U.S. Court of Appeals Case No. 19-16066

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

CAROLYN JEWEL, *et al.*,
Plaintiffs-Appellants,

v.

NATIONAL SECURITY AGENCY, *et al.*,
Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CALIFORNIA
Honorable Jeffrey S. White
Case No. 4:08-cv-04373-JSW

BRIEF OF AMICUS CURIAE NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF PLAINTIFFS-APPELLANTS

BENJAMIN B. AU
TARA J. NORRIS
W. HENRY HUTTINGER
DURIE TANGRI LLP
530 Molino Street, Suite 111
Los Angeles, CA 90013
(415) 362-6666
bau@durietangri.com
tnorris@durietangri.com
hhuttinger@durietangri.com

CATHERINE R. GELLIS
3020 Bridgeway #247
Sausalito, CA 94965
(202) 642-2849
cathy@cgcounsel.com

MICHAEL PRICE
Fourth Amendment Center
NACDL
1660 L St. NW, 12th Floor
Washington, D.C. 20036
(202) 465-7615
mprice@nacdl.org

GIA L. CINCONE
9th Circuit Vice Chair
NACDL *Amicus* Committee
Two Embarcadero Center, Suite 1900
San Francisco, California 94111
(415) 576-0200 Telephone
(415) 576-0300 Facsimile

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, the undersigned states that National Association of Criminal Defense Lawyers does not have a parent corporation, and no publicly held corporation owns 10% or more of its stock.

Dated: September 13, 2019

/s/ Benjamin B. Au
Benjamin B. Au
Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE WITH RULE 29(C)(5)

Counsel for the parties did not author this brief in whole or in part. The parties have not contributed money intended to fund preparing or submitting the brief. No person other than Amicus Curiae or its counsel contributed money to fund preparation or submission of this brief.

Dated: September 13, 2019

/s/ Benjamin B. Au
Benjamin B. Au
Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

IDENTITY AND INTEREST OF AMICUS CURIAE

The National Association of Criminal Defense Lawyers ("NACDL") is a nonprofit voluntary professional bar association that works on behalf of criminal defense attorneys to ensure justice and due process for those accused of crime or misconduct. NACDL was founded in 1958. It has a nationwide membership of many thousands of direct members, and more than 40,000 with affiliates. NACDL's members include private criminal defense lawyers, public defenders, military defense counsel, law professors, and judges. NACDL is the only nationwide professional bar association for public defenders and private criminal defense lawyers. NACDL is dedicated to advancing the proper, efficient, and just administration of justice. NACDL files numerous *amicus* briefs each year in the U.S. Supreme Court and other federal and state courts, seeking to provide amicus assistance in cases that present issues of broad importance to criminal defendants, criminal defense lawyers, and the criminal justice system as a whole.

NACDL has a particular interest in cases that involve surveillance technologies and programs that pose new challenges to personal privacy. The NACDL Fourth Amendment Center offers training and direct assistance to defense lawyers handling such cases in order to help safeguard privacy rights in the digital age. NACDL has also filed numerous *amicus* briefs in this Court and the Supreme Court on issues involving digital privacy rights, including: *Carpenter v. United*

States, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400 (2012); *United States v. Cotterman*, 709 F.3d 952, 956 (9th Cir. 2013) (en banc); and *United States v. Henderson*, 906 F.3d 1109 (9th Cir. 2018).

NACDL has a particular interest in this case because many of NACDL's members represent, or are themselves, individuals like the Plaintiffs who have had their Internet communications indiscriminately seized when passing through AT&T's network and subjected to broad, suspicionless, warrantless searches by the National Security Agency ("NSA"). NACDL's members are on the front lines of litigating Fourth Amendment issues. This case threatens to expand the government's ability to conduct warrantless searches and seizures on a massive scale and then use the fruits of these searches against individuals.

The risk is not hypothetical; the government has brought numerous criminal prosecutions based on information obtained through warrantless NSA surveillance. NACDL submits this amicus brief to highlight the dangers of allowing these warrantless, dragnet searches to continue. Permitting a massive, suspicionless surveillance program under the limited "special needs" exception would eviscerate bedrock constitutional protections against abuses of state power. The Court should reject the Government's invitation to do so.

