The Honorable James L. Robart

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

THE UNITED STATES DEPARTMENT OF JUSTICE, and LORETTA LYNCH, in her official capacity as Attorney General of the United States,

Defendants.

Case No. 2:16-cv-00538-JLR

MOTION TO FILE BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, ACCESS NOW, NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE, AND JENNIFER GRANICK IN SUPPORT OF PLAINTIFF'S OPPOSITION TO GOVERNMENT'S MOTION TO DISMISS

Noted on Motion Calendar:
September 23, 2016

TO: ALL PARTIES HEREIN AND THEIR COUNSEL OF RECORD

AND TO: CLERK OF THE ABOVE-ENTITLED COURT

Amici curiae Electronic Frontier Foundation, Access Now, New America's Open Technology Institute, and Jennifer Granick submit this request for leave to file the attached *amicus* brief pursuant to this Court's order on August 23, 2016 [Dkt. 42] in support of Plaintiff Microsoft Corporation's Opposition to Government's Motion to Dismiss [Dkt. 38].[1]

[1] *Amici* also requested and received consent to file from the government defendants.

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

I. STATEMENT OF INTEREST

Amici are non-profit organizations and a legal scholar who operate at the intersection of civil liberties and technology. We plainly have a different perspective and interest in this case than both Microsoft and the government. Representing the interests of technology users in the courts and through legislative and policy advocacy, our priority is to ensure that constitutional rights keep pace with innovation. We are particularly concerned when the interplay between law and technology prevents individuals from defending their constitutional rights. At issue in this case is the use by millions of people of "cloud" services to store highly personal and confidential information, and the applicability of a law—the Stored Communications Act (SCA), part of the Electronic Communications Privacy Act (ECPA)—that governs government access to such information, but makes it nearly impossible for the owners of that information to challenge government searches and seizures under the Fourth Amendment.

The **Electronic Frontier Foundation** ("EFF") is a San Francisco-based, non-profit, member-supported digital rights organization. Focusing on the intersection of civil liberties and technology, EFF actively encourages and challenges industry, government, and the courts to support free expression, privacy, and openness in the information society. Founded in 1990, EFF has over 25,000 dues-paying members.

Access Now is a non-governmental organization that defends and extends the digital rights of users at risk around the world, combining innovative policy, global advocacy, and direct technical support to fight for open and secure communications for all. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the Internet's continued openness and universality, and wields an action-focused global community of nearly half a million users from more than 185 countries. Access Now advocates globally for increased transparency around government surveillance and maintains the Transparency Reporting Index—a record of transparency reports from today's leading Internet companies and telcos.

New America's Open Technology Institute ("OTI") is New America's program dedicated to ensuring that all communities have equitable access to digital technology and its

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

benefits, promoting universal access to communications technologies that are both open and secure. New America is a Washington, DC-based think tank and civic enterprise committed to renewing American politics, prosperity, and purpose in the Digital Age through big ideas, bridging the gap between technology and policy, and curating broad public conversation. New America's OTI has a special interest in ensuring that Internet companies are able to be transparent with their customers about the extent of government demands for user data, as evidenced by research and advocacy work such as its extensive Transparency Reporting Toolkit project to standardize and promote internet transparency reporting, and its work to ensure that the USA FREEDOM Act of 2015 affirmed companies' legal right to report on national security demands.

Jennifer Granick is the Director of Civil Liberties at the Stanford Center for Internet and Society. Jennifer practices, speaks and writes about computer crime and security, electronic surveillance, consumer privacy, data protection, copyright, trademark and the Digital Millennium Copyright Act. She was selected by Information Security magazine in 2003 as one of 20 "Women of Vision" in the computer security field. She earned her law degree from University of California, Hastings College of the Law and her undergraduate degree from the New College of the University of South Florida.

II. *AMICI*'S BRIEF OFFERS UNIQUE AND HELPFUL INFORMATION

Amici's brief would provide the Court with unique and helpful information regarding the constitutionality of the SCA under the Fourth Amendment.

Our brief includes an historical overview of how the content of communications has been protected by the Fourth Amendment. We show that various courts have found that individuals have a reasonable expectation of privacy in their communications even when those communications have been facilitated by a third party. Thus we show that the "third-party doctrine" is inapplicable to personal and confidential content stored in the "cloud" by service providers such as Microsoft.

