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.

NO. 2:16-cv-00538-JLR

UNOPPOSED MOTION FOR LEAVE FILE BRIEF AS *AMICI CURIAE* BY APPLE, LITHIUM TECHNOLOGIES, MOZILLA, AND TWILIO IN SUPPORT OF MICROSOFT CORPORATION'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Noted for consideration:
September 2, 2016

SAVITT BRUCE & WILLEY LLP
1425 Fourth Avenue Suite 800
Seattle, Washington 98101-2272
(206) 749-0500

Apple, Lithium Technologies, Mozilla, and Twilio ("Amici"), respectfully submit this unopposed[1] motion for leave to appear as *amici curiae* and file the brief attached as Exhibit A in support of Microsoft Corporation and in opposition to the government's motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6). In support of their motion, Amici state as follows.

I. INTEREST OF AMICI

Apple, Lithium Technologies, Mozilla, and Twilio ("Amici") respectfully move for leave to appear as *amici curiae* and file the brief attached as Exhibit A in support of Microsoft Corporation and in opposition to the government's motion to dismiss pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6). In support of their motion, Amici state as follows.

Apple is committed to bringing the best user experience to its customers around the globe through its innovative hardware, software, and services. Apple leverages its unique ability to design and develop its operating systems, hardware, application software, and services to provide its customers new products and solutions with superior ease-of-use, seamless integration, and innovative design. In addition to selling iPhones, iPads, and personal computers, Apple also offers iCloud—a cloud service for storing photos, contacts, calendars, documents, device backups and more, keeping everything up to date and available to customers on whatever device they are using. Apple is committed to helping users understand how it handles their personal information and strives to provide straightforward disclosures regarding when it is compelled to comply with request for user data from law enforcement. Between July 1, 2015 and December 31, 2015, Apple received approximately over 1,000 requests from United States law enforcement authorities for user iCloud data.[2]

---

[1] Counsel for Microsoft and the Government have represented to Amici that they consent to the granting of Amici's Motion for Leave to File Brief and will not be opposing Amici's Motion. The parties also agree to the filing of Amici's Motion as an unopposed motion and noting it for same-day consideration under Local Rule 7(d)(1).

[2] *See, e.g.*, APPLE, Report on Government Information Requests (July 1 – December 31, 2015) (March 18, 2016), http://images.apple.com/legal/privacy/transparency/requests-2015-H2-en.pdf.

SAVITT BRUCE & WILLEY LLP
1425 Fourth Avenue Suite 800
Seattle, Washington 98101-2272
(206) 749-0500

So far in 2016, Apple has received approximately 590 nondisclosure orders of indefinite duration in connection with various forms of legal process.

Lithium Technologies provides businesses with a software-as-a-service (SaaS) technology platform on which to build vibrant online communities that drive sales, reduce service costs, accelerate innovation and grow brand advocacy. The Lithium Technologies platform delivers a seamless digital customer experience across websites, social channels and mobile devices. Businesses in more than 34 countries rely on Lithium Technologies to help them connect, engage, and understand their total community of customers and business partners. With more than 100 million unique monthly visitors over all Lithium Technologies communities and another 750 million online profiles, Lithium Technologies has one of the largest digital footprints in the world. Lithium Technologies customers rely on it to protect the privacy and security of their data; Lithium Technologies therefore strives to provide its customers and users with notice of any required data disclosures to law enforcement.

Mozilla is a global, mission-driven organization that works with a worldwide community to create open source products like its Firefox browser. Its mission is guided by the Mozilla Manifesto, a set of principles recognizing that, among other things, that individuals' security and privacy on the Internet are fundamental and must not be treated as optional. Transparency and openness are among Mozilla's founding principles and embedded in Mozilla's culture: from open source publicly auditable software to weekly public meetings. In furtherance of that Mozilla has also adopted data privacy principles that emphasize transparency, user control, limited data collection, and multi-layered security control and practices. This includes transparency regarding law enforcement requests for user data.[3]

Twilio is a cloud communications platform that makes communications easy and powerful. With Twilio's platform, businesses can embed real-time communication and

[3] Transparency Report (Reporting Period: January 1, 2015 to December 31, 2015), MOZILLA, https://www.mozilla.org/en-US/about/policy/transparency/jan-dec-2015/ (last visited Sept. 2, 2016).

SAVITT BRUCE & WILLEY LLP
1425 Fourth Avenue Suite 800
Seattle, Washington 98101-2272
(206) 749-0500

authentication capabilities directly into their software applications. Twilio's developer ecosystem, customers and end users expect Twilio to protect their personal information, sensitive data and user privacy. Transparency about law enforcement requests for user data is one of Twilio's core values. In the second half of 2015, Twilio received over 300 requests for user data from law enforcement, including 92 from the federal Government. As set forth in Twilio's privacy policy and transparency report, Twilio notifies customers of compliance with a law enforcement request whenever not prohibited from doing so.[4]

Amici have a strong interest in this case and have a valuable perspective on the importance on their ability to speak directly to their customers and users and regarding third-party and government demands for their data. Although Amici all regularly comply with valid legal process when they receive it, they are committed to ensuring that Government requests for user data are made within the bounds of applicable law and in a manner that allows their users to exercise their constitutional rights.

