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

# SUPPLEMENTAL BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF OREGON, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT

*Counsel for Amici Curiae*
Patrick Toomey
Alex Abdo
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**

**Other Authorities**

## Introduction

Amici file this brief in response to the Court's Order dated September 2, 2016, which requested supplemental briefing concerning the lawfulness of the government's surveillance of Mr. Mohamud under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). Amici make three points.

First, Mr. Mohamud has raised a facial challenge to Section 702, but whether his challenge is considered "facial" or "as-applied," the warrantless searching of his communications was unlawful. Just as the Supreme Court held in *Berger v. New York*, 388 U.S. 41 (1967), the surveillance of Mr. Mohamud lacked sufficient procedural safeguards to render it constitutional. While the government has argued that, once Mr. Mohamud's communications were collected, it was free to use and search them as it pleased, that is incorrect. Courts have long held that back-end "minimization" protections are essential to the lawfulness of electronic surveillance. Here, where the government seeks to query and use the communications of Americans that it acquired without a warrant, those procedures must at the very least interpose individualized judicial review after the fact.

Second, *Verdugo-Urquidez* does not excuse the warrantless surveillance of Mr. Mohamud because he is a U.S. person and because the government seized and searched his emails on U.S. soil, where the warrant requirement indisputably protects his communications.

Third, even if the government is permitted to warrantlessly target foreigners abroad, it cannot simply bootstrap away the Fourth Amendment rights of Americans. Amici have never argued that the government must obtain a warrant before surveilling any foreigner abroad—but it must, at a minimum, provide reasonable protections for Americans like Mr. Mohamud when their communications, too, are swept up without a warrant. *See* Amici Br. 29–31. Courts have routinely imposed post-seizure restrictions to address the often broad and imprecise nature of electronic surveillance. Yet the current procedures offer no such protection: they expressly authorize the government to collect, retain, and deliberately query the communications of Americans, including in criminal investigations. In other words, they license the very type of warrantless intrusions that the Fourth Amendment was intended to prohibit.

Because the existing procedures afford such anemic protection, there is a narrow way to resolve the challenge in this case: by finding the procedures that governed the surveillance of Mr. Mohamud unreasonable, including those that permitted the "secondary search" of his communications. Because the procedures failed to require individualized judicial approval of any kind—even after the fact, and even when the government sought to query the communications of a *known* U.S. person—the Court can and should find them defective, just as the Supreme Court found the wiretapping procedures defective in *Berger*.

## I. Mr. Mohamud has raised a facial challenge, but whether his challenge is characterized as "facial" or "as applied," the surveillance of him was unconstitutional.

The Court has asked whether Mr. Mohamud's challenge is a facial one. It is. As Mr. Mohamud explains in his prior briefing, Op. Br. 155–62, Section 702, as a statute, lacks "essential procedural safeguard[s] against arbitrary" searches of Americans' international communications. *Patel v. City of L.A.*, 738 F.3d 1058, 1064 (9th Cir. 2013) (en banc), *aff'd* 135 S. Ct. 2443 (2015). While the statute directs the government to adopt (and seek FISC approval of) "minimization procedures," the existing procedures—administered by the executive branch—are no substitute for the Fourth Amendment's imposition of individualized judicial involvement. *See Riley v. California*, 134 S. Ct. 2473, 2491 (2014) ("[T]he Founders did not fight a revolution to gain the right to government agency protocols."). Moreover, the Supreme Court has recently reaffirmed that "facial challenges under the Fourth Amendment are not categorically barred or especially disfavored." *City of L.A. v. Patel*, 135 S. Ct. 2443, 2449 (2015). And it has invalidated surveillance regimes that are inconsistent with the Fourth Amendment. *See, e.g.*, *Berger*, 388 U.S. at 56–58; *United States v. U.S. District Court* ("*Keith*"), 407 U.S. 297 (1972); *Torres v. Puerto Rico*, 442 U.S. 465 (1979).[1]

[1] Similarly, this Court and other federal appellate courts considered the constitutionality of Title III "on its face" in the years following its enactment. *See, e.g.*, *United States v. Turner*, 528 F.2d 143, 158–59 (9th Cir. 1975).