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

We also discuss precedent holding that government notice is a component of "reasonableness" under the Fourth Amendment. Thus the government is required to notify the parties to communications and other content creators when the government seeks to access that content—regardless of whether the access is by technological means or is justifiably conducted in secret for a limited time, or the legal process is served on a third party such as Microsoft.

We argue that government notice to the targets of an investigation is important when the government seeks to access "cloud" content because notice is not only a constitutional obligation on the government, it is often the only means by which accountholders may be able to vindicate their right to be free from unreasonable searches and seizures under the Fourth Amendment.

III. CONCLUSION

Amici respectfully request that the Court grant leave to file the attached *amicus* brief in support of Microsoft.

Dated this 2nd day of September, 2016.

Respectfully Submitted,

FOCAL PLLC

s/ Venkat Balasubramani
Venkat Balasubramani, WSBA #28269
900 1st Avenue S., Suite 203
Seattle, Washington 98134
Tel: (206) 529-4827
Fax: (206) 260-3966
Email: venkat@focallaw.com

Lee Tien
Sophia Cope
Andrew Crocker Nathan Cardozo
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Attorneys for Amici Curiae Electronic Frontier Foundation, Access Now, New America's Open Technology Institute, and Jennifer Granick

CERTIFICATE OF SERVICE

I hereby certify that on September 2, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to those attorneys of record registered on the CM/ECF system.

DATED this 2nd day of September, 2016.

FOCAL PLLC
Attorneys for Amici Curiae

By: *s/ Venkat Balasubramani*
Venkat Balasubramani, WSBA #28269
900 1st Avenue S., Suite 203
Seattle, Washington 98134
Tel: (206) 529-4827
Fax: (206) 260-3966
Email: venkat@focallaw.com

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

The Honorable James L. Robart

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

THE UNITED STATES DEPARTMENT OF JUSTICE, and LORETTA LYNCH, in her official capacity as Attorney General of the United States,

Defendants.

Case No. 2:16-cv-00538-JLR

[PROPOSED] ORDER GRANTING MOTION TO FILE BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, ACCESS NOW, NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE, AND JENNIFER GRANICK IN SUPPORT OF PLAINTIFF'S OPPOSITION TO GOVERNMENT'S MOTION TO DISMISS

Noted on Motion Calendar:
September 23, 2016

ORDER

Having considered the unopposed Motion to File Brief of *Amici Curiae* Electronic Frontier Foundation, Access Now, New America's Open Technology Institute, and Jennifer Granick in support of Plaintiff's Opposition to Government's Motion to Dismiss,

IT IS HEREBY ORDERED that the Motion to File Brief of *Amici Curiae* is GRANTED and the proposed brief submitted with the application is deemed filed.

DATED:

_____
JAMES L. ROPART
UNITED STATES DISTRICT JUDGE

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

Presented by:

FOCAL PLLC

Venkat Balasubramani, WSBA #28269
900 1st Avenue S., Suite 203
Seattle, Washington 98134
Tel: (206) 529-4827
Fax: (206) 260-3966
Email: venkat@focallaw.com

Lee Tien
Sophia Cope
Andrew Crocker
Nathan Cardozo
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Attorneys for Amici Curiae
Electronic Frontier Foundation, Access Now,
New America's Open Technology Institute,
and Jennifer Granick

The Honorable James L. Robart

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

THE UNITED STATES DEPARTMENT OF JUSTICE, and LORETTA LYNCH, in her official capacity as Attorney General of the United States,

Defendants.

Case No. 2:16-cv-00538-JLR

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, ACCESS NOW, NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE, AND JENNIFER GRANICK IN SUPPORT OF PLAINTIFF'S OPPOSITION TO GOVERNMENT'S MOTION TO DISMISS

Amici curiae Electronic Frontier Foundation, Access Now, New America's Open Technology Institute, and Jennifer Granick submit this *amicus* brief in support of Plaintiff Microsoft Corporation's Opposition to Government's Motion to Dismiss [Dkt. 38]. We have separately requested leave to file this *amicus* brief pursuant to this Court's order on August 23, 2016 [Dkt. 42].

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amici curiae* Electronic Frontier Foundation, Access Now, and New America's Open Technology Institute state that they do not have a parent corporation, and that no publicly held corporation owns 10% or more of the stock of *amici*.

