] The panel's reliance on *In re Directives*, 551 F.3d 1004, 1015 (FISCR 2008), was similarly misplaced. *See Mohamud*, 843 F.3d at 439. There, the Foreign Intelligence Surveillance Court of Review cited the incidental overhear rule only *after* holding that a "foreign intelligence exception" to the warrant requirement applied. *See* 551 F.3d at 1010-11. Unlike the panel decision, *In re Directives* nowhere suggests that the incidental overhear rule is itself an exception to the warrant requirement. *See id.* at 1015.

be overheard," the "complete absence of prior judicial authorization would make an intercept unlawful").

For these reasons, the incidental overhear rule is not an exception to the warrant requirement, as the panel opinion held, but rather the byproduct of a valid warrant.

Here, however, the government can point to no warrant. Section 702 surveillance is not based on a showing of probable cause. The surveillance does not involve individualized judicial review by a neutral magistrate. And the surveillance is not particularized, because the government purposely collects all of its targets' communications and retains them for at least five years. None of the basic prerequisites for lawfully invading an American's privacy are met. Yet the government, and the panel opinion, reason that the incidental overhear rule applies here too—and eliminates Americans' right to the protection of a warrant entirely.

That the government's "target" was not a U.S. person is of no moment in this case. The Fourth Amendment's protection is nowhere limited to "targets." Rather, the Fourth Amendment protects the right of the people "to be secure in their persons, houses, papers, and effects . . . ." U.S. Const. amend. IV.[6] There is

[6] Distinctions based on who is the "target" of surveillance are a creature of statute, not the Fourth Amendment. *See, e.g.*, 50 U.S.C. §§ 1801(f), 1881a(a)-(b). Fourth Amendment analysis typically avoids such subjective tests. *See Horton v. California*, 496 U.S. 128, 138 (1990).

no dispute that Mr. Mohamud is an American citizen, and that his private papers—here, his emails—are protected by the Fourth Amendment. Even if the government claims to be targeting someone who lacks Fourth Amendment rights, it is not entitled to ignore the warrant requirement when its surveillance implicates a U.S. person who plainly *is* entitled to that protection. Nothing in this Court's or the Supreme Court's decisions applying the incidental overhear rule permit the government to exploit the type of "mismatch" or constitutional loophole that the panel embraced here. To the extent that Americans' communications are intermingled with those of foreign targets, the government could readily seek after-the-fact judicial approval to use or access those protected communications, just as it does in other contexts. *See, e.g.*, 50 U.S.C. § 1801(h)(4) (requiring after-the-fact judicial approval to use or retain U.S. person communications); 18 U.S.C. § 2518(7) (same for emergency Title III surveillance). Instead, the government seeks an immense windfall.[7]

[7] Significantly, although the government labels its warrantless collection of Americans' communications merely "incidental," it is both foreseeable and deliberate. *See* PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* at 82, 86-87 (2014), http://bit.ly/1FJat9g ("PCLOB Report") ("Such 'incidental' collection of communications is not accidental, nor is it inadvertent"). Officials who advocated passage of Section 702 stated that their principal aim was to give the government broader authority to monitor Americans' international communications. *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).

The implications of the panel's novel reasoning are far-reaching and are not confined to the national-security context. Americans today engage in international internet communications on a massive scale—including email, web browsing, and online chats. Even seemingly "domestic" communications may be routed around the world, unbeknownst to the sender or recipient. If the panel's analysis were correct, the government could intercept any international communication without a warrant—including in criminal investigations—simply by "targeting" a party who lacked Fourth Amendment rights.[8] Indeed, the government could theoretically collect *all* international communications for any purpose, so long as it claimed to be targeting the foreigners on the other end of those communications—thereby "incidentally" and warrantlessly collecting the private communications of Americans. In other words, the panel's holding risks exposing the communications of countless Americans to warrantless surveillance.

B. The panel decision misapplied the third-party doctrine and is in conflict with this Court's precedent.

The panel's holding that the third-party doctrine "diminished" Mr. Mohamud's expectation of privacy is untenable and squarely at odds with this Court's precedent. *Mohamud*, 843 F.3d at 442. Although the panel acknowledged that private electronic communications retain the same Fourth Amendment

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

protection as letters, it concluded that "the communications at issue here had been sent to a third party, which reduces Mohamud's privacy interest at least somewhat." *Id.* For several reasons, this conclusion was in error.