Amici respectfully submit, however, that whether Mr. Mohamud's challenge is analyzed as "facial" or "as applied," the surveillance of him was unconstitutional. There is no dispute that Mr. Mohamud was in fact surveilled; there is no dispute that the surveillance took place without a warrant or any after-the-fact judicial authorization; and there is no dispute that it took place pursuant to a set of procedures required by statute. That surveillance was unconstitutional because it violated the warrant clause of the Fourth Amendment, and because, even if the warrant clause does not apply, the procedures relied upon were unreasonable in their failure to meaningfully protect the privacy of Americans ensnared in the government's warrantless surveillance. *See* Amici Br. 12–31.

This analysis does not turn on the nature of Mr. Mohamud's challenge, but on settled Supreme Court and Ninth Circuit precedent establishing that the constitutionality of electronic surveillance regimes depends on the strength of the totality of their protections—both restrictions on collection and restrictions on the later retention and use of what is collected. This point is critical to emphasize because of the government's apparent belief that, so long as its initial interception of Mr. Mohamud's communications was "lawful," restrictions on the government's retention or use of the information are irrelevant. This argument fundamentally misunderstands Fourth Amendment jurisprudence. Strict post-seizure restrictions are essential to the constitutionality of electronic surveillance.

The Supreme Court, the Ninth Circuit, and other courts have routinely judged the reasonableness of electronic surveillance by assessing the strength of the back-end protections. For example, the Supreme Court invalidated a New York eavesdropping statute because it failed to meaningfully restrict the state's conduct of surreptitious surveillance. *See Berger*, 388 U.S. at 58–60. The statute at issue in *Berger* 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. *Id.*

Lower courts have similarly evaluated the reasonableness of electronic-surveillance regimes by analyzing back-end protections. This Court, in *United States v. Turner*, 528 F.2d at 159, upheld the constitutionality of Title III based upon its agreement with other courts of appeals that the "specified safeguards" discussed by the Supreme Court in *Berger* were "essential under the Fourth Amendment" and had been met by Title III. The Fifth Circuit came to the same conclusion in *United States v. Sklaroff*, 506 F.2d 837, 840 (5th Cir. 1975), after observing that "a statute permitting wire interceptions under narrow restrictions and carefully circumscribed conditions may be constitutional." And the Second Circuit concurred after concluding that Title III "provide[s] for 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*." *United States v. Tortorello*, 480 F.2d 764, 773 (2d Cir. 1973); *accord United States v. Bobo*, 477 F.2d 974, 979 (4th Cir. 1973).

The lesson of these cases is simple: the constitutionality of wiretapping depends upon strict protections designed to minimize the inherent risks that secret surveillance poses to privacy. As the Supreme Court said in *Berger*, surveillance carries with it "inherent dangers," 388 U.S. at 60, and it must therefore be limited by "precise and discriminate" safeguards, *id.* at 58.

Courts have applied this same lesson in the context of foreign-intelligence surveillance. Indeed, the importance of strict safeguards is perhaps even greater in the context of intelligence surveillance because of "the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent." *Keith*, 407 U.S. at 320. In *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987), for example, the Fourth Circuit concluded that "FISA's numerous safeguards provide sufficient protection for the rights guaranteed by the Fourth Amendment within the context of foreign intelligence activities." It based that holding, in part, on FISA's requirement of "minimization procedures" designed to minimize the invasion of the privacy of U.S. persons. *See id.* (citing 50 U.S.C. § 1801).

Again, these cases reject the notion that wiretapping that is "lawful" at its inception is somehow immune from the Fourth Amendment's continuing requirement of reasonableness. *Cf. Tennessee v. Garner*, 471 U.S. 1, 7 (1985) (rejecting argument "that if [the probable-cause] requirement is satisfied the Fourth Amendment has nothing to say about *how* that seizure is made" (emphasis in original)); *Rodriguez v. United States*, 135 S. Ct. 1609, 1614–15 (2015).[2]

In this case, the surveillance of Mr. Mohamud was unreasonable because it lacked sufficiently protective back-end restrictions. The government premises its collection on the theory that its targets lack Fourth Amendment rights, but when it collects the communications of someone who indisputably *has* those rights, the protections remain paltry. As amici explained at length in their earlier submission, the procedures under Section 702 provide no meaningful protection to the many U.S. persons swept up in the government's warrantless surveillance. Amici Br. 23–29. Perhaps most troublingly, a central feature of the procedures is that they permit FBI agents to search Section 702 databases specifically for the protected communications of U.S. persons. It was the *absence* of the ability to conduct such

