

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  
28

**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE**

MICROSOFT CORPORATION,  
  
Plaintiff,

vs.

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

**STIPULATED MOTION OF AMAZON.COM,  
BOX, CISCO SYSTEMS, DROPBOX,  
EVERNOTE, GOOGLE, LINKEDIN,  
PINTEREST, SALESFORCE, SNAPCHAT,  
AND YAHOO FOR LEAVE TO  
PARTICIPATE AS AMICI CURIAE IN  
SUPPORT OF MICROSOFT CORPORATION**

**Noted on Motion Calendar:  
September 2, 2016**

1 Amazon.com, Inc.; Box, Inc.; Cisco Systems, Inc.; Dropbox, Inc.; Evernote Corporation;  
2 Google Inc.; LinkedIn Corporation; Pinterest, Inc.; salesforce.com, inc.; Snapchat, Inc.; and  
3 Yahoo! Inc. hereby move for leave to participate as *amici curiae* in support of Microsoft  
4 Corporation in this litigation. A proposed brief is attached. Neither party opposes this motion.  
5 In support of their motion, movants state:

6 1. Microsoft seeks a declaration that two provisions of the Stored Communications  
7 Act—18 U.S.C. §§ 2703 and 2705(b)—are unconstitutional under the First and Fourth  
8 Amendments to the U.S. Constitution. Microsoft’s lawsuit raises vitally important legal  
9 questions about the scope of the government’s power both to search the private information that  
10 internet users store in the cloud without notifying the target of the search and to prohibit a  
11 provider of cloud computing services from informing a customer that her information has been  
12 searched.

13 2. District courts have inherent authority to permit non-parties to participate as *amici*  
14 *curiae* in a case and broad discretion in deciding whether to permit *amicus* briefs. *See Hoptowit*  
15 *v. Ray*, 682 F.2d 1237, 1260 (9th Cir. 1982). “District courts may consider amicus briefs from  
16 non-parties ‘concerning legal issues that have potential ramifications beyond the parties directly  
17 involved or if the amicus has unique information or perspective that can help the court beyond  
18 the help that the lawyers for the parties are able to provide.’” *Skokomish Indian Tribe v.*  
19 *Goldmark*, 2013 WL 5720053, at \*1 (W.D. Wash. Oct. 21, 2013) (Robart, J.) (quoting *NGV*  
20 *Gaming, Ltd. v. Upstream Point Molate, LLC*, 355 F. Supp. 2d 1061, 1067 (N.D. Cal. 2005))  
21 (some internal quotation marks omitted). Generally speaking, “courts have exercised great  
22 liberality in permitting an amicus curiae to file a brief in a pending case.” *In re Roxford Foods*  
23 *Litig.*, 790 F. Supp. 987, 997 (E.D. Cal. 1991) (quoting *United States v. Louisiana*, 751 F. Supp.  
24 608, 620 (E.D. La. 1990)). A brief will typically be accepted if it is “timely and useful.”  
25 *Ellsworth Assocs., Inc. v. United States*, 917 F. Supp. 841, 846 (D.D.C. 1996) (internal quotation  
26 marks omitted). Movants’ brief is both.

27 3. First, movants’ brief is timely because it is filed on September 2, 2016, the date  
28 set for *amicus* submissions in this Court’s scheduling order of June 14, 2016. Dkt. 26 ¶ 5; *see*

1 also Dkt. 42, at 2-3 (Aug. 23, 2016) (reiterating September 2 deadline for parties seeking to file  
2 an *amicus curiae* brief related to Defendants' pending motion to dismiss); *cf.* Fed. R. App. P.  
3 29(e) ("An *amicus curiae* must file its brief . . . no later than 7 days after the principal brief of the  
4 party being supported is filed."). Movants' brief also complies with the page limit set forth in  
5 the Court's order of August 15, 2016 (Dkt. 40), because it does not exceed 12 pages in length,  
6 half the allowance for Microsoft's brief opposing Defendants' motion to dismiss. *See* W.D.  
7 Wash. Local Rule 7(e)(3); *cf.* Fed. R. App. P. 29(d).

8 4. Second, movants' brief is useful. This case presents legal questions that have  
9 ramifications beyond the parties directly involved, and movants' brief offers unique information  
10 and insight on those questions. In particular, movants provide a unique perspective as leading  
11 technology companies that provide cloud computing services to the public. Movants collectively  
12 respond to tens of thousands of government requests for user data pursuant to the Stored  
13 Communications Act each year. Movants have also been subject to nondisclosure orders under  
14 § 2705(b) and will likely be subject to many more such orders in the future unless § 2705(b) is  
15 declared unconstitutional. Movants' brief focuses on legal issues that have potential  
16 ramifications for the fundamental rights of entities beyond the parties directly involved in this  
17 litigation—including movants themselves, other providers of cloud computing services, and  
18 hundreds of millions of people who store private information in cloud accounts. Movants thus  
19 believe that the Court will benefit from the unique perspective and helpful information offered  
20 by their brief.

21 5. Movants have conferred with counsel for Microsoft and Defendants regarding this  
22 motion. The parties have consented to movants' participation as *amici curiae*.

23 For the foregoing reasons, the motion should be granted.

24 DATED: September 2, 2016

Respectfully submitted,

HOGAN LOVELLS US LLP

By:           s/ Neal Kumar Katyal          

Neal Kumar Katyal

Attorney for *Amici Curiae*

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  
28

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 September 2, 2016.