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

TABLE OF CONTENTS

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION ii

TABLE OF CONTENTS iii

TABLE OF AUTHORITIES iv

INTEREST OF *AMICI* 1

INTRODUCTION 1

ARGUMENT 3

I. THE FOURTH AMENDMENT PROTECTS DIGITAL CONTENT 3

II. THE NOTICE REQUIREMENT APPLIES TO DIGITAL SEARCHES AND SEIZURES 5

III. SECTION 2703 IS UNCONSTITUTIONAL TO THE EXTENT IT AUTHORIZES NO-NOTICE WARRANTS FOR DIGITAL CONTENT STORED BY THIRD PARTIES 7

IV. NOTICE BY INTERMEDIARIES TO ACCOUNTHOLDERS IS NO SUBSTITUTE FOR GOVERNMENT NOTICE 9

V. CONCLUSION 10

CERTIFICATE OF SERVICE 12

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

TABLE OF AUTHORITIES

Cases

Berger v. State of New York,
388 U.S. 41 (1967) 3, 6, 7

City of Los Angeles v. Patel,
135 S. Ct. 2443 (2015) 2

Dalia v. United States,
441 U.S. 238 (1979) 7

Ex Parte Jackson,
96 U.S. 727 (1877) 3

Hudson v. Michigan,
547 U.S. 586 (2006) 6

In re Grand Jury Subpoena, JK-15-029 v. Kitzhaber,
2016 WL 3745541 (9th Cir. 2016) 5

Katz v. United States,
389 U.S. 347 (1967) 3, 4, 5, 7

Kyllo v. United States, 533 U.S. 27 (2001) 8

Lambert v. California,
355 U.S. 225 (1957) 10

Lavan v. City of Los Angeles,
693 F.3d 1022 (9th Cir. 2012) 10

Olmstead v. United States,
277 U.S. 438 (1928) 3, 6

People v. Superior Court of Butte County,
275 Cal. App. 2d 489 (1969) 3

R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist. No. 2149,
894 F.Supp.2d 1128 (D. Minn. 2012) 4

Richards v. Wisconsin,
520 U.S. 385 (1997) 6, 7, 8, 9

Riley v. California,
134 S. Ct. 2473 (2014) 8

Smith v. Maryland,
442 U.S. 735 (1979) 3

United States v. Ali,
870 F.Supp.2d 10 (D. D.C. 2012) 4

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

United States v. Comprehensive Drug Testing, Inc.,
621 F.3d 1162 (9th Cir. 2010) 4

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013) 8

United States v. Donovan,
429 U.S. 413 (1977) 7

United States v. Eastman,
465 F.2d 1057 (3d Cir. 1972) 10

United States v. Forrester,
512 F.3d 500 (9th Cir. 2008) 4

United States v. Freitas,
800 F.2d 1451 (9th Cir. 1986) 6, 10, 11

United States v. Jacobsen,
466 U.S. 109 (1984) 3

United States v. Jones,
132 S. Ct. 945 (2012) 4, 9

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 4

Wilson v. Arkansas,
514 U.S. 927 (1995) 6

Statutes

18 U.S.C. § 2518(8)(d) 7

18 U.S.C. § 2703 ..... 2, 4, 9

18 U.S.C. § 2705(b) 8

Legislative Authorities

Oversight of the United States Department of Justice, Hearing Before the House Committee on the Judiciary, Serial No. 113–43 (May 15, 2013) 5

Other Authorities

Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance (May 2014) 11

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

INTEREST OF *AMICI*[1]

Amici are non-profit organizations and a legal scholar that operate at the intersection of civil liberties and technology. Representing the interests of technology users in the courts and through legislative and policy advocacy, our priority is to ensure that constitutional rights keep pace with innovation. We are particularly concerned when the interplay between law and technology prevents individuals from defending their constitutional rights. At issue in this case is the use by millions of people of "cloud" services to store highly personal and confidential information, and the applicability of a law—the Stored Communications Act (SCA), part of the Electronic Communications Privacy Act (ECPA)—that governs government access to such information, but makes it nearly impossible for the creators of that information to challenge government searches and seizures under the Fourth Amendment.

INTRODUCTION

Fundamental to protection of the Fourth Amendment is the rule that the government must notify those whose privacy it invades, ensuring that it provides aggrieved persons with the knowledge needed to contest the lawfulness of government searches and seizures. While government notice has been a regular and constitutionally required feature of search and seizure warrants since the nation's founding, notice is especially important today for a simple reason: with the rise of the Internet and cloud services, private communications and information are stored in places where the parties to those communications and the owners or creators of that information cannot independently know whether the government has violated their Fourth Amendment rights. Dkt. # 28, Microsoft First Amended Complaint ¶ 3 ("FAC").