[2] This principle is not unique to wiretapping cases. For example, as discussed *infra*, this Court has approved of warrants for computer hard-drives only when they restricted the government to searching for and accessing specific information on the drives. *See, e.g.*, *United States v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) ("[T]he government should not be able to comb through Seda's computers plucking out new forms of evidence that the investigating agents have decided may be useful, at least not without obtaining a new warrant.").

"secondary" or "backdoor" searches on which the FISCR rested its approval of warrantless surveillance under Section 702's predecessor statute. *See In re Directives*, 551 F.3d 1004, 1015 (FISCR 2008) ("The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary."). Yet even that protection has since been stripped away.

## II. *Verdugo-Urquidez* has no bearing on the surveillance of U.S. persons like Mr. Mohamud on U.S. soil.

The Court has also asked the parties to address the applicability, if any, of *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990), including its relevance to the location of the search. *Verdugo-Urquidez* has no application here for the simple reason that *Verdugo-Urquidez* concerned a physical search abroad of the property of a foreign national. It did not excuse the government from complying with the warrant requirement when it searches the communications of U.S. persons on U.S. soil. While the government may satisfy the Fourth Amendment rights of those U.S. persons after the fact, when it seeks to query or use their communications, it is not entitled to the windfall it seeks here.

*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, 74. *Verdugo-Urquidez* was expressly concerned with the warrant requirement's application *abroad*, in a case

involving what can be called a "foreign-cubed" search: (1) the search was conducted on foreign soil; (2) the privacy interests at stake were exclusively those of a foreign national; and (3) the subject of the search was, until his arrest, located abroad. In a fractured decision, the Supreme Court held that applying the warrant requirement to such a search would be "impracticable and anomalous." *Id.* at 278 (Kennedy, J., concurring).[3]

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

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 (plurality) (emphasizing that "the place searched was located in Mexico"). Since the founding, searches of "papers and effects" conducted on U.S. soil have presumptively required a warrant.

[3] Although the outcome here does not depend on it, amici note that it is the "impracticable and anomalous" standard set out in Justice Kennedy's concurrence that is controlling, because he supplied the crucial fifth vote while explaining that he disagreed with the plurality's narrow interpretation of the Fourth Amendment's "reach." *See Verdugo-Urquidez*, 494 U.S. at 276 (stating that he could not "place any weight on the reference to 'the people'"). The Supreme Court reaffirmed this "functional" test for determining when constitutional protections apply abroad in *Boumediene v. Bush*, 553 U.S. 723, 759–64 (2008), where it cited Justice Kennedy's concurrence twice, and the plurality opinion not at all.

Second, Mr. Mohamud 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, this case does not involve such a claim. The government argues that it targeted the foreign end of Mr. Mohamud's conversations, and thus that the Fourth Amendment does not apply. But the Fourth Amendment does not speak in terms of "targets." What matters, here, is that the government acquired a communication to which a United States person was a party. For that reason alone, the Fourth Amendment unquestionably applies, and nothing in *Verdugo-Urquidez* suggests that the government may bootstrap away an American's right to privacy by "targeting" the foreign end.

Longstanding historical practice confirms that *Verdugo-Urquidez*'s reasoning cannot be extended to the search here. The government has been routinely required to obtain a warrant to search the communications of Americans inside the United States, including their international communications. Indeed, until 2007, when Congress passed Section 702's predecessor statute, the government was required to obtain a warrant in these circumstances, regardless of whom it claimed to be targeting. *See Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."); *United States v. Ramsey*, 431 U.S.

606, 623–24 (1977) (citing 19 C.F.R. § 145.3 (1976), requiring a warrant to read the contents of international letters on U.S. soil); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (warrant required for search of stored emails 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, 1824 (individualized FISC order required for acquisition of wire communications and stored emails on U.S. soil). In other words, the government has for centuries obtained a warrant in order to access or use the private letters, phone calls, and emails of U.S. persons on U.S. soil.