HOGAN LOVELLS US LLP

By s/ Neal Kumar Katyal  
Neal Kumar Katyal  
555 Thirteenth Street, N.W.  
Washington, D.C. 20004  
Tel: (202) 637-5528  
Fax: (202) 637-5910  
neal.katyal@hoganlovells.com

Attorney for *Amici Curiae*

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  
28

**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE**

MICROSOFT CORPORATION,

Plaintiff,

vs.

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

**[PROPOSED] BRIEF OF AMICI CURIAE  
AMAZON.COM, BOX, CISCO SYSTEMS,  
DROPBOX, EVERNOTE, GOOGLE,  
LINKEDIN, PINTEREST, SALESFORCE,  
SNAPCHAT, AND YAHOO IN SUPPORT OF  
MICROSOFT CORPORATION**

**Noted on Motion Calendar:  
September 23, 2016**

**CORPORATE DISCLOSURE STATEMENT**

1 Amazon.com, Inc. has no parent corporation and no publicly held corporation owns 10%  
2 or more of Amazon.com's stock.

3 Box, Inc. has no parent corporation and no publicly held corporation owns 10% or more  
4 of Box's stock.

5 Cisco Systems, Inc. has no parent corporation and no publicly held corporation owns  
6 10% or more of Cisco's stock.

7 Dropbox, Inc. has no parent corporation and no publicly held corporation owns 10% or  
8 more of Dropbox's stock.

9 Evernote Corporation has no parent corporation and no publicly held corporation owns  
10 10% or more of Evernote's stock.

11 Google Inc. is a wholly owned subsidiary of Alphabet Inc., a publicly held corporation.

12 LinkedIn Corporation has no parent corporation and no publicly held corporation owns  
13 10% or more of LinkedIn's stock.

14 Pinterest, Inc. has no parent corporation and no publicly held corporation owns 10% or  
15 more of Pinterest's stock.

16 salesforce.com, inc. has no parent corporation and no publicly held corporation owns  
17 10% or more of salesforce.com's stock.

18 Snapchat, Inc. has no parent corporation and no publicly held corporation owns 10% or  
19 more of Snapchat's stock.

20 Yahoo! Inc. has no parent corporation and no publicly held corporation owns 10% or  
21 more of Yahoo's stock.

**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  
28

**Page**

CORPORATE DISCLOSURE STATEMENT ..... i

TABLE OF AUTHORITIES ..... iii

STATEMENT OF INTEREST.....1

INTRODUCTION .....4

ARGUMENT .....5

    I.    The Stored Communications Act Violates Users’ Privacy Rights .....5

    II.   The Stored Communications Act Violates the Free Speech Rights of  
          *Amici* and Other Cloud Computing Service Providers .....10

CONCLUSION.....12

CERTIFICATE OF SERVICE

**TABLE OF AUTHORITIES**

**Page(s)**

**CASES:**

1  
2  
3  
4 *Butterworth v. Smith*,  
494 U.S. 624 (1990) .....12  
5  
6 *Katz v. United States*,  
389 U.S. 347 (1967).....9  
7  
8 *New York Times Co. v. Sullivan*,  
376 U.S. 254 (1964).....11  
9  
10 *Olmstead v. United States*,  
277 U.S. 438 (1928).....9  
11  
12 *Riley v. California*,  
134 S. Ct. 2473 (2014).....8, 9  
13  
14 *Stromberg v. California*,  
283 U.S. 359 (1931).....10  
15  
16 *United States v. Freitas*,  
800 F.2d 1451 (9th Cir. 1986) .....5, 8, 12  
17  
18 *United States v. Robinson*,  
414 U.S. 218 (1973).....9  
19  
20 *United States v. Villegas*,  
899 F.2d 1324 (2d Cir. 1990).....12

**STATUTES:**

21 18 U.S.C. § 2518(8)(d) .....6, 12  
22 18 U.S.C. § 2703.....6  
23 18 U.S.C. § 2703(b)(1)(A).....7, 12  
24 18 U.S.C. § 2705(a) .....12  
25 18 U.S.C. § 2705(b) ..... *passim*  
26 18 U.S.C. § 3103a(b) .....6, 12  
27 18 U.S.C. § 3103a(c).....6, 12  
28 Electronic Communications Privacy Act of 1986 .....7



1 Stored Communications Act ..... *passim*

2 **RULES:**

3 Fed. R. Crim. P. 41 ..... 6

4 Fed. R. Crim. P. 41(f) ..... 12

5 Fed. R. Crim. P. 41(f)(1)(C) ..... 6

6 Fed. R. Crim. P. 41(f)(2)(C) ..... 6

7 Fed. R. Crim. P. 41(f)(3)..... 6

8 **LEGISLATIVE MATERIALS:**

9 S. Rep. No. 99-541 (1986) ..... 7

10 **OTHER AUTHORITIES:**

11 Amazon, *Information Requests*, [https://aws.amazon.com/compliance/amazon-](https://aws.amazon.com/compliance/amazon-information-requests/)  
 12 [information-requests/](https://aws.amazon.com/compliance/amazon-information-requests/) ..... 3

13 Cisco, *Trust and Transparency Center*, [http://www.cisco.com/c/en/us/about/trust-](http://www.cisco.com/c/en/us/about/trust-transparency-center/validation/report.html)  
 14 [transparency-center/validation/report.html](http://www.cisco.com/c/en/us/about/trust-transparency-center/validation/report.html) ..... 3