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, the sender's expectation of privacy in that information is typically extinguished. *See, e.g.*, *Miller v. United States*, 425 U.S. 435, 443 (1976). Although courts have applied the third-party doctrine to certain kinds of email "metadata," such as the "to" and "from" fields of a message, this Court and others have repeatedly recognized that Americans have a reasonable expectation of privacy in the *contents* of their private emails. *See In re Grand Jury Subpoena* (*Kitzhaber*), 828 F.3d 1083, 1090-91 (9th Cir. 2016) (finding a reasonable expectation of privacy in personal emails); *United States v. Forrester*, 512 F.3d 500, 509, 511 (9th Cir. 2007); *United States v. Warshak*, 631 F.3d 266, 286-88 (6th Cir. 2010) ("[A] subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial [internet service provider ('ISP')]").

More generally, the third-party doctrine cannot result in a "*reduced* expectation of privacy," as the panel opinion held. *Mohamud*, 843 F.3d at 442

(emphasis added). Properly understood, the third-party doctrine either applies—and eliminates Fourth Amendment protection—or it does not apply. Here, the doctrine does not apply, as Mr. Mohamud has a fully protected privacy interest in his emails. *See, e.g.*, *Kitzhaber*, 828 F.3d at 1090-91; *Warshak*, 631 F.3d at 286-88.

Moreover, the "third party" that the panel pointed to is not a third party at all, but simply the intended recipient of Mr. Mohamud's private communications. *Compare Mohamud*, 843 F.3d at 442, *with United States v. Graham*, 824 F.3d 421, 433 n.12 (4th Cir. 2016) (en banc). It is axiomatic that virtually all private communications have at least two parties. Thus, when a person sends a private email, the mere act of clicking the "send" button does not eliminate or reduce that privacy interest. Instead, these communications are precisely what the Fourth Amendment protects. *See Kitzhaber*, 828 F.3d at 1090-92. Yet the panel's reasoning would diminish Fourth Amendment protections for essentially *all* private online communications—a result directly in conflict with this Court's decisions in *Kitzhaber* and *Forrester*.

At bottom, the panel appears to have improperly conflated the third-party doctrine with the rule that, once a letter reaches its recipient, the sender's expectation of privacy may be lost. *See Mohamud*, 843 F.3d at 442. Critically, however, that rule has no bearing on the surveillance at issue in this case. As the panel itself acknowledged, "prior case law contemplates a diminished expectation

of privacy [after a recipient receives a letter] due to the risk that the recipient will reveal the communication, *not that the government will be monitoring the communication*" in secret. *Id.* (emphasis added). Here, the government did not obtain the communications from the recipient at all, voluntarily or otherwise; rather, agents seized the emails from an internet service provider—an intermediary responsible for transmitting those emails privately. Accordingly, the communications are entitled to full Fourth Amendment protection. *See Warshak*, 631 F.3d at 286 ("[I]f government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.").

C. The panel improperly and inexplicably ignored the government's widespread use of "secondary searches" to access and examine the communications of Americans, including Mr. Mohamud.

The government's practice of amassing U.S. person communications using Section 702 and later searching through them—so-called "secondary searches"—is one of the most controversial aspects of this surveillance. Although the record strongly suggests that the government conducted such a secondary search here, the panel expressly declined to consider their legality.

Through these searches, the government converts warrantless surveillance ostensibly directed at foreigners into a tool for investigating Americans.[9] The parties litigated whether the government's use of such searches to investigate Mr. Mohamud was lawful, and the district court ruled squarely on this question. Yet, contrary to all evidence in the public record and without elaboration, the panel abruptly concluded that the issue was not before the Court. *See, e.g.*, *Mohamud*, 843 F.3d at 438. The panel's failure to address this issue is significant because, as a result, its Fourth Amendment reasonableness analysis entirely ignores one of the critical—and, indeed, most *unreasonable*—ways in which the government uses Section 702 as a backdoor into Americans' private communications.