II. ARGUMENT

The Court has broad discretion to permit a non-party to participate in an action as amicus curiae. *See, e.g., Gerritson v. de la Madrid Hurtado*, 819 F.2d 1511, 1514 n.3 (9th Cir. 1987); *Skokomish Indian Tribe v. Goldmark*, C13-5071JLR, 2013 WL 5720053, at *1 (W.D. Wash. Oct. 21, 2013) ("The court has 'broad discretion' to appoint amicus curiae."); *Nat. Res. Def. Council v. Evans*, 243 F. Supp. 2d 1046, 1047 (N.D. Cal. 2003) (amici "may file briefs and may possibly participate in oral argument" in district court actions). Indeed, "[d]istrict courts frequently welcome amicus briefs from non-parties concerning legal issues that have potential ramifications beyond the parties directly involved or if the amicus has 'unique information or perspective that can help the court beyond the help that the lawyers for the parties are able to provide.'" *Sonoma Falls Dev., LLC v. Nevada Gold & Casinos, Inc.*, 272 F. Supp. 2d 919, 925 (N.D. Cal. 2003) (*quoting Cobell v. Norton*, 246 F Supp 2d

[4] Twilio Transparency Report (Second Half of 2015), *available at* https://www.twilio.com/marketing/bundles/legal/resources/Twilio-Transparency-Report-Second-Half-2015.pdf

SAVITT BRUCE & WILLEY LLP
1425 Fourth Avenue Suite 800
Seattle, Washington 98101-2272
(206) 749-0500

59, 62 (D.D.C. 2003) (citation omitted). No special qualifications are required; an individual seeking to appear as amicus must merely make a showing that his participation is useful to or otherwise desirable to the court." *In re Roxford Foods Litig.*, 790 F.Supp. 987, 997 (E.D.Cal. 1991).

Because Amici will present unique perspectives as diverse cloud service providers and will represent the interests of millions of their enterprise customers and end-users, their participation as *amici curiae* is appropriate in this matter in which the Court will consider issues of particular public interest. *See Liberty Resources, Inc. v. Philadelphia Hous. Auth.*, 395 F. Supp. 2d 206, 209 (E.D. Pa. 2005). ("Courts have found the participation of an amicus especially proper . . . where an issue of general public interest is at stake."). This is because the primary role of an *amicus* is "to assist the Court in reaching the right decision in a case affected with the interest of the general public." *Russell v. Bd. of Plumbing Examiners of the County of Westchester*, 74 F.Supp.2d 349, 351 (S.D.N.Y. 1999). In Liberty Resources, a case brought by a disability rights advocacy group against a public housing authority, the court granted amicus curiae status to another advocacy group that represented residents of public housing because the group's participation "will serve to keep the Court apprised of the interests of non-disabled Section 8 voucher recipients who may be affected by this case." *Id.* Similarly, Amici here will represent their own interests as providers offering a wide variety of cloud computing services as well as the interests of their customers and end-users in transparency regarding government access to data. Accordingly, this Court should allow Amici to appear as *amici curiae* and present argument in support of Microsoft in connection with the Government's Motion to Dismiss.

SAVITT BRUCE & WILLEY LLP
1425 Fourth Avenue Suite 800
Seattle, Washington 98101-2272
(206) 749-0500

III. CONCLUSION

For these reasons, Amici respectfully request that this Court enter an order granting Amici leave to file the brief attached hereto as Exhibit A in support of Microsoft Corporation.

DATED: September 2, 2016.

SAVITT BRUCE & WILLEY LLP

By: */s/ Miles A. Yanick*
Miles A. Yanick, WSBA #26603
Tel.: (206) 749-0500
Fax: (206) 749-0600
Email: myanick@sbwllp.com

ZWILLGEN PLLC
Marc Zwillinger *(pro hac vice pending)*
Jacob Sommer *(pro hac vice pending)*
Nury Siekkinen *(pro hac vice pending)*
1900 M Street NW, Suite 250
Washington, D.C. 20036
Tel.: (202) 296-3585
Email: marc@zwillgen.com
jake@zwillgen.com
nury@zwillgen.com

Attorneys for Apple, Lithium Technologies, Mozilla, and Twilio

CERTIFICATE OF SERVICE

I hereby certify that on September 2, 2016, I electronically filed the foregoing **UNOPPOSED MOTION FOR LEAVE FILE BRIEF AS *AMICI CURIAE* BY APPLE, LITHIUM TECHNOLOGIES, MOZILLA, AND TWILIO IN SUPPORT OF MICROSOFT CORPORATION'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS** with the Clerk of the Court using the CM/ECF system, which will send notification of each filing to those attorneys of record registered on the CM/ECF system.