15 Dropbox, *2015 Transparency Report*, <https://www.dropbox.com/transparency> ..... 3

16 Dropbox, *Law Enforcement Handbook*,  
 17 [https://dl.dropboxusercontent.com/s/77fr4t57t9g8tbo/law\\_enforcement\\_](https://dl.dropboxusercontent.com/s/77fr4t57t9g8tbo/law_enforcement_handbook.html)  
[handbook.html](https://dl.dropboxusercontent.com/s/77fr4t57t9g8tbo/law_enforcement_handbook.html) ..... 3

18 Evernote, *Transparency Report for 2015*, <https://evernote.com/legal/transparency> ..... 3

19 Google, *Transparency Report*,  
 20 <https://www.google.com/transparencyreport/userdatarequests/US/> ..... 3

21 Google, *Transparency Report*,  
 22 <https://www.google.com/transparencyreport/userdatarequests/legalprocess/> ..... 3

23 LinkedIn, *Our Transparency Report*,  
<https://www.linkedin.com/legal/transparency> ..... 3

24 LinkedIn, *Data Request Guidelines*,  
 25 [https://help.linkedin.com/ci/fattach/get/4773861/0/filename/LinkedIn%20Law](https://help.linkedin.com/ci/fattach/get/4773861/0/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf)  
[%20Enforcement%20Data%20Request%20Guidelines.pdf](https://help.linkedin.com/ci/fattach/get/4773861/0/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf) ..... 3

26 Pinterest, *Transparency Report*,  
 27 <https://help.pinterest.com/en/articles/transparency-report> ..... 3

28 Quentin Hardy, *The Era of Cloud Computing*, N.Y. Times (June 11, 2014) ..... 4

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  
28

Snapchat, *Law Enforcement Guide*, <https://www.snapchat.com/lawenforcement> .....3

Snapchat, *Transparency Report*, <https://www.snapchat.com/transparency>.....3

Yahoo, *Transparency Report*, [https://transparency.yahoo.com/government-data-requests/country/United%20States\\*/31/?tid=31](https://transparency.yahoo.com/government-data-requests/country/United%20States*/31/?tid=31) .....3

Yahoo, *Yahoo! Inc. Law Enforcement Response Guidelines*,  
<https://transparency.yahoo.com/law-enforcement-guidelines/us>.....3

## STATEMENT OF INTEREST

1  
2 Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Google, LinkedIn, Pinterest,  
3 Salesforce, Snapchat, and Yahoo respectfully submit this brief as *amici curiae*<sup>1</sup> in support of  
4 Microsoft Corporation.

5 **Amazon.com** is one of the world's largest and best known online retailers and cloud  
6 service providers. Amazon seeks to be the Earth's most customer-centric company, where  
7 customers can discover anything they might want to buy online at the lowest possible prices.  
8 Amazon's cloud computing business, Amazon Web Services, is trusted by more than a million  
9 active customers around the world—including the fastest growing startups, largest enterprises,  
10 and leading government agencies—to power their IT infrastructure, make them more agile, and  
11 lower costs.

12 **Box** is a cloud-based enterprise content management platform that makes it easier for  
13 people to securely collaborate and get work done faster. Today, more than 41 million users  
14 and over 66,000 businesses—including 60% of the Fortune 500—trust Box to manage content in  
15 the cloud.

16 **Cisco Systems** is the worldwide leader in providing infrastructure for the internet. It also  
17 offers various services, managed from data centers operated by Cisco, which allow its customers  
18 to use, among other things, remote data centers, wireless internet services, internet security  
19 services, and collaboration tools, which drive efficiency in their business.

20 **Dropbox** provides file storage, synchronization, and collaboration services. With over  
21 500 million users and 200,000 businesses, people around the world use Dropbox to work the way  
22 they want, on any device, wherever they go. Dropbox's products are built on trust; when people  
23 put their files in Dropbox, they can trust they're secure and their data is their own.

24 **Evernote** provides a platform that allows individuals and teams to bring their life's work  
25 together in one digital workspace. More than 200 million people and over 20,000 businesses

26  
27 <sup>1</sup> No party or counsel for a party authored or paid for this brief in whole or in part, or made a monetary contribution  
28 to fund the brief's preparation or submission. No one other than *amici* and their counsel made a monetary  
contribution to the brief. This brief is filed with the consent of all parties, and *amici* have submitted a motion for  
leave to file along with this proposed brief in accordance with this Court's order of August 23, 2016. Dkt. 42.

1 trust Evernote to help them collect their best ideas, write meaningful words, and move important  
2 projects forward.

3 **Google** is a diversified technology company whose mission is to organize the world's  
4 information and make it universally accessible and useful. Google offers a variety of web-based  
5 products and services—including Search, Gmail, Maps, YouTube, and Blogger—that are used  
6 by people throughout the United States and around the world.

7 **LinkedIn** is an Internet company that hosts the world's largest professional network,  
8 with over 450 million members worldwide and over 130 million members in the United States.  
9 LinkedIn's mission is to connect the world's professionals to enable them to be more productive  
10 and successful.

11 **Pinterest** is an online catalog of ideas. Every month, over 100 million people around the  
12 world use Pinterest to find and save ideas for cooking, parenting, style, and more.

13 **Salesforce** is a leading provider of enterprise cloud computing services headquartered in  
14 San Francisco, California. Trust is the number one value at Salesforce and nothing is more  
15 important to Salesforce than the privacy of its customers' data.

