

# Exhibit A

The Honorable James L. Robart

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

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**

**TABLE OF CONTENTS**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27

**I. PRELIMINARY STATEMENT ..... 1**

**II. ARGUMENT ..... 1**

    A. Courts Should Interpret Section 2705(b) to Require the Government to  
    Make a Particularized Showing of Need Before Issuing a Nondisclosure  
    Order. .... 2

        1. Nondisclosure Orders Are Prior Restraints that Burden  
        Amici’s Core Political Speech. .... 3

        2. Strict Scrutiny Requires the Government to Make a  
        Particularized Showing of Need Before Issuing a Non-  
        Disclosure Order Under Section 2705(b)..... 4

    B. Nondisclosure Orders of Unlimited Duration Fail Strict Scrutiny. .... 7

    C. Readily Available Gag Orders Negatively Impact Cloud Providers,  
    Especially Outside the United States..... 9

    D. Providers Have Standing to Assert the Fourth Amendment Rights of  
    their Customers..... 11

**III. CONCLUSION ..... 12**

**TABLE OF AUTHORITIES**

**Cases**

*Berger v. City of Seattle*, 569 F.3d 1029 (9th Cir. 2009) ..... 4

*Brown v. Entm't Merchants Ass'n*, 564 U.S. 786 (2011)..... 4

*Boumediene v. Bush*, 553 U.S. 723 (2008)..... 5

*Citizens United v. Fed. Election Comm'n*, 558 U.S. 310 (2010)..... 4

*Craig v. Boren*, 429 U.S. 190 (1976) ..... 11,12

*Doe v. Gonzales*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007)..... 9

*Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Const. Trades Council*,  
485 U.S. 568 (1988)..... 7

*Fair Hous. Council of San Fernando Valley v. Roommate.com, LLC*,  
666 F.3d 1216 (9th Cir. 2012) ..... 7

*Flanagan v. United States*, 465 U.S. 259 (1984) ..... 5

*Gentile v. State Bar of Nevada*, 501 U.S. 1030 (1991) ..... 4

*In re Grand Jury Subpoena to Facebook*,  
No. 1:16-mc-01300-JO (E.D.N.Y. May 12, 2016) ..... 2, 5-7

*In Matter of Search Warrant for [Redacted]@hotmail.com*,  
74 F. Supp. 3d 1184 (N.D. Cal. 2014) ..... 8, 9

*In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*,  
551 F.3d 1004 (Foreign Int. Surv. Ct. Rev. 2008)..... 11

*In re Nat'l Sec. Letter*, 930 F. Supp. 2d 1064 (N.D. Cal. 2013) ..... 5, 9

*John Doe, Inc. v. Mukasey*, 549 F.3d 861, 878 (2d Cir. 2008)..... 5, 7

*Lynch v. Under Seal*, No. 15-cv-01180-JKB (D. Md. Nov. 17, 2015)..... 9

*Matter of Grand Jury Subpoena for: [Redacted]@yahoo.com*,  
79 F. Supp. 3d 1091 (N.D. Cal. 2015)..... 8

*Moreland v. Las Vegas P.D.*, 159 F.3d 365 (9th Cir. 1998)..... 12

*Singleton v. Wulff*, 428 U.S. 106 (1976)..... 11

*Rakas v. Illinois*, 439 U.S. 128 (1978) ..... 12

*Reno v. Am. Civil Liberties Union*, 521 U.S. 844 (1997)..... 8

1 *Warth v. Seldin*, 422 U.S. 490 (1975)..... 11

2  
3 **Statutes, Rules, and Regulations**

4 Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 *et seq.*.....3, 10, 12

5 Fed. R. Civ. P. 12(b)(1) ..... 1

6 Fed. R. Civ. P. 12(b)(6) ..... 1

7 18 U.S.C. §2703(d)..... 11-12

8 18 U.S.C. §§ 2705(a) – (b) .....*passim*

9 18 U.S.C. § 2705 (a)(2)(A)..... 8

10 18 U.S.C. §§ 2705 (a)(2)(B)-(E) ..... 8

11 18 U.S.C. § 2705 (b)(1) ..... 8

12 18 U.S.C. §§ 2705 (b)(2)-(5) ..... 8

13 18 U.S.C. § 3103a..... 8

14 18 U.S.C. §3511(a)..... 11-12

15 50 U.S.C. §1881a(h)(4)(A)..... 11-12

16  
17 **Constitutional Provisions**

18 U.S. Const. amend. I.....*passim*

19 U.S. Const. amend. IV ..... 12

20 **Other**

21 Alan Butler, *How Would You Know if the Feds Searched Your E-mail?—*

22 *ECPA's Missing Notice Requirement*, PRIVACY RIGHTS BLOG @ EPIC.ORG

23 (Feb. 24, 2015, 4:15 PM), <http://epic.org/blog/2015/02/ECPA-missing-notice-requirement.html> ..... 3

24 *Data Protection: Model Contracts for the transfer of personal data to third countries,*

25 European Commission’s DG Justice and Consumers (Feb. 12 2015)

26 [http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).