DATED: September 2, 2016.

SAVITT BRUCE & WILLEY LLP

By: */s/ Miles A. Yanick*
Miles A. Yanick, WSBA #26603
Tel.: (206) 749-0500
Fax: (206) 749-0600
Email: myanick@sbwllp.com

SAVITT BRUCE & WILLEY LLP
1425 Fourth Avenue Suite 800
Seattle, Washington 98101-2272
(206) 749-0500

Exhibit A

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.	NO. 2:16-cv-00538-JLR **BRIEF OF *AMICI CURIAE* APPLE, LITHIUM TECHNOLOGIES, MOZILLA, AND TWILIO IN SUPPORT OF MICROSOFT CORPORATION'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS**

SAVITT BRUCE & WILLEY LLP
1425 Fourth Ave. Ste 800 Seattle, WA 98101 (206) 749-0500

TABLE OF CONTENTS

SAVITT BRUCE & WILLEY LLP
1425 Fourth Ave. Ste 800 Seattle, WA 98101 (206) 749-0500

TABLE OF AUTHORITIES

Cases

SAVITT BRUCE & WILLEY LLP
1425 Fourth Ave. Ste 800 Seattle, WA 98101 (206) 749-0500

Statutes, Rules, and Regulations

Constitutional Provisions

Other

SAVITT BRUCE & WILLEY LLP
1425 Fourth Ave. Ste 800 Seattle, WA 98101 (206) 749-0500

I. PRELIMINARY STATEMENT

Apple, Lithium Technologies, Mozilla, and Twilio ("Amici") respectfully submit this brief as *amici curiae* in support of Microsoft Corporation and in opposition to the Government's Motion to Dismiss pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6). Amici are cloud service providers, like Microsoft, serving both business customers and individual users. Transparency regarding access to the data of all customers is a core value of each of the Amici. Collectively, Amici have received thousands of nondisclosure orders, many of unlimited or indefinite duration, which have severely impacted their ability to be transparent about Government access to the data of customers and users. For the reasons stated below, Amici support Microsoft's Opposition and urge the Court to reach the merits of this matter.

II. ARGUMENT

The pervasive practice of issuing nondisclosure orders of indefinite or unknown duration deprives Amici of the ability to speak to and be transparent with its customers and the public about who is accessing the data they store. This diminished transparency and suppressed speech not only hampers users' ability to assert their own rights but hinders Amici's ability to comply with contractual commitments, enterprise customer demands and compete with providers located outside the United States. The Government serves Amici collectively with thousands of pieces of legal process each year, from subpoenas to court orders to warrants. Gag orders issued under 18 U.S.C. § 2705(b) often accompany these requests, prohibiting Amici from disclosing Government demands for data to the affected customer. These nondisclosure orders are frequently unlimited in practice because their endpoint is unclear, and the practice is so common that it is impractical to challenge each of the orders, **as it would result in a high volume of litigated proceedings each year**. Indeed, Apple has received approximately 590 unlimited or indefinite duration gag orders in 2016 alone. Because transparency with business customers and end-users is a core value of the Amici, they each support the claims asserted in Microsoft's First Amended Complaint and urge the Court to deny the Government's Motion to Dismiss in order to reach the merits of these important issues.

SAVITT BRUCE & WILLEY LLP
1425 Fourth Ave. Ste 800 Seattle, WA 98101 (206) 749-0500

The continued use of Section 2705(b) as a basis to seek and obtain gag orders of unlimited or indefinite duration in the absence of a specific showing that the particular target of an investigation is likely to engage in behavior described in 18 U.S.C. § 2705(b)(2) systematically violates the First Amendment.[1] Under well-established First Amendment principles, strict scrutiny demands a narrow interpretation of Section 2705(b) to require a particularized showing of the need for nondisclosure in each case and a reasonable time limit on each nondisclosure order, such as the time limit set forth in Section 2705(a)'s delayed notice provision. In addition to the constitutional ramifications of nondisclosure orders of unlimited duration, these orders also present particular challenges to cloud providers like Amici who face competing regulatory and contractual obligations, for example, under the EU-U.S. Privacy Shield and contractual clauses concerning security and privacy. The volume of nondisclosure orders providers receive puts them in a unique position—they are the only parties that have the information necessary to assert both their own First Amendment rights and their customers' Fourth Amendment rights. Thus, any prudential limitations on third-party standing should be disregarded to protect the constitutional rights of users routinely being denied the knowledge that the Government has sought their data.

A. Courts Should Interpret Section 2705(b) to Require the Government to Make a Particularized Showing of Need Before Issuing a Nondisclosure Order.