CONSENT OF THE PARTIES

Pursuant to Federal Rule of Appellate Procedure 29, counsel for amicus curiae note that all parties have consented to the filing of this brief.

I. SUMMARY OF ARGUMENT

Plaintiffs-Appellants challenge the warrantless, bulk collection of millions of ordinary Americans' Internet communications, including their own, made through the AT&T Internet network without their knowledge, consent, or individualized suspicion. One of the appealed orders is the district court's denial of Plaintiffs' motion for partial summary judgment on their Fourth Amendment claim. In arguing that its bulk data collection program does not violate the Constitution despite lacking a judicial warrant, the government argued that it was exempted from the warrant requirement because the program served a governmental "special need."

The mass interception, copying, and examination of Plaintiffs' Internet communications constitutes a search and seizure, triggering the Fourth Amendment's warrant requirement. This requirement cannot be evaded by invoking the "special needs" exception. First, the government has not shown, and cannot show, that the "primary purpose" of its surveillance program is something other than its interest in law enforcement, as required under the "special needs" exception. Second, even if the government could invoke the exception, the program is unreasonable because the massive intrusion on Plaintiffs' privacy interests and constitutional rights outweighs the government's need to collect foreign intelligence.

II. ARGUMENT

A. The Government's Mass Interception and Scanning of Americans' Internet Communications Is a Search and Seizure, Triggering the Fourth Amendment's Warrant Requirement

The Supreme Court has long recognized the "threats to personal privacy" that "new technology," including "electronic surveillance," poses. *United States v. U.S. Dist. Court* ("*Keith*"), 407 U.S. 297, 312 n.13 (1972). Given this risk, the Court cautioned that "the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." *Id.* at 313 (footnote omitted).

Since *Keith*, the Supreme Court has repeatedly applied these Fourth Amendment safeguards to digital communications. In *Riley v. California*, 573 U.S. 373 (2014), for example, the Court required a warrant to search a suspect's cell phone incident to arrest. *Id*. In so holding, it concluded that a cell phone contains information, including "picture messages, text messages, [and] Internet browsing history"—exactly the sort of information the challenged Upstream program searches without a warrant—in which a person has a reasonable expectation of privacy and thus is protected by the Fourth Amendment. *Id.* at 394. Subsequently, in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the Court extended the Fourth Amendment warrant requirement to cell phone location data held by a third party, because it recognized, as it had in *Riley*, that cell phones are

"'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society," and therefore due the same constitutional protection. *Id.* at 2210 (quoting *Riley*, 573 U.S. at 385). Notably the Upstream program at issue here collects similar information as that at issue in *Riley* and *Carpenter*—including, presumably, geolocation information associated with the use of applications, Internet posts, and search queries—for each and every communication sent or received over the Internet. The innumerable mobile devices—laptops, personal computers, tablets, and smartphones—swept up in the NSA's surveillance dragnet are just as ubiquitous and essential to modern life as the technology at issue in *Riley*.

This Court has also expressly recognized that the Fourth Amendment extends to personal email, which "can, and often does, contain all the information once found in the 'papers and effects' mentioned explicitly in the Fourth Amendment." *In re Grand Jury Subpoena, JK-15-029*, 828 F.3d 1083, 1090 (9th Cir. 2016). Similarly, the Sixth Circuit requires a warrant and probable cause for law enforcement access to email, finding that it "plays an indispensable part in the Information Age" and is the "technological scion of tangible mail." *United States*

v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).[1] The NSA's Upstream dragnet thus infringes on the reasonable expectation of privacy that individuals maintain in their Internet activity. *See Carpenter*, 138 S. Ct. at 2214 (the Fourth Amendment must continue to "secure the privacies of life against arbitrary power" and "place obstacles in the way of a too permeating police surveillance").

Yet the NSA's Internet surveillance programs lack any of the familiar Fourth Amendment safeguards.[2] The NSA instead seizes the Internet communications of U.S. persons in bulk, without a warrant, much less any attempt to show probable cause or particularity. This surveillance therefore presumptively violates the Fourth Amendment under recent Supreme Court jurisprudence. *Carpenter*, 138 S. Ct. at 2221; *Riley*, 573 U.S. at 382.