Finally, even as to the government's targets, Section 702 represents a gross expansion of *Verdugo-Urquidez*—and the facts of this case demonstrate why. The government takes the position that whenever it has formed a reasonable belief that its target is a foreigner abroad, it is entitled to warrantless access to all of that person's communications.[4] But even the *Verdugo-Urquidez* plurality required, at the very least, a far more individualized inquiry into the status of the persons searched. 494 U.S. at 271 (acknowledging that a foreign national with sufficient "voluntary connection" to the United States would be entitled to the protection of the Fourth Amendment). A foreign national who is located abroad today may have previously lived, worked, or studied in the United States. Not only that, but his or

[4] At last count, the government was monitoring more than 94,000 targets based on this bare finding. ODNI, 2015 Statistical Transparency Report 5 (Apr. 30, 2016), https://perma.cc/53CP-5WM7.

her stored emails may well date back to that time and thus represent wholly *domestic* communications. If, as the facts of the case suggest, the government targeted Amro Al-Ali—a Saudi national who lived and studied in the United States from 2008 to 2009—then the surveillance from the outset did not even meet *Verdugo-Urquidez*'s barest threshold. As a result, it cannot possibly serve as the pretext for warrantlessly surveilling Mr. Mohamud.

In short, the government has taken every premise relied upon in *Verdugo-Urquidez* and stretched it far past its limits, in order to gain warrantless access to the international communications of Americans. *See* Amici Br. 16–17 & n.18.

## III. The Fourth Amendment requires the government to obtain a warrant before seeking to access or use the communications of Americans collected under Section 702.

### A. The government cannot dispense with the Fourth Amendment rights of Americans simply because it is targeting foreigners.

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 U.S. persons like Mr. Mohamud. 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 the communications of *known* U.S. persons without ever satisfying the Fourth Amendment. *See 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."). Back-end minimization procedures can and must provide U.S. persons with the protection that is absent on the front end.

First, the incidental-overhear doctrine does not permit the government to collect and retain the communications of a U.S. person without a warrant simply by "targeting" a person who lacks Fourth Amendment rights. *See* Amici Br. 17–18. It is the higher standard—not the lower one—that controls when a U.S. person's protected privacy interests are at stake. *Cf. United States v. Bin Laden*, 126 F. Supp. 2d 264, 281 (S.D.N.Y. 2000) (rejecting the government's reliance on the incidental-overhear doctrine and applying the higher Fourth Amendment standard where the U.S. person was a "contemplated interceptee of electronic surveillance . . . even if he was not officially deemed a target"). The government has never before been allowed to exploit the type of "mismatch" or loophole it relies on here.[5] Instead, as noted above, the government has long been required to obtain a warrant on U.S. soil regardless of who it claims to be targeting. Indeed, the

[5] Under Section 702, the government is applying on a programmatic scale the very logic the district court rejected in *Bin Laden*. As amici explained in their prior brief, the government's explicit aim in advocating passage of Section 702 was to obtain warrantless access to the international communications of U.S. persons. Amici Br. 16–20. In other words, the government's collection of protected communications is both foreseeable and deliberate. The mere fact that the government cannot identify all of these "contemplated interceptees" in advance, does not entitle it to disregard their Fourth Amendment rights once it knows that a particular communication involves a U.S. person.

consequences of accepting the government's incidental-overhear theory would be far-reaching, because its logic is completely untethered even from any foreign-intelligence exception. By "targeting" the foreign end of communications, the government could bypass the courts and the warrant requirement for *any* international phone call, email, or letter involving a U.S. person, including in ordinary criminal investigations. In our nation's history, such power would be extraordinary and "anomalous." *Verdugo-Urquidez*, 494 U.S. at 278 (Kennedy, J., concurring).[6]

The government's theory is dangerously overbroad and incoherent in another way—because it would render the minimization procedures legally irrelevant. If the government's surveillance were "lawful" simply because it had satisfied the (non-existent) rights of its target, as it claims, then it would not matter what the government did after the fact. Yet even the government agrees that adequate minimization procedures are necessary to satisfy the Fourth Amendment rights of U.S. persons swept up in the surveillance. Gov't Br. 128–29. The Fourth Amendment requires the government to obtain a warrant to access the private

[6] To the extent the government falls back on a foreign-intelligence exception, if one exists at all it is not broad enough to render the surveillance of Mr. Mohamud lawful here. Courts have consistently limited the scope of any foreign-intelligence exception to cases where the Attorney General or the President has found probable cause to believe the target is the agent of a foreign power. *See* Amici Br. 21–23.

communications of U.S. persons, and thus the minimization procedures must afford comparable protection—even if it is after the fact.