Allowing the Government to obtain nondisclosure orders without a particularized showing of need specific to the case in question violates the First Amendment. Section 2705(b) as written does not specify whether a court must demand a particularized showing of need for a nondisclosure order in each case, and from Amici's experience, courts do not regularly undertake such an analysis. *See, e.g., In re Grand Jury Subpoena to Facebook*, No. 16-mc-01300-JO, slip op. at 1, 8 n.7 (E.D.N.Y. May 12, 2016) ("*Grand Jury Subpoena to Facebook*") (denying 15 applications for Section 2705(b) nondisclosure orders for failing to set forth particularized information about the underlying investigation and noting that such general applications "have [been] unquestioningly endorsed" by judges). Failing to find that Section 2705(b) requires a

[1] Amici have no objection to nondisclosure orders that are based on a particularized showing of need and for a reasonably limited duration, such as 90 days.

particularized need renders it unconstitutionally broad, because the goal of protecting the secrecy of investigations can be met through less restrictive means. To avoid this constitutional problem, the Court should interpret Section 2705(b) to require the Government to demonstrate a particular need for nondisclosure in each case.

1. Nondisclosure Orders Are Prior Restraints that Burden Amici's Core Political Speech.

The nondisclosure orders identified by Microsoft in its First Amended Complaint target core political speech. The question of the extent to which the Government can investigate citizens and how it can compel parties like Amici to participate in those investigations is highly political and subject to robust public debate, not just in the academic security and privacy community but by the press, and by politicians worldwide.[2] Amici's enterprise customers and end-users care tremendously about this issue and rely on information made available by Amici when making decisions about what products and companies to choose. Accordingly, Amici spend significant time, money and resources to implement privacy and security features in their products; provide enterprise customers and end-users with information about government demands; and explain how end-user data is collected, used, and shared. Amici make this information accessible to customers and end-users in sales decks; during contract negotiation; on their websites; in marketing campaigns; and through transparency reports.[3]

Transparency regarding that access is one of Amici's fundamental values. Amici make contractual commitments to customers that data will only be shared with others in narrow circumstances, and when that happens, that Amici will notify them. Nondisclosure orders issued

[2] *See, e.g.*, Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, HARV. L. & POL'Y REV. 313 (2012) ; Alan Butler, *How Would You Know if the Feds Searched Your E-mail?—ECPA's Missing Notice Requirement*, PRIVACY RIGHTS BLOG @ EPIC.ORG (Feb. 24, 2015, 4:15 PM), http://epic.org/blog/2015/02/ECPA-missing-notice-requirement.html; *see also* Ellen Nakashima, *Judge Criticizes Secrecy Rules Surrounding FBI Requests for Companies' Data*, The Washington Post (Aug. 5, 2016), https://www.washingtonpost.com/world/national-security/judge-criticizes-secrecy-rules-surrounding-fbi-requests-for-companies-data/2016/08/05/37f80ba6-5b2b-11e6-831d-0324760ca856_story.html.

[3] Indeed, some Amici engage in further political efforts around these issues through educational campaigns, advocating for legislative reform, and intervening in applicable legal cases. For example, several of the Amici joined in a letter to Congress concerning the Electronic Communications Privacy Act Amendments Act of 2015. Letter from Apple, Mozilla, *et al.* to Charles Grassley, Chairman, and Patrick Leahy, Ranking Member, Senate Judiciary Committee (May 25, 2016), *available at* http://www.digital4th.org/ wp-content/uploads/2016/05/ECPA-Provider-Emergency-Letter.pdf.

under Section 2705(b)—especially when they are of indefinite duration—silence Amici and prevent them from honoring such commitments. This is particularly troubling given that end-users would unavoidably have received notice of the Government's demand had the data been stored locally instead of in the cloud. Amici's desire to provide similar notice to users for cloud data, and to prevent the Government from engaging in silent data gathering, except in narrow circumstances is protected by the First Amendment. *See Gentile v. State Bar of Nevada*, 501 U.S. 1030, 1034 (1991) ("There is no question that speech critical of the exercise of the State's power lies at the very center of the First Amendment."). Corporations have First Amendment rights, including the right to express their viewpoint on core political issues. *Citizens United v. Fed. Election Comm'n*, 558 U.S. 310 (2010) (the "[G]overnment may not, under the First Amendment, suppress political speech on the basis of the speaker's corporate identity"). Accordingly, the First Amendment protects Amici's speech concerning Government requests for user data.

2. Strict Scrutiny Requires the Government to Make a Particularized Showing of Need Before Issuing a Non-Disclosure Order Under Section 2705(b).

A non-particularized showing of need fails strict scrutiny analysis in two ways – it fails to demonstrate a compelling need, and it fails to provide a narrowly tailored means to serve that interest. Under strict scrutiny review, a prior restraint is only permissible if it is (1) justified by a compelling Governmental interest and (2) narrowly tailored to serve that interest. *Brown v. Entm't Merchants Ass'n*, 564 U.S. 786, 799 (2011). Put another way, a prior restraint on speech "is valid only if it is the least restrictive means available to further a compelling government interest." *Berger v. City of Seattle*, 569 F.3d 1029, 1050 (9th Cir. 2009).