27 ..... 10-11

1 Ellen Nakashima, *Judge Criticizes Secrecy Rules Surrounding FBI Requests for Companies’*  
 2 *Data*, The Washington Post (Aug. 5, 2016),  
 3 [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](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  
 4  
 5 Letter from Apple, Mozilla, *et al.* to Charles Grassley, Chairman, and Patrick Leahy,  
 6 Ranking Member, Senate Judiciary Committee (May 25, 2016), *available at*  
 7 <http://www.digital4th.org/wp-content/uploads/2016/05/ECPA-Provider-Emergency-Letter.pdf> ..... 3  
 8  
 9 *Privacy Shield Framework—Privacy Shield Principles, Notice*, U.S. Department of  
 10 Commerce, <https://www.privacyshield.gov/article?id=1-NOTICE> (last visited  
 11 Sept. 2, 2016)..... 10-11  
 12  
 13 S. Rep. No. 99-541 (1986), *reprinted in* U.S.C.C.A.N. 3555, 3558 ..... 10  
 14  
 15 Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA’s Secret Docket*,  
 16 HARV. L. & POL’Y REV. 313 (2012)..... 3  
 17  
 18 *The EU-U.S. Privacy Shield*, European Commission’s DG Justice and Consumers  
 19 (Feb. 8, 2016), [http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm) ..... 10  
 20  
 21  
 22  
 23  
 24  
 25  
 26  
 27

1 **I. PRELIMINARY STATEMENT**

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

11 **II. ARGUMENT**

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

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

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

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

27 <sup>1</sup> 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.

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

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

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

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

22 <sup>2</sup> See, e.g., Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, HARV. L. &  
 23 POL'Y REV. 313 (2012) ; Alan Butler, *How Would You Know if the Feds Searched Your E-mail?—ECPA's*  
 24 *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](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).

25 <sup>3</sup> Indeed, some Amici engage in further political efforts around these issues through educational campaigns,  
 26 advocating for legislative reform, and intervening in applicable legal cases. For example, several of the Amici  
 27 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>.

1 under Section 2705(b)—especially when they are of indefinite duration—silence Amici and  
 2 prevent them from honoring such commitments. This is particularly troubling given that end-  
 3 users would unavoidably have received notice of the Government’s demand had the data been  
 4 stored locally instead of in the cloud. Amici’s desire to provide similar notice to users for cloud  
 5 data, and to prevent the Government from engaging in silent data gathering, except in narrow  
 6 circumstances is protected by the First Amendment. *See Gentile v. State Bar of Nevada*, 501 U.S.  
 7 1030, 1034 (1991) (“There is no question that speech critical of the exercise of the State’s power  
 8 lies at the very center of the First Amendment.”). Corporations have First Amendment rights,  
 9 including the right to express their viewpoint on core political issues. *Citizens United v. Fed.*  
 10 *Election Comm’n*, 558 U.S. 310 (2010) (the “[G]overnment may not, under the First Amendment,  
 11 suppress political speech on the basis of the speaker’s corporate identity”). Accordingly, the First  
 12 Amendment protects Amici’s speech concerning Government requests for user data.

13 **2. Strict Scrutiny Requires the Government to Make a Particularized**  
 14 **Showing of Need Before Issuing a Non-Disclosure Order Under Section**  
 15 **2705(b).**

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

23 Although the Government may have a compelling interest in keeping *certain*  
 24 investigations secret from the target in order to avoid adverse results in some cases, it does not  
 25 have that compelling need in all investigations. Nor will disclosure to a provider’s business  
 26 customer always lead to a disclosure to the target of an investigation. Microsoft’s complaint  
 27 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

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

8 Overcoming a provider’s First Amendment interests requires more than general statements  
 9 and certifications without meaningful review. *See, e.g., Boumediene v. Bush*, 553 U.S. 723  
 10 (2008); *In re Nat’l Sec. Letter*, 930 F. Supp. 2d 1064, 1077 (N.D. Cal. 2013); *John Doe, Inc. v.*  
 11 *Mukasey*, 549 F.3d 861, 882-83 (2d Cir. 2008). The need that would overcome a strict scrutiny  
 12 analysis is a compelling need in the particular case, and should pertain to a particular target. The  
 13 general need to avoid trial delays may be a societal interest, but it is not sufficiently compelling to  
 14 overcome a third-party’s First Amendment rights.<sup>6</sup>

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

---

22 <sup>4</sup> In addition to the allegations in the Complaint, this court can also take judicial notice of Judge Orenstein’s  
 23 decision in *Grand Jury Subpoena to Facebook*, in which Judge Orenstein noted that he had received fifteen  
 24 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.