To conduct Upstream surveillance under Section 702, the government uses a fiber-optic splitter to intercept and copy all Internet communications transiting major junctions on the Internet backbone. Each instance of capturing and copying a single electronic communication in this way constitutes a seizure under the

---

[1] Following *Warshak*, the Department of Justice issued a policy requiring investigators to seek warrants to access the contents of online messages. *See* Email Privacy Act, H.R. REP. NO. 114-528, at 9 (Apr. 26, 2016) (noting, "[s]oon after the [*Warshak*] decision, the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013.").

[2] The *Keith* Court expressly rejected a "domestic security surveillance" exception to the Fourth Amendment warrant requirement, 407 U.S. at 316-17, although it suggested that "foreign intelligence information" might be treated differently. *Id.* at 308. In this case, however, Section 702 surveillance intercepts not just the Internet communications of foreigners overseas, but also the domestic communications of American citizens and U.S. persons within the United States.

Fourth Amendment. A seizure occurs when "there is some meaningful interference with an individual's possessory interests in that property." *Jones*, 565 U.S. at 419 (Alito, Ginsburg, Breyer & Kagan, JJ., concurring) (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). Here, the NSA is interfering with one of the "most essential sticks" in the bundle of property rights, "the right to exclude others." *Kaiser Aetna v. United States*, 444 U.S. 164, 176 (1979). Copying data interferes with individuals' possessory interests in controlling the flow of, and limiting access to, their data. *See United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (government "seized data" by copying hard drive); *Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197, 220 (2d Cir. 2016), *vacated and remanded on other grounds by United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (describing government's data copying as "seiz[ure]"); *United States v. Bach*, 310 F.3d 1063, 1065, 1067 (8th Cir. 2002) (referring to "seizure" of information from Yahoo email accounts); *United States v. Taylor*, 764 F. Supp. 2d 230, 237 (D. Me. 2011) (obtaining copies of emails from internet service provider "for subsequent searching" is a seizure); *United States v. Bowen*, 689 F. Supp. 2d 675, 684 (S.D.N.Y. 2010) (copying of entire email account described as seizure); *United States v. Jefferson*, 571 F. Supp. 2d 696, 703 (E.D. Va. 2008) (copying documents interferes with a person's "sole possession of

the information contained in those documents: it diminishes the person's privacy value in that information."). Copying Internet communications invades and asserts dominion over them. It is the equivalent of the NSA secretly "bcc"ing itself on every email sent or received.

Likewise, the government's review of copied communications for designated "selectors" is a Fourth Amendment search. The law on this point is clear: electronic communications receive the same protection as did physical property understood to be protected at the founding. *United States v. Ackerman*, 831 F.3d 1292, 1307 (10th Cir. 2016) ("[W]arrantless opening and examination of (presumptively) private correspondence that could have contained much besides potential contraband for all anyone knew . . . seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment."). As then-Judge Gorsuch concluded, "a more obvious analogy from principle to new technology is hard to imagine and, indeed, many courts have already applied the common law's ancient trespass to chattels doctrine to electronic, not just written, communications." *Id*. at 1308. The Fourth Amendment remains just as relevant today as it did at the founding, and should not give way simply because communications are now digital.

B. The "Special Needs" Exception to the Warrant Requirement Cannot Justify the Government's Surveillance Program

Warrantless searches are "per se unreasonable" under the Fourth Amendment, "subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967). These exceptions are "jealously and carefully drawn," because warrants guard against "arbitrary intrusions by official power." *Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971) (internal quotation marks omitted) (citation omitted). The warrant requirement assures citizens that governmental searches "are not the random or arbitrary acts of government agents" and that their personal communications and belongings will not be subject to examination by omnipotent governmental institutions. *See Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 621-22 (1989). For this reason, courts "closely guard[]" the warrant requirement's scope. *See Chandler v. Miller*, 520 U.S. 305, 309, 313-14 (1997). The government will always argue (as it does here) that its failure to obtain a warrant is justified. But it is critical that the judiciary resist such claims and jealously guard the Fourth Amendment's protections, even in the face of government assertions that the warrant requirement is impractical or inefficient. "If times have changed … in an urban and industrial world, the changes have made the values served by the Fourth Amendment more, not less, important." *Coolidge*, 403 U.S. at 455.