Although the Government may have a compelling interest in keeping ***certain*** investigations secret from the target in order to avoid adverse results in some cases, it does not have that compelling need in all investigations. Nor will disclosure to a provider's business customer always lead to a disclosure to the target of an investigation. Microsoft's complaint sufficiently alleges, and discovery will likely make clear, that nondisclosure orders are routinely based on the experience of law enforcement in other criminal matters and not based on specific

findings related to the target of the investigation. And that they are often issued under the catch-all provision of 18 U.S.C. § 2705(b), allowing such orders to be issued whenever they would result in "otherwise seriously jeopardizing an investigation or unduly delaying a trial."[4] (*See* Compl. ¶ 32.) Amici's experiences with nondisclosure orders confirm this practice. For example, some nondisclosure orders served on Amici concern accounts operated by Amici's business customers where the target is not the customer. In such cases, there is often no indication that disclosure to the customer would jeopardize the investigation aimed at the end-user.[5]

Overcoming a provider's First Amendment interests requires more than general statements and certifications without meaningful review. *See, e.g.*, *Boumediene v. Bush*, 553 U.S. 723 (2008); *In re Nat'l Sec. Letter*, 930 F. Supp. 2d 1064, 1077 (N.D. Cal. 2013); *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 882-83 (2d Cir. 2008). The need that would overcome a strict scrutiny analysis is a compelling need in the particular case, and should pertain to a particular target. The general need to avoid trial delays may be a societal interest, but it is not sufficiently compelling to overcome a third-party's First Amendment rights.[6]

Furthermore, even where the interest is compelling, the method of obtaining the nondisclosure orders must be narrowly tailored to serve that interest. On its face, Section 2705(b) is ambiguous. It does not specify whether the Government must demonstrate a particular showing of need for a nondisclosure order. If Section 2705(b) is interpreted to allow for just generalized articulations of need, it would burden more speech than needed to serve a compelling governmental interest. *See also, In re Nat'l Sec. Letter*, 930 F. Supp. 2d at 1075. Section 2705(b)

---

[4] In addition to the allegations in the Complaint, this court can also take judicial notice of Judge Orenstein's decision in *Grand Jury Subpoena to Facebook*, in which Judge Orenstein noted that he had received fifteen applications for non-disclosure orders under 18 U.S.C. § 2705(b) and "[i]n each case, the application relies on a boilerplate recitation of need that includes no particularized information about the underlying criminal investigation." *Id.* at 1.

[5] Moreover, some nondisclosure orders received by Amici do not even identify the provider as an entity to be gagged, but generally, impose nondisclosure on any provider who subsequently provides service to the customer.

[6] The authority cited by the Government supporting the general societal interest in avoiding trial delays pertains to the period between arrest and trial, and not the investigation. (*See* Gov't's Mot. to Dismiss at 21, ECF No. 38 ("Gov't's Mot."), *citing Flanagan v. United States*, 465 U.S. 259, 264-65 (1984) ("Delay between arrest and punishment prolongs public anxiety over community safety if a person accused of a serious crime is free on bail. It may also adversely affect the prospects for rehabilitation.")).

should be interpreted, instead, to require the Government to make a ***particularized*** showing in each case. This reading of 2705(b) would be less restrictive and would match the remedy – the nondisclosure order – to the Government's interest. And it is unclear how the Government is harmed by tying the need for nondisclosure to the particular facts of the case, or why it would resist such an interpretation.[7] A broader interpretation of Section 2705(b) – allowing nondisclosure orders to be issued based on the Government's experience in other cases – renders Section 2705(b) unconstitutional.

This is essentially the conclusion reached by Magistrate Judge Orenstein in *Grand Jury Subpoena to Facebook*. In that case, the court denied fifteen applications for nondisclosure orders under Section 2705(b) containing substantially the same assertions that disclosure by service providers such as Facebook would or could result some of the harms enumerated in Section 2705(b)(1)-(5). Slip Op. at 1-3. These assertions, however, were generalized and not tied to any particular facts of the underlying investigation. *Id.* at 3. The court reasoned:

> [T]here is no reason to assume that tipping off an investigative target to the instigation's existence necessarily 'will' result in one of the harms contemplated by [Section 2705(b)]. To be sure, such information can easily have such an effect. But if Congress presumed that providing such information to an investigative target would inevitably lead to such consequences, the judicial finding [Section 2705(b)] requires would be meaningless. There will plainly on occasion be circumstances in which an investigative target either lacks the ability or the incentive to flee, to tamper with evidence, or otherwise to obstruct an investigation. To cite just two possibilities: the target may be incarcerated and lack effective access to evidence and witnesses; alternatively, the target may be a public figure with a strong incentive to affect a public posture of innocence and cooperation with law enforcement. In most cases, ***it seems likely that the government can easily make a showing*** that there is reason to believe that a target's knowledge of an investigation will indeed lead to obstructive behavior***—but not in every case.***

Id. at 7 (emphasis added). Put another way, because Section 2705(b) requires a judicial finding that there is reason to believe one of the enumerated harms will occur if disclosure is permitted, then it is clear that "sometimes notifying the target of the existence of an investigation will result in certain types of misconduct but that other times it will not." *Id.* Therefore, under Section

[7] It is hypocritical of the Government to suggest that Microsoft must challenge each order individually because each case involves particular facts, but not require the Government—who seeks to intrude upon the users' privacy—not to address those particular facts in each application for a nondisclosure order.