16 With more than 150 million daily active users, **Snapchat** is one of the world's leading  
17 camera applications. Snapchat empowers its users to tell their stories and talk with their friends.  
18 It also features news coverage and video content from premium publishers like ESPN and the  
19 Wall Street Journal.

20 **Yahoo** is a guide to digital information discovery, focused on informing, connecting, and  
21 entertaining users through its search, communications, and digital content products. Yahoo's  
22 wholly-owned subsidiary, Tumblr, Inc.—with an audience of over 500 million people per  
23 month—provides a platform for users to connect, to explore new ideas and creative expressions,  
24 and to form communities.

25 *Amici* often compete vigorously with Microsoft and with each other. But *amici* here  
26 speak with one voice because of the singular importance of this case to them and to their  
27 customers. *Amici* offer cloud computing services to customers and use cloud computing to offer  
28 a wide range of other services, including the ability to communicate and collaborate in real-time;

1 to work seamlessly from multiple devices; and to store and share photographs, documents, and  
 2 other data. *Amici* have been champions of cloud computing and believe deeply in its potential.  
 3 And that means *amici* are uniquely well positioned to see the special threat to users' privacy  
 4 posed by secret government searches of cloud accounts. *Amici* therefore submit this brief in  
 5 support of Microsoft's challenge to provisions of the Stored Communications Act, 18 U.S.C.  
 6 §§ 2701-2712, that impose unjustified and unconstitutional burdens on the free speech rights of  
 7 Microsoft and *amici*, and on the privacy rights of their customers.

8 To be clear: *Amici* respect the important work that law enforcement agencies do every  
 9 day. Technology companies like *amici* have, or in the future may have, obligations under the  
 10 Stored Communications Act and other laws to deliver customer data to law enforcement in  
 11 response to proper legal process, and *amici* take these obligations seriously. Many *amici* have  
 12 full-time teams of employees—with someone on duty or on call around the clock—dedicated to  
 13 responding to law enforcement requests for data. Indeed, in just the last six months of 2015,  
 14 *amici* collectively responded to tens of thousands of U.S. government data requests in criminal  
 15 investigations.<sup>2</sup> Many *amici* also publish guidelines for law enforcement that explain their  
 16 products, describe what customer data can be requested through legal process, and set out how  
 17 best to serve process on the company.<sup>3</sup> *Amici*, in short, have no desire to shield criminals.

18 But *amici* also believe that their customers have a right to be informed of government  
 19 searches of their private data and that *amici* have a right to inform them. Of course, those rights  
 20 may be limited as necessary to protect compelling state interests, including interests in  
 21

22 <sup>2</sup> See, e.g., Amazon, *Information Requests*, <https://aws.amazon.com/compliance/amazon-information-requests/>;  
 23 Cisco, *Trust and Transparency Center*, [http://www.cisco.com/c/en/us/about/trust-transparency-center/validation/  
 24 report.html](http://www.cisco.com/c/en/us/about/trust-transparency-center/validation/report.html); Dropbox, *2015 Transparency Report*, <https://www.dropbox.com/transparency>; Evernote, *Transparency  
 25 Report for 2015*, <https://evernote.com/legal/transparency>; Google, *Transparency Report*, [https://www.google.com/  
 26 transparencyreport/userdatarequests/US/](https://www.google.com/transparencyreport/userdatarequests/US/); LinkedIn, *Our Transparency Report*, [https://www.linkedin.com/legal/  
 27 transparency](https://www.linkedin.com/legal/transparency); Pinterest, *Transparency Report*, <https://help.pinterest.com/en/articles/transparency-report>; Snapchat,  
 28 *Transparency Report*, <https://www.snapchat.com/transparency>; Yahoo, *Transparency Report*,  
[https://transparency.yahoo.com/government-data-requests/country/United%20States\\*\\*/31/?tid=31](https://transparency.yahoo.com/government-data-requests/country/United%20States**/31/?tid=31).

<sup>3</sup> See, e.g., Dropbox, *Law Enforcement Handbook*, [https://dl.dropboxusercontent.com/s/77fr4t57t9g8tbo/law\\_  
 29 enforcement\\_handbook.html](https://dl.dropboxusercontent.com/s/77fr4t57t9g8tbo/law_enforcement_handbook.html); Google, *Transparency Report*, [https://www.google.com/transparencyreport/  
 30 userdatarequests/legalprocess/](https://www.google.com/transparencyreport/userdatarequests/legalprocess/); LinkedIn, *Data Request Guidelines*, [https://help.linkedin.com/ci/fattach/get/  
 31 4773861/0/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf](https://help.linkedin.com/ci/fattach/get/4773861/0/filename/LinkedIn%20Law%20Enforcement%20Data%20Request%20Guidelines.pdf); Snapchat, *Law  
 32 Enforcement Guide*, <https://www.snapchat.com/lawenforcement>; Yahoo, *Yahoo! Inc. Law Enforcement Response  
 33 Guidelines*, <https://transparency.yahoo.com/law-enforcement-guidelines/us>.

1 apprehending criminals and in protecting the public. But the provisions of the Stored  
2 Communications Act that Microsoft challenges go far beyond any necessary limits and infringe  
3 the fundamental rights of *amici* and their customers.