Although the courts have carved out a limited exception for circumstances when a "special need" can justify a warrantless search, this exception only applies where the search serves a special need "beyond the normal need for law enforcement" and for reasons "other than crime detection." *See Chandler*, 520 U.S. at 309, 313-14. Whether a particular warrantless search can be permitted pursuant to the "special needs" exception is a "context-specific inquiry," in which the court must evaluate the "competing private and public interests." *Id.* at 314. The "special needs" exception must be strictly cabined precisely because it permits searches without either the judicial oversight a warrant provides or the individualized suspicion and particularity a warrant requires.

To satisfy the "special needs" exception, the government must first establish that the "primary purpose" of a search serves a need other than the government's general interest in law enforcement. *Ferguson v. City of Charleston*, 532 U.S. 67, 81 (2001); *see also City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2452 (2015); *Indianapolis v. Edmond*, 531 U.S. 32, 38-41 (2000). Then, even if the government demonstrates the existence of a non-law enforcement "special need," the Fourth Amendment still demands more, requiring that the government's interest in conducting the warrantless search outweigh the effect of the intrusion upon individual rights. *Board of Educ. of Indep. Sch. Dist. No. 92 v. Earls*, 536 U.S. 822, 830 (2002). Only then, if "the privacy interests implicated by the search are

minimal, *and* [] an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion," can a warrantless search be permitted. *Skinner*, 489 U.S. at 624 (emphasis added). As elaborated below, the Upstream program cannot meet this burden.

1. Foreign Intelligence is Not the "Primary Purpose" of the NSA's Dragnet Surveillance Program

The government identified "foreign intelligence collection" as the "special need" served by the warrantless searches at issue here. Even assuming that "foreign intelligence collection" is *not* a law enforcement purpose, the government cannot demonstrate that "foreign intelligence collection" is the *primary* purpose of the Upstream program.[3] Without that showing, the search cannot be permitted under the Fourth Amendment.

a. The "Special Needs" Exception Applies Only Where the "Primary Purpose" of the Challenged Search or Seizure Is Not Law Enforcement

The Supreme Court's "special needs" jurisprudence makes clear that this exception is limited to those unique cases where the "primary"—and, indeed, overwhelming—purpose of the search was not law enforcement. In *City of Indianapolis v. Edmond*, for example, the Court rejected as an unconstitutional

[3] The district court, of course, drew no such conclusion, electing instead to rely solely on the grounds of state secrets privilege to grant the government's motion for summary judgment on Plaintiffs' Fourth Amendment claims.

seizure a set of suspicionless "drug checkpoints" in which vehicles were briefly stopped and assessed by narcotics-detection dogs. The Court distinguished the challenged checkpoints from those vehicle checkpoints that it had previously approved, "principally" because the "primary purpose" of the challenged *Edmond* checkpoints differed from the non-law enforcement purposes of the permissible checkpoints. 531 U.S. at 40. The Court rejected the government's explanation that because these checkpoints aided the government in combatting illegal narcotics trade and thereby protected the community, they had anything other than a law enforcement purpose, noting that "[t]he detection and punishment of almost any criminal offense serves broadly the safety of the community" and thus the government could not so easily dispense with the warrant requirement. *Id.* at 42-43.

The Supreme Court reinforced its *Edmond* analysis in *Ferguson v. City of Charleston*, in which it concluded that warrantless, non-consensual drug screens on pregnant women—the results of which were then shared with law enforcement officers—violated the Fourth Amendment. The Court rejected the government's argument that any criminal prosecutions that resulted from its warrantless investigations were in service of the permissible purpose of getting pregnant women "into substance abuse treatment and off of drugs." 532 U.S. at 82–83. The "primary purpose" of the drug testing program, the Court explained, was "to use

the threat of arrest and prosecution in order to force women into treatment." Thus, the program was unconstitutional. *Id.* at 84.

b. The "Primary Purpose" of the Upstream Program Is Not Foreign Intelligence Collection