2705(b) "it is up to a judge to make the necessary determination in a given case based on the available evidence." *Id.* Without case-specific information, such a finding is impossible.

Accordingly, Section 2705(b) should be interpreted to require a particularized showing of need in each case to avoid the constitutional problems associated with a prior restraint on speech. "It is well established that courts should resolve ambiguities in statutes in a manner that avoids substantial constitutional issues." *See Mukasey*, 549 F.3d at 872. *See also Edward J. DeBartolo Corp. v. Fl. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988) ("where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress"); *Fair Hous. Council of San Fernando Valley v. Roommate.com, LLC*, 666 F.3d 1216, 1223 (9th Cir. 2012).

B. Nondisclosure Orders of Unlimited Duration Fail Strict Scrutiny.

Even where 2705(b) nondisclosure orders are issued after the Government makes a particularized showing, strict scrutiny requires that such orders not be issued for lengthy periods, and not for unlimited or unknown duration. *See In Matter of Search Warrant for [Redacted]@hotmail.com*, 74 F. Supp. 3d 1184, 1186 (N.D. Cal. 2014) ("*Hotmail*"), (refusing to issue nondisclosure order of indefinite duration though Government had made a particularized showing that disclosure would jeopardize investigation). Although Section 2705(a) nondisclosure orders are limited to 90-day periods, Section 2705(b) orders are not. In Amici's experience, this lack of specificity in Section 2705(b) has caused many courts and the Government to default to orders of unlimited or unknown duration, even though limited time periods for such orders would be less restrictive on providers' speech and would still serve the Government's legitimate interest in secrecy in some cases. These indefinite orders often persist even when the basis for the order—a threat to life or jeopardy to an investigation—has long since passed, leaving providers guessing about when they can or should challenge orders restraining their speech.

The pervasive use of nondisclosure orders of unlimited duration, based on the assumption that Section 2705(b) allows for such orders,[8] fails strict scrutiny. To satisfy strict scrutiny when seeking a lengthy or unlimited nondisclosure order, the Government must demonstrate there are no "less restrictive alternatives [that] would be at least as effective in achieving the Act's legitimate purpose…" *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 846 (1997). Here, however, other statutes demonstrate that there are less restrictive alternatives available. Section 2705(a), providing for notice to the target of an investigation to be delayed for a set amount of time—90 days—and requiring the Government to come back to court to justify any further delay, is an example of a less restrictive means of achieving the Government's interest in maintaining the secrecy of certain investigations. Both Sections 2705(a) and (b) list the same "adverse results" as potential bases for a nondisclosure order. Most of those are, by definition, limited in duration, and there is no basis for continued nondisclosure obligations after they have passed. Any danger to life or physical safety usually passes once the investigation ends or the target is arrested. 18 U.S.C. §§ 2705 (a)(2)(A), (b)(1). The same goes for flight from prosecution and destruction of evidence, intimidation of potential witnesses, or otherwise seriously jeopardizing an investigation or delaying a trial. *Id.* at §§ 2705(a)(2)(B)-(E), (b)(2)-(5).

Similarly, the statute governing "sneak and peek" warrants – which is also designed to protect the same governmental interests – only allows for notice to be delayed for a period of 30 days, unless the Government justifies a longer period for a particular case. *See* 18 U.S.C. §3103a. These two delayed-notice provisions demonstrate that the Government interests can be served adequately by less restrictive means. The temporal limitations contained in these other statutes properly place the burden on the Government—the party seeking to suppress speech—to justify

[8] One court has interpreted Section 2705(b) as prohibiting orders of indefinite duration unless the Government shows that such an order is necessary in a particular case. *See Hotmail*, 74 F. Supp. 3d at 1185 (Section 2705(b)'s requirement that a court preclude notice "for such period as the court deems appropriate" prohibited the issuance of an indefinite order absent justification for such an order); *Matter of Grand Jury Subpoena for: [Redacted]@yahoo.com*, 79 F. Supp. 3d 1091, 1094–95 (N.D. Cal. 2015) (holding same as in *Hotmail*). In the Amici's experience, most courts have not interpreted Section 2705(b) in this way.

SAVITT BRUCE & WILLEY LLP
1425 Fourth Ave. Ste 800 Seattle, WA 98101 (206) 749-0500

the continued suppression, rather than on the speaker.[9] Shifting the burden to the Government to justify, and continue to justify, a disfavored prior restraint on speech better comports with the First Amendment and the principles underlying the strict scrutiny test. The Government has not shown why these narrower limitations on secrecy are adequate under Sections 2705(a) and 3103a, but are inadequate for legal process under Section 2705(b), particularly where the same potential "adverse results" justify nondisclosure in all three cases.