Amici support Microsoft's argument that 18 U.S.C. § 2703 "is facially unconstitutional to the extent it absolves the government of the obligation to give notice to a customer whose content it obtains by warrant, without regard to the circumstances of the particular case." FAC ¶

[1] No party or party's counsel participated in the writing of the brief in whole or in part. No party, party's counsel or other person contributed money to fund the preparation or submission of the brief.

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

35. Section 2703 governs government access to information stored in the cloud, yet it expressly authorizes no-notice warrants. *See* 18 U.S.C. § 2703(b)(1)(A) ("without required notice to the subscriber or customer, if the governmental entity obtains a warrant").

Amici argue that the Fourth Amendment's protection against unreasonable searches and seizures by the government broadly applies to digital information, including that stored in the cloud by third-party providers for the benefit of their customers. We also argue that the failure of the SCA to require government notice to targets of warrants for digital search and seizure violates the Fourth Amendment's reasonableness requirement.[2] That the government can obtain information from Microsoft or other cloud providers without disturbing the targets of investigations is a mere happenstance of modern technology and social practices that cannot affect the notice requirement.

[2] *Amici* believe that searches and seizures of communications content and records under subpoenas or court orders not based on probable cause are also subject to the notice requirement. *See, e.g., City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2453 (2015) (subpoena recipient's opportunity to "move to quash the subpoena before any search takes place" protects his or her Fourth Amendment rights, thus implying required government notice). But *amici* limit their argument here to the warranted searches and seizures challenged by Microsoft.

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

ARGUMENT

I. THE FOURTH AMENDMENT PROTECTS DIGITAL CONTENT

The content of communications are protected by the Fourth Amendment. This is true even when content is held by a third party, thus making the "third-party doctrine"[3] immaterial in this case. Almost 140 years ago, the Supreme Court ruled that the Fourth Amendment protected the content of letters sent in the postal mail from warrantless government search while in transit. *Ex Parte Jackson*, 96 U.S. 727, 733 (1877); *People v. Superior Court of Butte County*, 275 Cal. App. 2d 489, 496 (1969) ("first class mail is sacrosanct"); *United States v. Jacobsen*, 466 U.S. 109, 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."). Nearly a century later, the Court ruled that a person making a phone call on a public pay phone was entitled to expect the conversation would remain private. *Katz v. United States*, 389 U.S. 347 (1967). *See also Berger v. State of New York*, 388 U.S. 41 (1967).

In *Katz*, the Supreme Court articulated two core principles of Fourth Amendment jurisprudence. First, "the Fourth Amendment protects people, not places." *Katz*, 389 U.S. at 351. Second, the Fourth Amendment must be interpreted expansively to protect the privacy of communications. Although *Olmstead v. United States*, 277 U.S. 438 (1928), had held that wiretaps are not governed by the Fourth Amendment because they involve no "trespass" upon property, the Supreme Court overruled *Olmstead* largely because "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." *Katz*, 389 U.S. at 352.[4]

---

[3] *See generally Smith v. Maryland*, 442 U.S. 735 (1979).

[4] In *United States v. Jones*, 132 S. Ct. 945 (2012), the Court explained that government conduct can constitute a Fourth Amendment search either when it infringes on a reasonable expectation of privacy or when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing for the purpose of obtaining information. The Court stated, "Fourth Amendment rights do not rise or fall with the *Katz* formulation … for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

Today, the Internet and its ability to host "cloud" content plays a "vital role" in private communication. Federal courts across the country have applied the principles of *Katz* and reached the same result when considering digital content, finding that individuals can expect their emails and private social media conversations to remain private. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (reasonable expectation of privacy in emails); *R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist. No. 2149*, 894 F.Supp.2d 1128, 1132 (D. Minn. 2012) (reasonable expectation of privacy in private Facebook messages); *United States v. Ali*, 870 F.Supp.2d 10, 39 n. 39 (D. D.C. 2012) (reasonable expectation of privacy in emails). In *Warshak*, the Sixth Circuit held that there exists a reasonable expectation of privacy in the content of emails stored in the cloud by a commercial third-party service provider, and thus the Fourth Amendment requires that the government obtain a warrant based on probable cause before accessing such emails. *Warshak*, 631 F.3d at 288. The court further held Section 2703 unconstitutional to the extent it permits the government to obtain the content of communications without a warrant if those communications are older than 180 days. *See* 18 U.S.C. § 2703(a).[5] Additionally, the Ninth Circuit recently held that "[p]ersonal email can, and often does, contain all the information once found in the 'papers and effects' mentioned explicitly in the Fourth Amendment," and therefore the accountholder "has a strong claim to a legitimate expectation of privacy in his personal email, given the private information it likely contains." *In re Grand Jury Subpoena, JK-15-029 v. Kitzhaber*, 2016 WL 3745541, at *5 (9th Cir. 2016). *See also United States v. Forrester*, 512

areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding." *Id.* at 950. Thus government searches of emails and other communications may also qualify as the type of "trespass" that the framers sought to prevent when they adopted the Fourth Amendment.

[5] *Amici* contend that government surveillance authorized by the SCA is both a search and a seizure of communications. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171-72, 1176 (9th Cir. 2010) (*en banc*) (*per curiam*) (describing the government's copying of electronic data as a seizure); *Katz*, 389 U.S. at 354 (describing the government's recording of a phone call as a "search and seizure").

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

F.3d 500, 511 (9th Cir. 2008) (emails contain "content that the sender presumes will be read only by the intended recipient").

Indeed, the government agrees that a reasonable expectation of privacy attaches to cloud content, thus a warrant is required. In May 2013, then-Attorney General Eric Holder testified that "having a warrant to obtain the content of communication from a service provider is something that we support." *Oversight of the United States Department of Justice, Hearing Before the House Committee on the Judiciary*, Serial No. 113–43, at 87 (May 15, 2013).[6]

II. THE NOTICE REQUIREMENT APPLIES TO DIGITAL SEARCHES AND SEIZURES

When the Fourth Amendment was adopted, government threats to privacy and property were generally physical. And it was almost inherent in such searches and seizures that the target would know that the sanctity of her private life had been invaded. Yet the government can now intrude on a person's privacy or property whether or not the person knows of the intrusion. As Justice Brandeis warned, "Subtler and more far-reaching means of invading privacy have become available to the Government. . . . Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *Olmstead*, 277 U.S. at 473-74 (Brandeis, J., dissenting).

With the pervasiveness of cloud computing, "some day" is here. And today, as always, the notice requirement must reach as far as the Fourth Amendment itself does.

In *Wilson v. Arkansas*, 514 U.S. 927 (1995), the Supreme Court made clear that governmental provision of notice to targets of physical search or seizure "forms a part of the reasonableness inquiry under the Fourth Amendment." *Id.* at 929. Prior or contemporaneous notice need not always be given, but it is the default rule. *See Richards v. Wisconsin*, 520 U.S. 385, 387 (1997) ("the Fourth Amendment incorporates the common law requirement that police officers entering a dwelling must knock on the door and announce their identity and purpose

[6] https://judiciary.house.gov/wp-content/uploads/2016/02/113-43-80973-1.pdf.

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

before attempting forcible entry"); *Hudson v. Michigan*, 547 U.S. 586, 589 (2006) ("The common-law principle that law enforcement officers must announce their presence and provide residents an opportunity to open the door is an ancient one."); *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (finding sneak-and-peek warrant "constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry").

Because the notice requirement is a component of the reasonableness analysis, not of the Warrant Clause, it applies to the entire range of Fourth Amendment activities, including electronic searches conducted outside the home. For electronic eavesdropping, where "success depends on secrecy," the Supreme Court condemned a statute used to authorize surveillance of a business office for having "no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts." *Berger*, 388 U.S. at 60. Indeed, the *Berger* Court declared, "Such a showing of exigency, in order to avoid notice, would appear more important in eavesdropping, with its inherent dangers, than that required when conventional procedures of search and seizure are utilized." *Id.* Government notice to the surveillance target therefore cannot be dismissed as a mere fortuity of physical searches or seizures that occur within the person's sphere of awareness. Instead, to the extent that electronic surveillance was effectively invisible, and that prior notice could not be given, the Fourth Amendment requires government notice once any exigency justifying delay had lapsed. *Katz*, 389 U.S. at 355, n.16.