Originally, the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. §§ 1801–1885c, required the government to certify that "*the* purpose" of the surveillance was to obtain "foreign intelligence information," which is narrowly defined with respect to searches of U.S. persons as information deemed "necessary" to national security or the conduct of foreign affairs. *Id.* § 1801(e)(2) (emphasis added). This requirement aligned with court decisions that had recognized a limited foreign intelligence exception to the warrant requirement in certain individual cases, but only after the government had established that obtaining "foreign intelligence" was the primary purpose of the surveillance. *See United States v. Truong*, 629 F.2d 908, 913 (4th Cir. 1980). The Patriot Act of 2001 eliminated this requirement, however, and instead allowed the government to obtain FISA orders as long as it had certified that acquiring foreign intelligence was "a *significant* purpose" of the surveillance. Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act"), Pub. L. No. 107-56, 115 Stat. 272 (2001) (emphasis added); *see* 50 U.S.C. § 1881a(g)(2)(A)(v). The Patriot Act thus permitted the government to obtain a FISA order *even* if its primary goal was to

gather evidence for a criminal prosecution, as long as "a significant purpose" of the surveillance was foreign-intelligence collection. This revision made the statute inconsistent with recognized constitutional limitations.

The standard for approval under Section 702 (a "significant" purpose) is plainly different from the standard for invoking the "special needs" exception (the "primary" purpose): "significant" means of sufficient importance to be noticeable, while "primary" means of a *greater* importance than any other purpose. *Compare significant Definition*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/significant (defining "significant" as "having or likely to have influence or effect"), *with primary Definition*, MERRIAM-WEBSTER.COM, https://www.merriam-webster.com/dictionary/primary (defining "primary" as "of first rank, importance, or value") (last visited Sept. 13, 2019).

If a warrantless search could be justified because a cited non-law enforcement purpose was merely "significant," the "special needs" exception would stop being a limited exception. The government can almost always generate *some* explanation, other than criminal investigation, for a search. Limiting the exception only to searches where the non-law enforcement special need is the *primary* purpose of the search ensures that the exception does not become an end run around the Fourth Amendment's warrant requirement. Recognizing that it easily could become one, the Supreme Court has rejected efforts to let the "special

needs" exception provide "a pretext to enable law enforcement authorities to gather evidence of penal law violations." *Skinner*, 489 U.S. at 621 n.5 (internal quotation marks omitted) (citation omitted); *see also Edmond*, 531 U.S. at 33 (the existence of a "lawful secondary purpose" cannot save a warrantless search or seizure).

Moreover, any argument that the program primarily serves to collect foreign intelligence information is belied by the government's well-documented reliance on evidence collected from the challenged surveillance program in criminal investigations and prosecutions. Multiple agencies now routinely search Section 702 data for information about U.S. persons, a practice known as "back-door" searching. The FBI, for example, searches these databases whenever it opens a criminal investigation or even an "assessment," a preliminary inquiry for which FBI agents do not need to show any suspicion of criminal activity. *See* Privacy & Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), at 137, available at https://www.pclob.gov/library/702-Report.pdf.[4] Law

[4] Additionally, the Department of Justice has looked to cases involving the NSA program challenged here when evaluating the legality of bulk collection programs run by other law enforcement entities, such as the DEA—suggesting that data resulting from the challenged surveillance program is shared with other law enforcement agencies. Office of the Inspector General, U.S. Department of Justice, *A Review of the Drug Enforcement Administration's Use of Administrative Subpoenas to Collect or Exploit Bulk Data* (2019), at 95-96, available at https://oig.justice.gov/reports/2019/o1901.pdf (drawing comparison between DEA bulk collection program and NSA bulk collection program).

enforcement agencies, including the FBI and DEA, regularly use "parallel construction" to conceal investigative methods (like NSA surveillance), shielding those methods from judicial scrutiny. *See* Human Rights Watch, *Dark Side*: *Secret Origins of Evidence in US Criminal Cases* (2018) at 17-27, available at https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases; Natasha Babazadeh, *Concealing Evidence: 'Parallel Construction,' Federal Investigations, and the Constitution*, 22 Va. J. of Law & Tech. 1, 8-18 (2018).[5] If the NSA is permitted to engage in bulk data collection, and the FBI is permitted to search that data at its leisure, then there are no principled constitutional restrictions on the surveillance state and its corrosive effect on due process. *See Keith*, 407 U.S. at 317 ("The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.").

The government's arguments assume that "foreign intelligence collection" could itself qualify as a "special need" sufficient to justify a warrantless search.

[5] Other legal violations, such as failure to notify criminal defendants of Section 702 surveillance, have occurred as a result of the government's reliance on "parallel construction" to cover up the true nature of its criminal investigations. Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance— Again?*, Just Sec. (Dec. 11, 2015), available at https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again/.