By contrast, by allowing nondisclosure orders of unlimited duration, Section 2705(b) is "overbroad because [it] ensure[s] that nondisclosure continues longer than necessary to serve the [Government's] interests at stake." *In re Nat'l Security Letter*, 930 F. Supp. 2d at 1076. *See also Doe v. Gonzalez*, 500 F. Supp. 2d 379, 421 (S.D.N.Y. 2007), *aff'd in part, rev'd in part*, 549 F.3d 861 (2d Cir. 2008) ("Once disclosure no longer poses a threat to national security, there is no basis for further restricting recipients of National Security Letters from communicating their knowledge of the Government's activities."). And unlike shorter duration orders, they require providers to repeatedly ascertain the status of investigations, and then petition courts to rescind a prior nondisclosure order. *See In re Nat'l Security Letter*, 930 F. Supp. 2d at 1076 ("The issuance of a nondisclosure order is, in essence, a permanent ban on speech absent the rare recipient who has the resources and motivation to hire counsel and affirmatively seek review by a district court."). But "nothing in the statute suggests putting the burden on the provider to guess that circumstances might have changed so that a request to lift the order is warranted." *Hotmail*, 74 F. Supp. 3d at 1186. This process is expensive and places the burden, not on the Government that seeks to suppress speech, but on the provider that wishes to exercise its First Amendment rights.

C. Readily Available Gag Orders Negatively Impact Cloud Providers, Especially Outside the United States.

The inability to disclose legal requests causes particular harm to providers like Amici that have built their businesses on trust and transparency. A cornerstone of cloud computing is

[9] Indeed, in cases challenging gag orders of unlimited duration in the National Security letter context, courts have ordered the Government to review the justification for the non-disclosure Order every 180 days. *See Lynch v. Under Seal*, No. 15-cv-01180-JKB (D. Md. Nov. 17, 2015).

ensuring that customers trust their providers to handle their data, and that storing the data in the cloud is comparable to storing data locally. In fact, this was the very goal that ECPA was designed to further. *See* S. Rep. No. 99-541, at 5 (1986), *reprinted in* U.S.C.C.A.N. 3555, 3558 (noting that the lack of "Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology . . . may unnecessarily discourage potential customers from using innovative communications systems" and proposing ECPA as a remedy that strikes a balance between privacy and legitimate law enforcement needs). Furthermore, negotiated agreements, end-user terms, and privacy policies require providers like Amici to provide users with notice of how their data will be used, and allow users to trust providers with intimate details of their lives and work. If providers cannot disclose the existence of third-party requests, it significantly affects their ability to be transparent with their customers and lay the cornerstone of cloud computing: trusting another party to store your most valuable data. The inability to disclose law enforcement requests also prevents cloud providers from meeting customer demands and fulfilling contractual promises to customers to provide notice when their data is disclosed.

Gag orders of unlimited duration make fulfilling these promises to customers much more difficult or impossible. The problem is especially acute in the European Union, which has, through model contractual clauses and now the Privacy Shield, demanded that cloud providers give notice to users about how and when data is disclosed—including to law enforcement.[10] To compete, U.S. providers must comply with these contractual promises – particularly when contained in the EU's model contractual clauses – as an essential prerequisite to transferring data back to the U.S.[11] Nondisclosure orders of unlimited duration disadvantage American companies that do business globally by impairing their ability to provide required disclosures in Europe.

[10] *Privacy Shield Framework—Privacy Shield Principles, Notice,* U.S. Department of Commerce, https://www.privacyshield.gov/article?id=1-NOTICE (last visited Sept. 2, 2016).

[11] *The EU-U.S. Privacy Shield*, European Commission's DG Justice and Consumers (Feb. 8, 2016), http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm; *Data*

SAVITT BRUCE & WILLEY LLP
1425 Fourth Ave. Ste 800 Seattle, WA 98101 (206) 749-0500

D. Providers Have Standing to Assert the Fourth Amendment Rights of their Customers.

Microsoft has standing to assert its customers' Constitutional rights. Courts have allowed an organization with a close relationship to its customer to assert rights on the customer's behalf, especially when the customer is unlikely to do so. *Singleton v. Wulff*, 428 U.S. 106, 117-18 (1976); *see also Craig v. Boren*, 429 U.S. 190, 194-95 (1976). Providers, like Microsoft and Amici, have Article III standing, because each "faces an injury in the nature of the burden that it must shoulder to facilitate the Government's surveillances of its customers; that injury is obviously and indisputably caused by the Government through the directives; and this court is capable of redressing the injury." *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1008 (Foreign Int. Surv. Ct. Rev. 2008); *see also Craig*, 429 U.S. at 194. Limitations on the ability to vicariously assert the Fourth Amendment rights of others are prudential standing limitations only and can be overcome. *See Warth v. Seldin*, 422 U.S. 490, 501 (1975) (noting prudential nature of limitation can be relaxed). Amici's end-users, particularly those impacted by nondisclosure orders who have no knowledge of the issue, cannot dispute their specific cases with the Government or challenge the constitutionality of the statute. Amici's enterprise customers may be in a similar situation to the extent that they do not have knowledge of the nondisclosure orders to even be aware that there may be an ongoing contractual violation.