#### 4 INTRODUCTION

5 Cloud computing, one of the major technological advances of the early twenty-first  
6 century, has already brought about tremendous economic and social benefits.<sup>4</sup> In essence, cloud  
7 computing takes advantage of the Internet to connect users to a vast “cloud” of interlinked  
8 servers, data storage systems, and other digital devices located all over the world. Whereas the  
9 user of a computer was once limited to the processing power, storage capacity, and programs  
10 within her own machine, cloud computing offers her seamless access to virtually unlimited  
11 power and data storage, along with applications tailored to her needs.

12 The cloud also connects the user’s devices—her computer, smartphone, tablet, and even  
13 her thermostat or watch—to one another, letting her access her data from any device in any  
14 location at any time. The cloud connects her to her friends, family, and colleagues through  
15 social networks, chat and email services, online games, photo-sharing services, and workplace  
16 collaboration applications. It connects her to movies, music, and other media; to crowd-sourced  
17 reviews of products and restaurants; and to real-world services like car rentals and food  
18 deliveries. The cloud also promotes competition in the marketplace by reducing the cost and  
19 complexity of information technology services, which reduces barriers to entry for new firms  
20 while allowing them to quickly and easily offer their services to the public. In short, cloud  
21 computing is ushering in a more interconnected world in which social relationships are deeper,  
22 the economy is more efficient, and life is easier.

23 The growth and enormous potential of cloud computing make the challenged provisions  
24 of the Stored Communications Act all the more troubling. The government’s ability to engage in  
25 surreptitious searches of homes and tangible things is practically and legally limited. But the Act  
26 allows the government to search personal data stored in the cloud without ever notifying an  
27

---

28 <sup>4</sup> See, e.g., Quentin Hardy, *The Era of Cloud Computing*, N.Y. Times (June 11, 2014).

1 account owner that her data has been searched. And it empowers the government, upon a  
2 minimal showing, to obtain a gag order from a court preventing cloud computing service  
3 providers like *amici* from informing their customers or anyone else that the data has been turned  
4 over. Even worse, those gag orders often have no specified end date. These provisions—and the  
5 resulting proliferation of indefinite gag orders—are harmful for a number of reasons. First,  
6 surreptitious searches of the personal information stored in cloud accounts invade the Fourth  
7 Amendment privacy rights of *amici*'s customers. Second, the specter of surreptitious searches  
8 may chill customers from using cloud computing in the first place, dampening a promising  
9 technology and the potential for further innovation. Finally, the gag orders violate the First  
10 Amendment rights of *amici* to speak on a matter of public concern—the nature and prevalence of  
11 electronic surveillance. There may well be some circumstances in which a narrowly tailored and  
12 time-limited gag order is justified, but the Act's authorization of gag orders sweeps far too  
13 broadly. As a result, the public will lack the information it needs to address the problem of  
14 surveillance through democratic means. *Amici* therefore submit this brief in support of Microsoft  
15 and in opposition to Defendants' motion to dismiss.

## 16 ARGUMENT

### 17 I. The Stored Communications Act Violates Users' Privacy Rights.

18 The government's ability to conduct secret searches has historically been subject to both  
19 practical and legal limits. The practical limit is that, in order to execute a search warrant, the  
20 government generally has to seize some tangible object or enter a home. The fact of the  
21 intrusion will usually be apparent to the owner of the seized object or the occupant of the  
22 searched home. The legal limit—grounded in the Fourth Amendment—is that surreptitious  
23 searches, while not categorically proscribed, have to be confined to circumstances in which they  
24 are truly necessary. In the Ninth Circuit's words:

25 [S]urreptitious searches . . . strike at the very heart of the interests protected by the Fourth  
26 Amendment. The mere thought of strangers walking through and visually examining the  
27 center of our privacy interest, our home, arouses our passion for freedom as does nothing  
28 else. That passion, the true source of the Fourth Amendment, demands that surreptitious  
entries be closely circumscribed.

*United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986).

1 Thus, when a federal law enforcement officer executes a warrant to search a home or  
2 other physical location and seize property, Federal Rule of Criminal Procedure 41 provides that  
3 “[t]he officer executing the warrant must give a copy of the warrant and a receipt for the property  
4 taken to the person from whom, or from whose premises, the property was taken or leave a copy  
5 of the warrant and receipt at the place where the officer took the property.” Fed. R. Crim. P.  
6 41(f)(1)(C). Similarly, where a law enforcement officer uses a tracking device, the Rules  
7 provide that “[w]ithin 10 days after the use of the tracking device has ended, the officer  
8 executing a tracking-device warrant must serve a copy of the warrant on the person who was  
9 tracked or whose property was tracked.” Fed. R. Crim. P. 41(f)(2)(C). And the federal wiretap  
10 statute requires detailed notice to the target of the communications interception “[w]ithin a  
11 reasonable time but not later than ninety days after . . . the termination” of the interception  
12 period. 18 U.S.C. § 2518(8)(d).<sup>5</sup>

13 The notice required by Rule 41 may be delayed where authorized by statute, Fed. R.  
14 Crim. P. 41(f)(3), but the general rule is that delayed notice is permitted only where a court  
15 “finds reasonable cause to believe that providing immediate notification . . . may have an adverse  
16 result” and “the warrant provides for the giving of such notice within a reasonable period not to  
17 exceed 30 days after the date of its execution, or on a later date certain if the facts of the case  
18 justify a longer period of delay.” 18 U.S.C. § 3103a(b). Any extension of the delay period may  
19 “only be granted upon an updated showing of the need for further delay.” *Id.* § 3103a(c). And  
20 law enforcement officers generally have no legal authority to silence third parties who become  
21 aware of an investigation.