But the Supreme Court has never recognized such an exception to the warrant requirement. Nor has the Supreme Court permitted the warrantless bulk collection, searching, and retention of domestic communications. In *Keith*, for instance, the Supreme Court rejected the notion that intelligence needs justified dispensing with the warrant requirement in domestic surveillance cases. 407 U.S. at 316–21. Instead, the Court described warrantless domestic surveillance conducted at the discretion of executive officers as contrary to "the very heart of the Fourth Amendment directive." *Id.* at 316. In describing its rejection of the government's warrantless domestic surveillance program, the *Keith* Court explained that the Fourth Amendment's warrant requirement had to be enforced even where the government had identified "pragmatic" reasons for evading it:

> Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent.

Id. at 320. This reasoning is equally applicable here, where the government is intercepting, copying, and scanning millions of individuals' electronic

communications.[6]

Ultimately, this case is no different from *Edmond* or *Ferguson*, in which the Supreme Court rejected government efforts to obscure routine criminal investigations with references to security and harm prevention. Suspicionless searches and seizures cannot be justified by only "the generalized and ever-present possibility that . . . inspection may reveal that any given [Internet user] has committed some crime." *Edmond*, 531 U.S. at 44. The Fourth Amendment requires a warrant even in cases where the crime under investigation is serious. *See, e.g.*, *Flippo v. West Virginia*, 528 U.S. 11, 13–14 (1999) (per curiam) (no "murder-scene" exception to warrant requirement); *Abel v. United States*, 362 U.S. 217, 219-20 (1960) ("[T]he fact that [this case] was a prosecution for espionage[] has no bearing whatever upon the legal considerations relevant to the admissibility of evidence."). Given that the fruits of the NSA's dragnet surveillance are routinely used in ordinary criminal investigations, that these searches might also

[6] The Ninth Circuit's decision in *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016), is not to the contrary. In that case, the Ninth Circuit explicitly excluded from its analysis of foreign and domestic surveillance programs the sort of "Upstream" collection challenged here, focusing instead on the PRISM program, in which the government targeted specific accounts used by non-U.S. persons to communicate foreign intelligence information. *See id.* at 438 & n.19; *see also In re Directives to Yahoo! Inc.*, No. 08-01, 2008 WL 10632524, *7 (Foreign Intel. Surv. Ct. of Review Aug. 22, 2008) (limiting holding to facts of that case, involving to/from communications from an ISP, not Upstream collection). Moreover, unlike in *Mohamud* or *In re Directives to Yahoo! Inc.*, the search and seizure of domestic communications here is not merely "incidental"—it is a central part of the program's design.

have been intended for foreign intelligence collection is not enough to show that the government's stated purpose is the primary purpose. Instead, the program demonstrates why it is so important to guard against the government's efforts to evade the warrant requirement.

C. The Impact of the Intrusion from the NSA's Internet Surveillance Outweighs the Government's Need

Even if the government could invoke a "special need" for foreign intelligence collection, that would not end the constitutional inquiry. The court must still balance the search's intrusion upon individual rights against the government's interest in the warrantless search. In the case of this surveillance, the program imposes a significant burden on the entire Internet-using public, representing an unreasonable intrusion upon constitutionally-protected privacy interests that outweighs any governmental interest.

1. The Privacy Interests Harmed by Upstream Surveillance Outweigh the Government's Interest in the Program

The privacy interests implicated by the challenged search program are far from "minimal." *Skinner*, 489 U.S. at 624. To the contrary, the Upstream program invades potentially every single communication sent or received through the Internet.

The Fourth Amendment privacy interest is particularly weighty where, as here, the deprivation and intrusion caused by the governmental actions impede on

communications, which by definition involve the exercise of associational and expressive rights protected by the First Amendment. *Stanford v. Texas*, 379 U.S. 476, 485 (1965) (requiring that the Fourth Amendment be applied with "scrupulous exactitude" when significant First Amendment rights are at stake); *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978). Accordingly, a search or seizure of "materials presumptively protected by the First Amendment" must be made pursuant to a warrant supported by probable cause. *See New York v. P. J. Video*, 475 U.S. 868, 873–75 (1986) (seizure of films or books implicates First Amendment concerns not raised by other kinds of seizures); *Stanford Daily*, 436 U.S. at 565 (recognizing that courts must "apply the warrant requirements with particular exactitude when First Amendment interests would be endangered by the search."); *Jacobsen*, 466 U.S. at 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."). In fact, the Fourth Amendment explicitly extends to "papers" and "effects" in part *because* the Founding Fathers recognized that the "unrestricted power of search and seizure could also be an instrument for stifling liberty of expression." *Marcus v. Search Warrants of Prop. at 104 E. Tenth St., Kan. City, Mo.*, 367 U.S. 717, 729 (1961).