25 <sup>5</sup> 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.

26 <sup>6</sup> The authority cited by the Government supporting the general societal interest in avoiding trial delays pertains to  
 27 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.”)).

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

8 This is essentially the conclusion reached by Magistrate Judge Orenstein in *Grand Jury*  
9 *Subpoena to Facebook*. In that case, the court denied fifteen applications for nondisclosure orders  
10 under Section 2705(b) containing substantially the same assertions that disclosure by service  
11 providers such as Facebook would or could result some of the harms enumerated in Section  
12 2705(b)(1)-(5). Slip Op. at 1-3. These assertions, however, were generalized and not tied to any  
13 particular facts of the underlying investigation. *Id.* at 3. The court reasoned:

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

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

---

<sup>7</sup> 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.

1 2705(b) “it is up to a judge to make the necessary determination in a given case based on the  
2 available evidence.” *Id.* Without case-specific information, such a finding is impossible.

3 Accordingly, Section 2705(b) should be interpreted to require a particularized showing of  
4 need in each case to avoid the constitutional problems associated with a prior restraint on speech.  
5 “It is well established that courts should resolve ambiguities in statutes in a manner that avoids  
6 substantial constitutional issues.” *See Mukasey*, 549 F.3d at 872. *See also Edward J. DeBartolo*  
7 *Corp. v. Fl. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988) (“where an  
8 otherwise acceptable construction of a statute would raise serious constitutional problems, the  
9 Court will construe the statute to avoid such problems unless such construction is plainly contrary  
10 to the intent of Congress”); *Fair Hous. Council of San Fernando Valley v. Roommate.com, LLC*,  
11 666 F.3d 1216, 1223 (9th Cir. 2012).

12 **B. Nondisclosure Orders of Unlimited Duration Fail Strict Scrutiny.**

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

1           The pervasive use of nondisclosure orders of unlimited duration, based on the assumption  
2 that Section 2705(b) allows for such orders,<sup>8</sup> fails strict scrutiny. To satisfy strict scrutiny when  
3 seeking a lengthy or unlimited nondisclosure order, the Government must demonstrate there are  
4 no “less restrictive alternatives [that] would be at least as effective in achieving the Act’s  
5 legitimate purpose...” *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 846 (1997). Here,  
6 however, other statutes demonstrate that there are less restrictive alternatives available. Section  
7 2705(a), providing for notice to the target of an investigation to be delayed for a set amount of  
8 time—90 days—and requiring the Government to come back to court to justify any further delay,  
9 is an example of a less restrictive means of achieving the Government’s interest in maintaining  
10 the secrecy of certain investigations. Both Sections 2705(a) and (b) list the same “adverse  
11 results” as potential bases for a nondisclosure order. Most of those are, by definition, limited in  
12 duration, and there is no basis for continued nondisclosure obligations after they have passed.  
13 Any danger to life or physical safety usually passes once the investigation ends or the target is  
14 arrested. 18 U.S.C. §§ 2705 (a)(2)(A), (b)(1). The same goes for flight from prosecution and  
15 destruction of evidence, intimidation of potential witnesses, or otherwise seriously jeopardizing  
16 an investigation or delaying a trial. *Id.* at §§ 2705(a)(2)(B)-(E), (b)(2)-(5).

17           Similarly, the statute governing “sneak and peek” warrants – which is also designed to  
18 protect the same governmental interests – only allows for notice to be delayed for a period of 30  
19 days, unless the Government justifies a longer period for a particular case. *See* 18 U.S.C. §3103a.  
20 These two delayed-notice provisions demonstrate that the Government interests can be served  
21 adequately by less restrictive means. The temporal limitations contained in these other statutes  
22 properly place the burden on the Government—the party seeking to suppress speech—to justify  
23  
24

---

25 <sup>8</sup> One court has interpreted Section 2705(b) as prohibiting orders of indefinite duration unless the Government  
26 shows that such an order is necessary in a particular case. *See Hotmail*, 74 F. Supp. 3d at 1185 (Section 2705(b)’s  
27 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.