22 Against this background, the Stored Communications Act is a troubling outlier. The Act  
23 provides the legal framework for law enforcement to compel the provider of an “electronic  
24 communication service” or a “remote computing service” to disclose the contents of customer  
25 communications stored on the service. *Id.* § 2703. For no discernible policy reason, however,  
26 the Act departs sharply from the norm of notice embodied in legal provisions described above. It  
27

---

28 <sup>5</sup> A judge may “postpone[]” the required notice upon a finding of good cause to do so. 18 U.S.C. § 2518(8)(d).



1 does so in two mutually reinforcing ways. First, where the government uses a warrant to compel  
2 the service provider to turn over user content, it may do so “without required notice to the  
3 subscriber or customer.” *Id.* § 2703(b)(1)(A). Second, and even more disturbing, the  
4 government may ask a court to impose a gag order on the service provider, precluding it from  
5 “notify[ing] any other person of the existence of the warrant,” and the court “shall enter such an  
6 order if it determines that there is reason to believe that notification of the existence of the  
7 warrant . . . will result in” any of a range of disfavored consequences, including “seriously  
8 jeopardizing an investigation or unduly delaying a trial.” *Id.* § 2705(b). The gag order remains  
9 in effect “for such period as the court deems appropriate.” *Id.*

10 The Stored Communications Act became law thirty years ago, as Title II of the Electronic  
11 Communications Privacy Act of 1986. At that time, before the rise of the modern Internet, no  
12 one could have foreseen how ubiquitous personal computers and electronic communications  
13 would become. Still less could one have envisioned the advent of cloud computing and the  
14 ongoing migration of private information from homes and hard drives to the data storage systems  
15 of the cloud. Indeed, when it passed the Act, Congress actually contemplated that an email  
16 provider might print out an email and deliver it via the postal service. S. Rep. No. 99-541, at 8  
17 (1986). Needless to say, no one then would have appreciated just how destructive the Act’s anti-  
18 notice provisions would become to Fourth Amendment rights three decades down the road.

19 Today, *amici*, as well as other cloud computing service providers, are subject to tens of  
20 thousands of law enforcement demands from authorities in the United States for private customer  
21 data every year.<sup>6</sup> Those demands are frequently accompanied by § 2705(b) gag orders. And  
22 many of those gag orders—thousands per year—have no definite end date. In particular:

- 23 • In 2016, Dropbox has received over 200 gag orders of indefinite duration, amounting to  
24 approximately 25% of all of the subpoenas and warrants it has received.
- 25 • So far this year, more than three-quarters (7 of 9) of the subpoenas and search warrants  
26 received by Evernote were accompanied by indefinite gag orders.
- 27 • Since the beginning of 2015, LinkedIn has received hundreds of gag orders, and almost  
28 two-thirds of them are of indefinite duration.

---

<sup>6</sup> See the transparency reports cited *supra* note 2.

- 1 • Pinterest, in the first six months of 2016, received law enforcement information requests on 41 accounts, but was only able to notify 4 account holders. The gag orders affecting all accounts except *one*—in other words, 97%—were indefinite.
- 2 • Between April and June of this year, nearly three-quarters (58 of 79) of all gag orders received by Snapchat under § 2705(b) had no definite end.
- 3 • In the first seven months of 2016, Yahoo has received over 700 federal search warrants for user data, and well over half—about 60%—were accompanied by gag orders of indefinite duration. Google reports a similar percentage.

4  
5  
6 In contrast to a search of a home or a seizure of physical property, there may be no way  
7 for a user to detect that the provider has disclosed information stored in the account to the  
8 government. Thus, although *amici* regularly release transparency reports providing aggregate  
9 data, government gag orders keep customers, policymakers, and the public in the dark regarding  
10 the details of individual cases. And because a gag order prevents the customer from learning of  
11 the search in the first place, *amici* are the only ones with the practical ability to challenge  
12 individual gag orders. But the sheer volume of the gag orders can make challenging them one by  
13 one impossible.

14 This new threat of secret government searches has several important consequences. The  
15 first is the obvious damage to the privacy of all of us who use the Internet. To have a  
16 government agent secretly pore over a digital record of the details of one's life, from the intimate  
17 to the mundane, "strike[s] at the very heart of the interests protected by the Fourth Amendment."  
18 *Freitas*, 800 F.2d at 1456. The second consequence is that the fear of secret surveillance could  
19 limit the adoption and use of cloud services, sacrificing the social benefits discussed above and  
20 chilling cloud-based speech, social relationships, innovation, and economic development. Users  
21 should not be put to a choice between reaping the benefits of technological innovation and  
22 maintaining the privacy rights guaranteed by the Constitution.

23 A third consequence is less obvious but equally pernicious: Because users do not see the  
24 full extent of government surveillance in criminal cases, they cannot make informed democratic  
25 choices about whether to cabin it. If law enforcement were openly ransacking homes, then the  
26 people would see those invasions of privacy and could respond through the democratic process.  
27 Indeed, that is precisely what happened during the founding generation: "Opposition" to "general  
28

1 warrants,” “which allowed British officers to rummage through homes in an unrestrained search  
2 for evidence of criminal activity,” was “one of the driving forces behind the Revolution itself.”  
3 *Riley v. California*, 134 S. Ct. 2473, 2494 (2014). By the same token, users may well decide to  
4 take political action to reduce government intrusions into their cloud-based accounts—but only if  
5 they know about those intrusions. When the government can act in secrecy, it can expand its  
6 intrusions into individual privacy without an effective democratic check.