The federal Wiretap Act, largely inspired by *Berger*, unsurprisingly requires post-surveillance government notice to targets of interception orders. 18 U.S.C. § 2518(8)(d). *See also Dalia v. United States*, 441 U.S. 238, 248 (1979) (permitting covert entry into a business office in order to plant listening device, but noting "that Title III provided a constitutionally adequate substitute for advance notice by requiring that, once the surveillance operation is completed, the authorizing judge must cause notice to be served on those subjected to surveillance"); *United States v. Donovan*, 429 U.S. 413, 430 (1977) ("The *Berger* and *Katz* decisions established that

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

notice of surveillance is a constitutional requirement of any surveillance statute.") (quoting legislative history of Title III).

Berger and *Dalia* prove that the notice requirement is not limited to physical search and seizure cases of homes and businesses. The familiar "knock-and-announce" requirement is merely a species of the more general notice requirement. The government has a default duty to notify the persons whose privacy it invades, and courts craft that notice requirement in light of the characteristics of the type of surveillance, preserving the values protected by government notice while accommodating the legitimate interests of law enforcement. *Richards*, 520 U.S. at 394. Thus, the government is incorrect to argue that notice to Microsoft—as the recipient of the legal process, rather than the person whose privacy is invaded—is sufficient to satisfy the Fourth Amendment. Dkt. 38 at 22.

III. SECTION 2703 IS UNCONSTITUTIONAL TO THE EXTENT IT AUTHORIZES NO-NOTICE WARRANTS FOR DIGITAL CONTENT STORED BY THIRD PARTIES

If the government intrudes into a person's office to seize documents from a cabinet or device, the government clearly has a default obligation to provide notice of its presence and authority, subject to recognized judicial exceptions for exigency. But under the SCA, the government not only has no baseline duty to notify the person, it can also gag the service provider. 18 U.S.C. § 2705(b). Persons should not be deprived of notice, and the government should not be excused from providing notice, merely because they use cloud services to store their private communications and information. *Riley v. California*, 134 S. Ct. 2473, 2494-95 (2014) ("that technology now allows an individual to carry … in his hand" a cell phone containing "the privacies of life" "does not make the information any less worthy of the protection for which the Founders fought") (internal quotation marks and citations omitted); *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (when confronted by new technologies, courts must "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted"). In short, "technology matters." *United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (*en banc*).

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

Moreover, that the SCA expressly authorizes no-notice warrants in general alone renders it unconstitutional under the Fourth Amendment, because the statute creates a prohibited blanket exception to the notice requirement by insulating an entire category of searches from judicial review. *Richards*, 520 U.S. at 388, 394 (rejecting blanket notice exception for all felony drug investigations and stating, "in each case, it is the duty of a court confronted with the question to determine whether the facts and circumstances of the particular entry justified dispensing with the knock-and-announce requirement").

Equally important, reasons for dispensing with the notice requirement recognized in other contexts are largely inapplicable to the digital searches and seizures authorized by the SCA. For instance, the knock-and-announce requirement for prior or contemporaneous notice may "give way under circumstances presenting a threat of physical violence or where police officers have reason to believe that evidence would likely be destroyed if advance notice were given." *Richards*, 520 U.S at 391 (internal quotation marks and citation omitted). But for searches under the SCA, where the warrant is served on an electronic communications service or remote computing service provider—not directly on the person or persons whose privacy is invaded—there is no threat of physical violence remotely comparable to that of an armed homeowner overreacting to police at the door. Nor is there any realistic chance that digital content will be destroyed were notice given to the target. The SCA expressly authorizes the government to compel service providers to preserve evidence even before a warrant is presented. 18 U.S.C. § 2703(f).

Privacy, of course, is the key value here. Searches and seizures intrude on Fourth Amendment privacy as well as property interests, whether or not the person knows of them.[7] In

[7] First Amendment rights are also implicated. While Microsoft champions its First Amendment rights to inform its users of government intrusions, the knowledge that the government searches and seizes our communications—but does not notify us—produces the worst kind of chilling effect, a general awareness of widespread surveillance with no particular knowledge of who is being watched. *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("Awareness that the Government may be watching chills associational and expressive freedoms.").

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

today's world of communications intermediaries and digital information, that concern is far greater than before, because we cannot know about a government search or seizure of digital information in the first place unless the government tells us (or allows the intermediary to do so). And we cannot challenge such searches as unlawful without such knowledge. *See United States v. Eastman*, 465 F.2d 1057, 1063, n.13 (3d Cir. 1972) (Wiretap Act notice provision "intended to provide the defendant whose telephone has been subject to wiretap an opportunity to test the validity of the wiretapping authorization").