Until the panel's opinion, there was little doubt that the government used a secondary search to retrieve and examine Mr. Mohamud's private emails. The public record provides multiple reasons to believe the government conducted such a search. First, the Privacy and Civil Liberties Oversight Board has stated that, "[W]henever the FBI opens a new national security investigation or assessment, FBI personnel will query previously acquired 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

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

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.[10] E.R. 5122-23. Second, unlike the panel's opinion, the district court directly addressed the lawfulness of secondary searches in a discussion titled "Querying After Acquisition" that spanned four pages. *United States v. Mohamud*, No. 10-cr-00475, 2014 WL 2866749, at *24-27 (D. Or. June 24, 2014) (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. *Id.* at *26. This entire discussion is inexplicable if the government never conducted a warrantless search for Mr. Mohamud's communications. Finally, throughout the litigation, the government never once disclaimed or denied having conducted a secondary search as part of its prosecution of Mr. Mohamud. Instead, it defended the lawfulness of those searches over many pages, both in the district court and on appeal. *See, e.g.*, Gov't Resp. Br. 130-35 (9th Cir. Dec. 7, 2015). That defense would have been

[10] The FBI has stated that its FISA and Section 702 data are commingled and thus queried simultaneously. PCLOB Report at 59.

entirely unnecessary if the retention and querying of Mr. Mohamud's communications was simply not "at issue" as the panel later claimed.[11]

Under the Fourth Amendment, the legality of Section 702 surveillance depends on the strength and sufficiency of the protections provided for Americans, based on the "totality of the circumstances." *Samson v. California*, 547 U.S. 843, 848 (2006). By carving out the government's secondary searches, the panel artificially limited the scope of that analysis. It disregarded one of the most intrusive ways in which the government exploits its warrantless collection of Americans' communications and, in so doing, it deprived Mr. Mohamud of what the district court considered his "most persuasive" challenge to the surveillance.

II. En banc review is necessary because of the far-reaching consequences of the panel's decision.

Because the government collects vast quantities of Americans' international communications under Section 702, the panel's decision affects not only Mr. Mohamud, but countless others. Yet, for the overwhelming majority of Americans who are subject to this surveillance but lack notice of that fact, there is effectively no opportunity to challenge the warrantless collection of their communications.

[11] Contrary to the panel's suggestion, all Section 702 communications are initially retained, often for a period of five years. The sheer number of intercepted communications—at least hundreds of millions per year—makes reviewing them in real-time impossible. Instead, many communications simply sit in the government's databases until they are specifically retrieved by an agent, typically "in response to a database query." PCLOB Report 128-29.

See, e.g., *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013) (denying plaintiffs standing to challenge Section 702). Thus, the Fourth Amendment interests of potentially millions of Americans depend on the legal analysis applied in a small handful of criminal cases like this one. As the only circuit court to address the legality of Section 702, it is imperative that the Court accurately and authoritatively review this surveillance.

Significantly, the panel's reasonableness analysis failed to consider measures that would adequately safeguard the privacy of Americans' communications—such as requiring individualized court review after the fact, when the government seeks to use or access protected communications. The government, and the panel, say that the minimization procedures are what save this surveillance. But those procedures leave FBI agents around the country free to use and access Americans' incidentally collected communications, even in ordinary criminal investigations. *See* PCLOB Report at 59. In other words, the procedures—which are supposed to protect the privacy of Americans—authorize the very kind of intrusion that the Fourth Amendment was designed to guard against.

Finally, the panel's decision has far-reaching implications for the scope of the Fourth Amendment in today's digital world. The panel's embrace of two novel and unsupported doctrinal rules is not only in conflict with the law of this Court, but has significant consequences for Americans' privacy in their online

communications writ large. By treating the "incidental overhear" rule as an exception to the warrant requirement, the panel's opinion potentially exposes myriad communications to warrantless surveillance. Similarly, by applying the third-party doctrine to emails that were indisputably kept private, the opinion risks eroding basic Fourth Amendment protections for sensitive online communications. In short, while the panel described its decision as a narrow one, *see Mohamud*, 843 F.3d at 438, it adopted some of the broadest possible arguments to justify the government's warrantless surveillance of Mr. Mohamud's emails.

Conclusion

For the foregoing reasons, the Court should grant rehearing or rehearing en banc.

Dated: February 27, 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

Counsel for Amici Curiae

Of Counsel:
Mathew W. dos Santos
AMERICAN CIVIL LIBERTIES
UNION OF OREGON FOUNDATION
P.O. Box 40585
Portland, OR 97240
Phone: (503) 227-6928
MdosSantos@aclu-or.org

Of Counsel:
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

CERTIFICATE OF COMPLIANCE
PURSUANT TO FED. R. APP. P. 32(g)

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Oregon, and Electronic Frontier Foundation in Support of Defendant–Appellant complies with Ninth Circuit Rule 29-2(c)(2), because the brief contains 4,187 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: February 27, 2017

/s/ Patrick Toomey
Patrick Toomey

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on February 27, 2017.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: February 27, 2017

/s/ Patrick Toomey
Patrick Toomey

Counsel for Amici Curiae