7 While the broad anti-notice provisions of the Stored Communications Act set it apart  
8 from the rules that apply to physical searches and seizures, tracking devices, and wiretaps, there  
9 is nothing new in the need for courts to take technological developments into account in  
10 fulfilling their role as guardians of the Constitution. In the early days of telephony, for example,  
11 the Supreme Court held that a wiretap was not a “search” within the meaning of the Fourth  
12 Amendment because the government could listen in on a person’s phone calls without  
13 trespassing on her physical property. *Olmstead v. United States*, 277 U.S. 438 (1928). But the  
14 Court righted its course in *Katz v. United States*, 389 U.S. 347 (1967), which established that  
15 people are entitled to a “constitutionally protected reasonable expectation of privacy” even  
16 outside of their physical property. *Id.* at 360 (Harlan, J., concurring). Similarly, in the 1970s the  
17 Court ruled that the police may search objects found on the person of a suspect upon arrest  
18 without a warrant or probable cause. *See United States v. Robinson*, 414 U.S. 218 (1973). But  
19 now that the average person carries “a digital record of nearly every aspect” of her life in her  
20 pocket on a smartphone, things are dramatically different. *Riley*, 134 S. Ct. at 2490. And so in  
21 2014 the Supreme Court unanimously refused to apply *Robinson* to cellphones and instead held  
22 that cellphones may generally be searched only pursuant to a warrant. *Id.* at 2485; *see also id.* at  
23 2484 (observing that modern cellphones “are based on technology nearly inconceivable just a  
24 few decades ago”).

25 The shift to cloud computing also has significant implications for the protection of  
26 fundamental privacy rights. Indeed, what the Supreme Court said of cellphones is equally true of  
27 cloud computing: A search of a typical user’s cloud accounts would “expose to the government  
28 far *more* than the most exhaustive search of a house.” *Id.* at 2491. A cloud account can be like

1 an unexpurgated transcript of a user’s life; there is simply no analogue in the pre-Internet world.  
2 And, if the government can keep its searches secret, then the people cannot act through the  
3 democratic process to limit surveillance of cloud accounts. It thus falls to the courts to make  
4 sure that democratic process can function effectively.

5 **II. The Stored Communications Act Violates the Free Speech Rights of *Amici* and**  
6 **Other Cloud Computing Service Providers.**

7 “The maintenance of the opportunity for free political discussion to the end that  
8 government may be responsive to the will of the people and that changes may be obtained by  
9 lawful means, an opportunity essential to the security of the Republic, is a fundamental principle  
10 of our constitutional system.” *Stromberg v. California*, 283 U.S. 359, 369 (1931). By  
11 empowering the government to silence *amici* and other service providers, § 2705(b) eliminates  
12 “the opportunity for free political discussion” and undermines “the end that government may be  
13 responsive to the will of the people.”

14 *Amici* wish to exercise their First Amendment rights to speak on a matter of profound  
15 public concern: governmental surveillance of the private materials stored in the cloud. Members  
16 of the public have the right to know when the government searches their private accounts and—  
17 absent exceptional and compelling circumstances—*amici* should have the right to tell them. The  
18 public also has a substantial interest in receiving the information necessary to inform its  
19 democratic deliberations about the appropriate privacy safeguards for this new technological  
20 context. *Amici* already provide aggregate statistics in their transparency reports. But gag orders  
21 prevent users and the public from learning the details of particular cases. Those concrete facts  
22 would enable the people to evaluate whether the government is overreaching in a manner that  
23 requires a democratic response. It is therefore vital that *amici* be permitted to be more  
24 transparent with users regarding government demands for their data.

25 Section 2705(b) burdens the constitutional rights of *amici* to speak on this matter of  
26 public concern. Empowering law enforcement to silence someone who learns of an investigation  
27 is virtually unheard of outside the context of these digital searches under the Stored  
28 Communications Act. Even where the government can search a person’s house without first

1 notifying him, it has no roving power to silence a neighbor who witnesses the search and decides  
2 to disclose it. To grant the government power to silence public discussions of police practices  
3 would fly in the face of our “profound national commitment to the principle that debate on public  
4 issues should be uninhibited, robust, and wide-open.” *New York Times Co. v. Sullivan*, 376 U.S.  
5 254, 270 (1964).

6 That is just what § 2705(b) does. *Amici* do not contest that a narrowly tailored gag order  
7 in some circumstances might be necessary to further a compelling governmental interest. But  
8 two particular features of § 2705(b) broaden its reach well beyond those limited circumstances.  
9 First, the statute simply does not provide for the level of judicial scrutiny required to justify the  
10 severe infringement on the service provider’s freedom of speech. It states that the court “shall  
11 enter” a gag order upon a determination that there is “reason to believe” that disclosure of the  
12 search will have one of a number of adverse effects, including “seriously jeopardizing an  
13 investigation or unduly delaying a trial.” 18 U.S.C. § 2705(b). The Act thus does not instruct  
14 the court to take into account the privacy rights of the user or the speech rights of the service  
15 provider—indeed, its mandatory language seems not even to leave the court the discretion to do  
16 so. And “reason to believe” is too low a standard of proof given the gravity of the constitutional  
17 rights involved. In short, § 2705(b) does not require the government to make a meaningful  
18 showing that a gag order is justified, which means that gag orders will often issue despite the  
19 absence of any facts justifying the resulting burdens on constitutional rights.