Notice does not only promote government accountability for those who are targets. If a target's emails are searched and seized, every party to those emails has also had his or her privacy invaded. Notice to the target will promote accountability for them as well. More generally, notice safeguards the greater cause of public accountability. Targets can challenge government action with fuller information about why and how government conducts surveillance—information that can lead to judicial, congressional or public scrutiny and thus robust oversight of surveillance practices. Without notice, the government can avoid judicial determinations, legislative action or public debate that might limit its discretion.[8]

IV. NOTICE BY INTERMEDIARIES TO ACCOUNTHOLDERS IS NO SUBSTITUTE FOR GOVERNMENT NOTICE

Although Microsoft is arguing for the ability to notify users of government access to their online files, it is important to underscore that the constitutional obligation of notice belongs to the government, not to Microsoft or any other service provider. The notice requirement has always been about the government announcing its presence and its authority, and the lack of notice affects the validity of a warrant. *See Freitas*, 800 F.2d at 1456 ("the absence of any notice

[8] The notice requirement is also essential to due process. *See Lambert v. California*, 355 U.S. 225, 228 (1957) ("Engrained in our concept of due process is the requirement of notice. Notice is sometimes essential so that the citizen has the chance to defend charges."); *Lavan v. City of Los Angeles*, 693 F.3d 1022, 1032 (9th Cir. 2012) ("the government may not take property like a thief in the night; rather, it must announce its intentions and give the property owner a chance to argue against the taking") (internal quotation marks and citation omitted).

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

requirement in the warrant casts strong doubt on its constitutional adequacy"). No private entity can cure a defective warrant.

Constitutional rules cannot depend on the varied and variable behavior of private actors. Microsoft could change its policy of providing notice to its customers. Other service providers may not even have a policy of always providing notice.

Or Microsoft may be placed in situations where it is not sure whether it can lawfully provide notice, or, more likely, where Microsoft simply lacks the knowledge that notice is now required. For instance, the Fourth Amendment requires the government to provide reasonably prompt notice in the absence of specific showings that would justify delay. *Freitas*, 800 F.2d at 1456; *Dalia*, 441 U.S. at 247–48. But a service provider is unlikely to know anything about when notice need no longer be delayed. There is no reason to believe that Microsoft would know, weeks or months after it complied with a warrant, that the relevant investigation had ended or for some other reason no longer need be kept secret. Only the government possesses the relevant facts, and only the government is or can be bound by the Fourth Amendment to provide notice.[9]

V. CONCLUSION

For the foregoing reasons, this Court should deny the government's motion to dismiss Microsoft's Fourth Amendment claim.

[9] Notice to accountholders is also an international norm. *See Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance* (May 2014), http://necessaryandproportionate.org/principles [http://perma.cc/L4NU-4KMM] (explaining that "[t]hose whose communications are being surveilled should be notified of a decision authorising Communications Surveillance with enough time and information to enable them to challenge the decision or seek other remedies and should have access to the materials presented in support of the application for authorization … The obligation to give notice rests with the State, but communications service providers should be free to notify individuals of the Communications Surveillance, voluntarily or upon request.").

focal PLLC
900 1st Ave. S., Suite 203
Seattle, Washington 98134
telephone (206) 529-4827
fax (206) 260-3966

Dated this 2nd day of September, 2016.

Respectfully Submitted,

FOCAL PLLC

s/ Venkat Balasubramani
Venkat Balasubramani, WSBA #28269
900 1st Avenue S., Suite 203
Seattle, Washington 98134
Tel: (206) 529-4827
Fax: (206) 260-3966
Email: venkat@focallaw.com

Lee Tien
Sophia Cope
Andrew Crocker Nathan Cardozo
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Attorneys for Amici Curiae Electronic Frontier Foundation, Access Now, New America's Open Technology Institute, and Jennifer Granick

CERTIFICATE OF SERVICE

I hereby certify that on September 2, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to those attorneys of record registered on the CM/ECF system.

DATED this 2nd day of September, 2016.

FOCAL PLLC
Attorneys for Amici Curiae

By: *s/ Venkat Balasubramani*
Venkat Balasubramani, WSBA #28269
900 1st Avenue S., Suite 203
Seattle, Washington 98134
Tel: (206) 529-4827
Fax: (206) 260-3966
Email: venkat@focallaw.com