In the present context, Congress clearly understood that only ***providers*** would be in a position to challenge law enforcement process and has repeatedly built in provisions allowing providers to challenge various forms of legal process served upon them seeking customer data. *See* 18 U.S.C. §2703(d); *see also* 18 U.S.C. §3511(a); 50 U.S.C. §1881a(h)(4)(A). In these circumstances – where no notice is provided to the customer – providers are the ***only*** entities in a

---

Protection: Model Contracts for the transfer of personal data to third countries, European Commission's DG Justice and Consumers (Feb. 12 2015) http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

position to raise Fourth Amendment issues.[12]

Allowing a provider to challenge the practice at issue here on behalf of its users comports with the case law. In *Craig v. Boren*, the Supreme Court allowed a store to assert the Equal Protection rights of its customers in challenging a state statute regulating the sale of beer. The Court noted that "vendors and those in like positions have been uniformly permitted to resist efforts at restricting their operations by acting as advocates of the rights of third parties who seek access to their market or function." *Id.* at 195. That is the situation here. The non-disclosure orders at issue create a situation where it is unlikely—or impossible—that Microsoft's customers (and those of other providers such as Amici) can assert their own rights. Under these circumstances, Microsoft has standing to assert its customers' Fourth Amendment Rights.

III. CONCLUSION

The Government's pervasive use of generalized nondisclosure orders of unlimited duration burdens Amici's First Amendment rights. Interpreting 2705(b) to require a particularized showing of need for nondisclosure and requiring nondisclosure orders issued to providers to be limited in duration, would remedy the First Amendment problems inherent in such orders. These unlimited nondisclosure orders particularly disadvantage cloud providers like Amici because of their obligations under contractual provisions, data transfer agreements like the Privacy Shield, and general marketplace demands, which further supports interpreting ECPA to allow these providers to compete on a level playing field with entities outside the U.S. For these reasons and those stated in Microsoft's Opposition, the Government's Motion to Dismiss should be denied.

[12] The Government's reliance on exclusionary rule and Section 1983 cases is unavailing. *See Gov't's Mot.* at 10-11. *Rakas v. Illinois*, 439 U.S. 128 (1978), concerned with the use of the exclusionary rule as a vehicle for enforcing Fourth Amendment rights of another. The court reasoned that limiting the assertion of Fourth Amendment rights was permissible because the person whose rights were violated by the search could "seek redress" in a private action. *Id.* at 134. The ability to seek redress necessarily meant that the person whose rights were violated ***actually knew about the illegal search.*** Here, Amici's customers and end-users do not know that the Government has accessed their data and cannot "seek redress." *Moreland v. Las Vegas P.D* notes that third parties ***can*** assert the Fourth Amendment rights of another in Section 1983 actions where the "state's law authorizes a survival action … ." 159 F.3d 365, 369 (9th Cir. 1998) (internal citation omitted).

SAVITT BRUCE & WILLEY LLP
1425 Fourth Ave. Ste 800 Seattle, WA 98101 (206) 749-0500

DATED: September 2, 2016.

SAVITT BRUCE & WILLEY LLP

By: */s/ Miles A. Yanick*
Miles A. Yanick, WSBA #26603
Tel.: (206) 749-0500
Fax: (206) 749-0600
Email: myanick@sbwllp.com

ZWILLGEN PLLC
Marc Zwillinger *(pro hac vice pending)*
Jacob Sommer *(pro hac vice pending)*
Nury Siekkinen *(pro hac vice pending)*
1900 M Street NW, Suite 250
Washington, D.C. 20036
Tel.: (202) 296-3585
Email: marc@zwillgen.com
jake@zwillgen.com
nury@zwillgen.com

Attorneys for *Amici Curiae*

CERTIFICATE OF SERVICE

I hereby certify that on September 2, 2016, I electronically filed the foregoing **BRIEF OF *AMICI CURIAE* APPLE, LITHIUM TECHNOLOGIES, MOZILLA, AND TWILIO IN SUPPORT OF MICROSOFT CORPORATION'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS** with the Clerk of the Court using the CM/ECF system, which will send notification of each filing to those attorneys of record registered on the CM/ECF system.

DATED: September 2, 2016.

SAVITT BRUCE & WILLEY LLP

By: */s/ Miles A. Yanick*
Miles A. Yanick, WSBA #26603
Tel.: (206) 749-0500
Fax: (206) 749-0600
Email: myanick@sbwllp.com