20 Second, the Act does not instruct the court to limit the gag order to the period necessary  
21 to achieve its purpose, or even to any definite period. Rather, § 2705(b) permits and even  
22 encourages the government to request that a judge issue gag orders of indefinite duration. The  
23 statutory language “for such period as the court deems appropriate” places no specific temporal  
24 bound on the court’s discretion. Nor does § 2705(b) direct the court to consider a later request  
25 by the provider to lift the gag order in light of the passage of time, changed circumstances (such  
26 as the termination of the investigation), or any other factor. Even if the court were to entertain  
27 such a request, § 2705(b) provides no standard for the court to apply in doing so. And, again, at  
28 no point is the court instructed to consider the constitutional interests at stake. By contrast, as

1 discussed above, other federal statutes and rules intended to safeguard the same government  
2 interest in secrecy during criminal investigations set specific time periods and require the  
3 government to specifically justify any request for an extension. *See* 18 U.S.C. §§2705(a),  
4 2518(8)(d), 3103a(b)-(c); Fed. R. Crim. P. 41(f); *United States v. Villegas*, 899 F.2d 1324, 1337  
5 (2d Cir. 1990); *Freitas*, 800 F.2d at 1456. Section 2705(b)'s departure from those other statutes  
6 has no discernible policy justification and, in combination with § 2703(b)(1)(A)'s rule that the  
7 government itself need never disclose the search, raises the very real specter that the user will  
8 never learn that the government has invaded her privacy.

9 *Amici* acknowledge the importance of governmental efforts to prevent crime, and *amici*  
10 put substantial resources into cooperating with the government, including by responding to law  
11 enforcement requests for data. There might be situations in which a gag order would be  
12 narrowly tailored to serve a compelling state interest related to a criminal investigation, and  
13 therefore justify the burden on free expression. At the very least, however, such a gag order  
14 would have to be limited in time to match the duration of that compelling interest, and any  
15 extensions would have to be carefully scrutinized by a court, with due consideration of the First  
16 and Fourth Amendment interests of the user and the service provider. *See Butterworth v. Smith*,  
17 494 U.S. 624 (1990) (holding that the state may not prohibit a grand jury witness from publicly  
18 disclosing his grand jury testimony after the expiration of the grand jury's term). Section  
19 2705(b)'s blunderbuss approach includes no safeguards for constitutional rights and sweeps well  
20 beyond the limited situations in which a gag order might be justified.

## 21 CONCLUSION

22 For the foregoing reasons, the Court should deny Defendants' motion to dismiss.

23 DATED: September 2, 2016

HOGAN LOVELLS US LLP

24 By:           s/ Neal Kumar Katyal            
25 Neal Kumar Katyal  
26 Attorney for *Amici Curiae*  
27  
28

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 September 2, 2016.

HOGAN LOVELLS US LLP

By s/ Neal Kumar Katyal

Neal Kumar Katyal  
555 Thirteenth Street, N.W.  
Washington, D.C. 20004  
Tel: (202) 637-5528  
Fax: (202) 637-5910  
neal.katyal@hoganlovells.com

Attorney for *Amici Curiae*

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  
28

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  
28

**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE**

MICROSOFT CORPORATION,

Plaintiff,

vs.

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

**[PROPOSED] ORDER GRANTING  
MOTION OF AMAZON.COM, BOX,  
CISCO SYSTEMS, DROPBOX,  
EVERNOTE, GOOGLE, LINKEDIN,  
PINTEREST, SALESFORCE,  
SNAPCHAT, AND YAHOO FOR  
LEAVE TO PARTICIPATE AS AMICI  
CURIAE IN SUPPORT OF  
MICROSOFT CORPORATION**

**Noted on Motion Calendar:  
September 2, 2016**

**ORDER**

The Court has reviewed the unopposed Motion of Amazon.com, Inc.; Box, Inc.; Cisco Systems, Inc.; Dropbox, Inc.; Evernote Corporation; Google Inc.; LinkedIn Corporation; Pinterest, Inc.; salesforce.com, inc.; Snapchat, Inc.; and Yahoo! Inc. for Leave To Participate as Amici Curiae in Support of Microsoft Corporation.

The Court hereby GRANTS the Motion and ORDERS that the proposed amici may file the brief attached to the Motion.

Dated this \_\_\_ day of September, 2016.

\_\_\_\_\_  
HON. JAMES L. ROBART  
United States District Judge



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  
28

**Presented by:**

**HOGAN LOVELLS US LLP**

s/ Neal Kumar Katyal

Neal Kumar Katyal

555 Thirteenth Street, N.W.

Washington, D.C. 20004

Tel: (202) 637-5528

Fax: (202) 637-5910

neal.katyal@hoganlovells.com

Attorney for *Amici Curiae*

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  
28

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 September 2, 2016.

HOGAN LOVELLS US LLP

By s/ Neal Kumar Katyal

Neal Kumar Katyal  
555 Thirteenth Street, N.W.  
Washington, D.C. 20004  
Tel: (202) 637-5528  
Fax: (202) 637-5910  
neal.katyal@hoganlovells.com

*Attorney for Amici Curiae*