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

7 By contrast, by allowing nondisclosure orders of unlimited duration, Section 2705(b) is  
 8 “overbroad because [it] ensure[s] that nondisclosure continues longer than necessary to serve the  
 9 [Government’s] interests at stake.” *In re Nat’l Security Letter*, 930 F. Supp. 2d at 1076. *See also*  
 10 *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  
 11 861 (2d Cir. 2008) (“Once disclosure no longer poses a threat to national security, there is no  
 12 basis for further restricting recipients of National Security Letters from communicating their  
 13 knowledge of the Government’s activities.”). And unlike shorter duration orders, they require  
 14 providers to repeatedly ascertain the status of investigations, and then petition courts to rescind a  
 15 prior nondisclosure order. *See In re Nat’l Security Letter*, 930 F. Supp. 2d at 1076 (“The issuance  
 16 of a nondisclosure order is, in essence, a permanent ban on speech absent the rare recipient who  
 17 has the resources and motivation to hire counsel and affirmatively seek review by a district  
 18 court.”). But “nothing in the statute suggests putting the burden on the provider to guess that  
 19 circumstances might have changed so that a request to lift the order is warranted.” *Hotmail*, 74 F.  
 20 Supp. 3d at 1186. This process is expensive and places the burden, not on the Government that  
 21 seeks to suppress speech, but on the provider that wishes to exercise its First Amendment rights.

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

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

26 \_\_\_\_\_  
 27 <sup>9</sup> 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).

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

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

25  
26 <sup>10</sup> *Privacy Shield Framework—Privacy Shield Principles, Notice*, U.S. Department of Commerce,  
<https://www.privacyshield.gov/article?id=I-NOTICE> (last visited Sept. 2, 2016).

27 <sup>11</sup> *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](http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm); *Data*

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

3           Microsoft has standing to assert its customers' Constitutional rights. Courts have allowed  
 4 an organization with a close relationship to its customer to assert rights on the customer's behalf,  
 5 especially when the customer is unlikely to do so. *Singleton v. Wulff*, 428 U.S. 106, 117-18  
 6 (1976); *see also Craig v. Boren*, 429 U.S. 190, 194-95 (1976). Providers, like Microsoft and  
 7 Amici, have Article III standing, because each "faces an injury in the nature of the burden that it  
 8 must shoulder to facilitate the Government's surveillances of its customers; that injury is  
 9 obviously and indisputably caused by the Government through the directives; and this court is  
 10 capable of redressing the injury." *In re Directives Pursuant to Section 105B of Foreign*  
 11 *Intelligence Surveillance Act*, 551 F.3d 1004, 1008 (Foreign Int. Surv. Ct. Rev. 2008); *see also*  
 12 *Craig*, 429 U.S. at 194. Limitations on the ability to vicariously assert the Fourth Amendment  
 13 rights of others are prudential standing limitations only and can be overcome. *See Warth v.*  
 14 *Seldin*, 422 U.S. 490, 501 (1975) (noting prudential nature of limitation can be relaxed). Amici's  
 15 end-users, particularly those impacted by nondisclosure orders who have no knowledge of the  
 16 issue, cannot dispute their specific cases with the Government or challenge the constitutionality of  
 17 the statute. Amici's enterprise customers may be in a similar situation to the extent that they do  
 18 not have knowledge of the nondisclosure orders to even be aware that there may be an ongoing  
 19 contractual violation.

20           In the present context, Congress clearly understood that only *providers* would be in a  
 21 position to challenge law enforcement process and has repeatedly built in provisions allowing  
 22 providers to challenge various forms of legal process served upon them seeking customer data.  
 23 *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  
 24 circumstances – where no notice is provided to the customer – providers are the *only* entities in a

25  
 26  
 27           \_\_\_\_\_

*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](http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm).

1 position to raise Fourth Amendment issues.<sup>12</sup>

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

### 11 **III. CONCLUSION**

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

22  
23  
24 <sup>12</sup> The Government’s reliance on exclusionary rule and Section 1983 cases is unavailing. *See Gov’t’s Mot.* at 10-11.  
25 *Rakas v. Illinois*, 439 U.S. 128 (1978), concerned with the use of the exclusionary rule as a vehicle for enforcing  
26 Fourth Amendment rights of another. The court reasoned that limiting the assertion of Fourth Amendment rights  
27 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).