Indeed, the fact that the protected communications of U.S. persons may be intermingled with those of foreigners does not forever excuse the government from complying with the warrant requirement. Both Congress and courts—including this Court—have often dealt with similar overcollection problems, especially when confronted with broad seizures of digital information. In response, they have imposed rules to ensure that the scope of the government's searches match the scope of its Fourth Amendment authority. These rules routinely require the government either to refrain from using information that is beyond the scope of its legal authority or to secure additional court authorization after the fact.

- In the case of computer hard-drive searches, where data is often intermingled, this Court has prohibited the government from making investigative use of information outside the scope of its original warrant—unless it first obtains a new warrant. *See Sedaghaty*, 728 F.3d at 914 ("To the extent the agents wanted to seize relevant information beyond the scope of the warrant, they should have sought a further warrant."). As the Court has made clear, these restrictions ensure that the government does not reap precisely the type of Fourth Amendment windfall it seeks here. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1172 (9th Cir. 2010) (computer review procedures were "designed to reassure the issuing magistrate that the government wouldn't sweep up large quantities of data in the hope of dredging up information it could not otherwise lawfully seize").
- In the case of traditional FISA surveillance, Congress imposed a special set of strict minimization rules to ensure that *warrantless* surveillance directed exclusively at foreign powers does not intrude upon the Fourth Amendment 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 Protect America Act surveillance, the FISCR predicated its Fourth Amendment ruling on the fact that the government was not amassing a searchable database of incidentally collected U.S.-person communications. *See In re Directives*, 551 F.3d at 1015. The government represented that it was not deliberately storing or searching for Americans' communications—and, indeed, the government's procedures prohibited such "secondary searches" for years. *See infra* Section III.B.

- In the case of FISA pen-register surveillance, the FISCR recently relied on rules that prohibit the government from making any investigative use of Fourth-Amendment protected content obtained in the course of acquiring unprotected metadata. *In re Certified Question of Law*, No. 16-01, slip op. at 33–34 (FISCR Apr. 14, 2016), https://perma.cc/MHL9-D2KE. The fact that protected and unprotected data may be intermingled does not give the government carte blanche to disregard basic Fourth Amendment protections.

- In the case of Section 702 surveillance itself, the FISC has strictly limited the government's ability to use communications obtained via Upstream surveillance—*including its ability to conduct secondary searches*—precisely because Upstream surveillance involves significant amounts of overcollection, even by the government's standards. [*Redacted*], 2011 WL 10945618, at *10–13 & n.21 (FISC Oct. 3, 2011).

- In the case of Title III surveillance, the government is required to segregate and destroy non-responsive communications in real-time, thereby ensuring that the collection does not exceed the scope of the initial court authorization. *See Turner*, 528 F.2d at 156 (finding Title III constitutional because "measures [must] be adopted to reduce the extent of . . . interception [of irrelevant or innocent communications] to a practical minimum").

In each of these instances, courts and Congress have adopted practical solutions to a practical problem involving intermingled data—in order to ensure that the government's searches comply with the Fourth Amendment. In the same way, the

mere fact that the government is targeting foreigners under Section 702 when it acquires the communications of U.S. persons is not a valid reason for jettisoning the warrant requirement altogether.

Finally, while back-end minimization procedures could adequately protect the rights of U.S. persons, the current procedures do the opposite. It is plain that the minimization procedures do not afford U.S. persons anything resembling the basic protections of the Fourth Amendment. *See* Amici Br. 25–29. They allow the government to collect Americans' communications on U.S. soil without a warrant, under the guise of targeting foreigners. They allow the government to retain those communications for five years by default—and to pool them in massive centralized databases.[7] And they allow agents to conduct queries that deliberately target U.S. persons' communications after they are collected, including for use in all manner of *criminal* investigations. *See* PCLOB Report 55–60. In short, the procedures—which are supposed to protect the privacy of Americans—authorize the very type of intrusion that the Fourth Amendment was designed to guard against.