The communications intercepted under Section 702, including phone calls, emails, chats, video calls, and text messages, are the modern equivalent of one's "papers" and "effects." Like the digital devices used to send and receive them, Internet communications comprise "a digital record of nearly every aspect of [people's] lives—from the mundane to the intimate." *Riley*, 573 U.S. at 395. They have such significant expressive and associational implications that "some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010). As with the cell phone in *United States v. Cano* or the laptop in *United States v. Cotterman*, they "contain the most intimate details of our lives," the "uniquely sensitive nature" of which "carries with it a significant expectation of privacy." *United States v. Cano*, No. 17-50151, 2019 WL 3850607, at *8 (9th Cir. Aug. 16, 2019) (quoting *Cotterman*, 709 F.3d at 965–66). As a result, they demand the same Fourth Amendment protection as pamphlets, books, and letters do. *See Carpenter*, 138 S. Ct. at 2214 ("As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure [] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'") (quoting *Kyllo v. United States*, 544 U.S. 27, 34 (2001)); *see also 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.").

Moreover, the scope of the Upstream surveillance program means that, regardless of the weight of the individual intrusion, the collective effect is a massive intrusion on privacy interests in Internet communications. The volume of the data collected extends far beyond the scale of the searches that have historically been permitted under the "special needs" exception. *See Mohamud*, 843 F.3d at 440 (noting that collections of "vast" quantities of data are "troubling"). A surveillance program like the one challenged here, which allows the government to search all domestic individuals' communications, without judicial oversight or individualized suspicion, amounts to exactly the sort of "general, exploratory rummaging in a person's belongings" that the Fourth Amendment prohibits. *Coolidge*, 403 U.S. at 467. Worse, it is not just one individual's papers the government is rummaging through, but the communications belonging to millions of innocent people.

Such a significant intrusion on individual privacy inherently renders the Upstream surveillance program unreasonable under the Fourth Amendment. *See Maryland v. King*, 569 U.S. 435, 448 (2013) ("Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution."). National security is not a talisman that shields

the government from judicial oversight where it steps outside the bounds of the Fourth Amendment; to the contrary, the Supreme Court has rejected attempts to remove surveillance activities from the scope of the Fourth Amendment under the guise of protecting national security. *See Keith*, 407 U.S. at 320–21. This Court should do the same here.

2. Indiscriminately Seizing and Searching Communications Will Include Attorney-Client Communications and Therefore Impact Individuals' Sixth Amendment Rights

The Sixth Amendment requires, as a practical matter, that attorneys and clients be able to communicate without the risk of governmental oversight. The Upstream collections program places an unacceptable burden on that ability by subjecting a vast swath of otherwise private communications—including privileged communications with attorneys—to government examination. The "special needs" exception cannot justify subordinating this critical constitutional right.

As the Supreme Court has noted, for the attorney-client relationship to be effective it must be afforded "a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel." *Hickman v. Taylor*, 329 U.S. 495, 510 (1947); *see also Hunt v. Blackburn*, 128 U.S. 464, 470 (1888) ("The rule which places the seal of secrecy upon communications between client and attorney is founded upon the necessity, in the interest and administration of justice, of the

aid of persons having knowledge of the law and skilled in its practice, which assistance can only be safely and readily availed of when free from the consequences or the apprehension of disclosure.").