[7] During this time, analysts rarely minimize anything. *See* PCLOB Report 129 ("[A]lthough a communication must be 'destroyed upon recognition' when an NSA analyst recognizes that it involves a U.S. person and determines that it clearly is not relevant to foreign intelligence or evidence of a crime, in reality this rarely happens.").

### B. The Court should hold the secondary search of Mr. Mohamud unlawful.

The Court can and should find the surveillance of Mr. Mohamud unlawful based on its warrantless query of his communications.

The government is wrong that a rule restricting such post-seizure queries would be anomalous. For one thing, such a restriction already exists in the context of Section 702 itself: the government is *already* prohibited from conducting secondary searches targeting Americans within its Upstream databases. *See* 2015 NSA Minimization Procedures § 3(b)(5), https://perma.cc/4PRP-MGS3. In fact, up until 2011, secondary searches targeting Americans within the NSA's PRISM databases were also prohibited. *See* [*Redacted*], 2011 WL 10945618, at *7 ("The procedures previously approved by the Court effectively impose a wholesale bar on queries using United States-Person identifiers."); Ellen Nakashima, *Obama Administration Had Restrictions on NSA Reversed in 2011*, Wash. Post, Sept. 7, 2013, https://perma.cc/5E85-T7EU. And, when the FISCR ruled on Section 702's predecessor statute, such searches were categorically barred. *See In re Directives*, 551 F.3d at 1015. Indeed, rules that restrict the government's later use of information—especially electronic information—or require the government to seek court approval after the fact are especially common when the government has engaged in broad collection or relied on an exception to the warrant requirement. *See, e.g.*, 50 U.S.C. 1801(h)(4) (requiring individualized FISC authorization to

retain and use Americans' communications); *In re Application of the FBI*, No. BR 14-01, slip op. at 6–9 (FISC Feb. 4, 2014), https://perma.cc/2MVK-LER7 (requiring individualized FISC authorization to query bulk call-records database); 50 U.S.C. § 1805(e) (requiring after-the-fact FISC authorization in emergencies); 18 U.S.C. § 2518(7) (similar for Title III).

Moreover, in rejecting Mr. Mohamud's challenge to the secondary search of his communications, the district court made a significant factual error. The court appeared to assume that the collected communications are invariably reviewed by human analysts—and "minimized"—at the time of the collection. Dist. Ct. Op. 45 (I:216). Based on that premise, the court theorized that a query to extract Mr. Mohamud's communications could not be more intrusive than the original review.

That premise is wrong. The sheer number of communications collected under Section 702—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 either selected through a specific query or automatically purged after five years. *See* PCLOB Report 128–29 ("NSA analysts do not review all or even most communications acquired under Section 702 as they arrive at the agency. Instead, those communications often remain in the agency's databases unreviewed until they are retrieved in response to a database query, or until they are deleted . . . without ever having been reviewed."). For that reason,

queries designed to extract the communications of specific U.S. persons often constitute a new intrusion—one directed at communications that the government *knows* are protected by the Fourth Amendment.

A rule requiring the government to obtain individualized court approval in order to query the communications of a known U.S. person would simply require the type of protection the government has bypassed on the front-end. As amici have described previously, the President's Review Group, the House of Representatives, and then-Senator Obama have all called for similar protection. *See* Amici. Br. 30. Given the breadth and intrusiveness of this surveillance, such a requirement is a practical, necessary, and reasonable safeguard.

## Conclusion

For the foregoing reasons, the Court should hold that the surveillance of Mr. Mohamud was unconstitutional.

Dated: October 3, 2016

Respectfully submitted,

*/s/ Patrick Toomey*

Patrick Toomey
Alex Abdo
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
WITH THE LENGTH LIMITATION,
TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Supplemental 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 the Court's Order dated September 2, 2016, because the brief contains no more than twenty pages, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); 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 3, 2016

*/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 October 3, 2016.

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: October 3, 2016

*/s/ Patrick Toomey*
Patrick Toomey

*Counsel for Amici Curiae*