The NSA's Internet surveillance program threatens both the privacy of attorney-client communications and, by extension, the Sixth Amendment right to counsel itself, because the government's mass surveillance program inevitably captures attorney-client communications. Indeed, the NSA's partially declassified "minimization" procedures recognize that privileged materials are regularly intercepted and expressly allow the agency to retain an attorney-client communication if it appears to contain "evidence of a crime." The NSA apparently places no limits on its ability to scour privileged communications unless they relate to a charged criminal case. And even then, the so-called "minimization" procedures only prohibit the government from using privileged communications "in any trial, hearing, or other proceeding" without the Attorney General's approval. The NSA is free to review and disseminate attorney-client communications "for intelligence purposes only" even when the client is under

indictment.[7] Far from "minimizing" the risk of Sixth Amendment violations, the NSA's procedures are an open invitation to government abuse, including an intrusion on the right to counsel.

The "minimization" procedures of this program are drastically less protective than those employed for all other types of domestic electronic surveillance. For instance, the Department of Justice ordinarily uses "taint team" procedures to protect the rights of criminal defendants, i.e. the Department appoints a separate, walled-off team of lawyers and agents to review seized emails in order to identify privileged materials that should not be in the hands of prosecutors. But even with these more robust procedures in place, courts have still taken a "skeptical view of the Government's use of 'taint teams'" and often order independent review by a special master. *See, e.g.*, *United States v. SDI Future Health, Inc.*, 464 F. Supp. 2d 1027, 1037 (D. Nev. 2006). The stark contrast between the NSA's handling of attorney-client communications and the rules that govern normal criminal investigations highlights the serious risks that Upstream

[7] *See* Exhibit B, Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended at pp. 7-8, available at Office of Director of National Intelligence Releases FISA Section 702 Documents, *Lawfare* (May 11, 2017), available at https://www.lawfareblog.com/office-director-national-intelligence-releases-fisa-section-702-documents

surveillance poses to attorney-client communications and, thus, to the very right to counsel.

Without the ability to protect attorney-client communications from prying governmental eyes, clients will be unable to avail themselves of the full benefits guaranteed by the Sixth Amendment, which depends on the ability of lawyers and their clients to engage in candid communication. The attorney-client privilege promotes "free and open exchange between the attorney and client" and "substantial questions of fundamental fairness are raised where," as inevitably is the case here, "the government invades that privilege." *United States v. Neill*, 952 F. Supp. 834, 839 (D.C. Cir. 1997).

III. CONCLUSION

The sheer scope of the challenged surveillance program—encompassing millions of individuals' Internet communications spanning a period of years—is almost impossible to grasp. The ubiquity of the surveillance, encompassing potentially every communication from every person, far exceeds any legitimate, much less "special," governmental need. *Amicus curiae* ask this Court to limit the government's ability to conduct such surveillance without the safeguard of the Fourth Amendment's warrant requirement, in order to ensure that the founding liberties underpinning our constitutional order remain in effect.

DATED: September 13, 2019

Respectfully submitted,

By_____*/s/ Benjamin B. Au*_____

BENJAMIN B. AU
TARA J. NORRIS
W. HENRY HUTTINGER
DURIE TANGRI LLP
530 Molino Street, Suite 111
Los Angeles, CA 90013
(415) 362-6666
bau@durietangri.com
tnorris@durietangri.com
hhuttinger@durietangri.com

CATHERINE R. GELLIS
3020 Bridgeway #247
Sausalito, CA 94965
(202) 642-2849
cathy@cgcounsel.com

MICHAEL PRICE
Fourth Amendment Center
NACDL
1660 L St. NW, 12th Floor
Washington, D.C. 20036
(202) 465-7615
mprice@nacdl.org

GIA L. CINCONE
9th Circuit Vice Chair
NACDL *AMICUS* COMMITTEE
Two Embarcadero Center, Suite 1900
San Francisco, California 94111
(415) 576-0200
gcincone@kilpatricktownsend.com

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

I hereby certify that pursuant to Fed. R. App. P. 32(a)(7)(C) and Ninth Circuit Rule 32-1 this brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and (6), because it is written in 14-pt Times New Roman font, and with the type-volume limitations of Fed. R. App. P. 29(d) and Ninth Circuit Rule 29-2(c), because it contains 5,356 words, excluding the portions excluded under Fed. R. App. P. 32(a)(7)(B)(iii). This count is based on the word count feature of Microsoft Word.

DATED: September 13, 2019

/s/ Benjamin B. Au
Benjamin B. Au
Counsel for Amicus 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 September 13, 2019.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

DATED: September 13, 2019

/s/ Benjamin B. Au
Benjamin B. Au
Counsel for Amicus Curiae