

JUDGE JAMES L. ROBERT

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

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

Defendants.

Case No. 2:16-cv-00538 JLR

**BRIEF OF THE CHAMBER OF
COMMERCE OF THE UNITED
STATES OF AMERICA, THE
CENTER FOR DEMOCRACY AND
TECHNOLOGY, THE NATIONAL
ASSOCIATION OF
MANUFACTURERS, *ET AL.* AS
AMICI CURIAE IN SUPPORT OF
MICROSOFT'S OPPOSITION TO
DEFENDANT'S MOTION TO
DISMISS**

NOTE ON MOTION CALENDAR:
September 23, 2016

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES.....	ii
INTEREST OF AMICI CURIAE	1
INTRODUCTION AND SUMMARY OF ARGUMENT.....	1
ARGUMENT	2
I. ECPA’s Authorization Of Surreptitious Searches Will Impede Realization Of The Very Substantial Benefits Of Cloud Computing Services.	2
A. Business and Individual Users of Internet-Based Data Services Entrust Their Most Intimate, Confidential, and Valuable Information to Third- Party Providers.	3
B. Cloud Computing Technology Promises Dramatic Economic and Societal Benefits.	4
C. Many Individuals And Businesses Will Be Reluctant To Use Cloud Computing Services If, As The Government Asserts, Their Private Information Receives Significantly Diminished Legal Protection.....	6
II. Section 2705(b)’s Broad Gag Order Authorization Violates The Constitution.	8
A. The First Amendment Prohibits Restriction of Speech Based on a Mere “Reason to Believe” that Adverse Consequences Would Occur.....	8
1. A gag order must satisfy the strict scrutiny standard.	8
2. The statutory guidelines for issuing a gag order do not satisfy strict scrutiny.	8
B. ECPA’s Warrant Authority Violates The Fourth Amendment.	10
1. The Fourth Amendment generally requires contemporaneous notice to the owner of property to be searched or seized, absent a strong justification for withholding notice.	10
2. The Fourth Amendment’s protection of users’ confidential personal and business information is not vitiated because users store that information with third-party providers.	11
CONCLUSION	13

TABLE OF AUTHORITIES

Page(s)

CASES

<i>Bantam Books, Inc. v. Sullivan</i> , 372 U.S. 58 (1963)	8
<i>City of Ontario v. Quon</i> , 560 U.S. 746 (2010)	4
<i>Florida v. Harris</i> , 133 S. Ct. 1050 (2013)	9
<i>Hopper v. City of Pasco</i> , 241 F.3d 1067 (9th Cir. 2001)	9
<i>In Matter of Search Warrant for [redacted]@hotmail.com</i> , 74 F. Supp. 3d 1184 (N.D. Cal. 2014)	9
<i>In re Fifteen Subpoenas</i> , No. 16-MC-1300 (E.D.N.Y. May 12, 2016) (Doran Decl. [Dkt. 45], Ex. E)	9
<i>In re Grand Jury Subpoena</i> , ___ F.3d ___, 2016 WL 3745541 (9th Cir. July 13, 2016)	12
<i>In re: National Security Letters</i> , Nos. 11-cv-02173-SI (N.D. Cal. Mar. 29, 2016) (Doran Decl. [Dkt. 45], Ex. B)	9
<i>In re Sealing and Non-Disclosure of Pen/Trap/2703(D)</i> , 562 F. Supp. 2d 876 (S.D. Tex. 2008)	9
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	11, 12
<i>Levine v. United States Dist. Court for the Cent. Dist. of Cal.</i> , 764 F.2d 590 (9th Cir. 1985)	8
<i>Nebraska Press Ass'n v. Stuart</i> , 427 U.S. 539 (1976)	8
<i>Organization for a Better Austin v. Keefe</i> , 402 U.S. 415 (1971)	10
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	<i>passim</i>

TABLE OF AUTHORITIES
(continued)

		Page(s)
1	<i>Sorrell v. IMS Health Inc.</i> ,	
2	564 U.S. 552 (2011)	8
3	<i>United States v. Freitas</i> ,	
4	800 F.2d 1451 (9th Cir. 1986)	11
5	<i>United States v. Gorman</i> ,	
6	314 F.3d 1105 (9th Cir. 2002)	9
7	<i>United States v. Jones</i> ,	
8	132 S. Ct. 945 (2012)	12
9	<i>United States v. Playboy Entm't Group, Inc.</i> ,	
10	529 U.S. 803 (2000)	8
11	<i>United States v. Warshak</i> ,	
12	631 F.3d 266 (6th Cir. 2010)	12
13	<i>Wilson v. Arkansas</i> ,	
14	514 U.S. 927 (1995)	10, 11
15	STATUTES	
16	18 U.S.C. § 2703(b)	1
17	18 U.S.C. § 2703(b)(1)(A)	10, 12
18	18 U.S.C. § 2705(b)	1, 8, 9
19	OTHER AUTHORITIES	
20	Damon C. Andrews & John M. Newman, <i>Personal Jurisdiction and Choice of</i>	
21	<i>Law in the Cloud</i> , 73 Md. L. Rev. 313, 325 (2013)	5
22	Lee Badger et al., <i>Recommendations of the Nat'l Inst. of Standards & Tech.</i> ,	
23	<i>U.S. Dep't of Commerce, NIST Special Publication 800-146: Cloud</i>	
24	<i>Computing Synopsis and Recommendations</i> (2012), http://goo.gl/KNlaJM	6
25	Berkman Center for Internet & Society at Harvard University, <i>Don't Panic:</i>	
26	<i>Making Progress on the "Going Dark" Debate</i> (2016), http://goo.gl/98KaEc	7
27	Daniel Castro and Alan McQuinn, <i>Beyond the USA Freedom Act: How U.S.</i>	
	<i>Surveillance Still Subverts U.S. Competitiveness</i> (2015),	
	http://goo.gl/Ob21Jn	7
	Elizabeth Dwoskin and Frances Robinson, <i>NSA Internet Spying Sparks Race to</i>	
	<i>Create Offshore Havens for Data Privacy</i> , Wall St. J. (Sept. 27, 2013),	
	http://goo.gl/i2NLss	7

TABLE OF AUTHORITIES
(continued)

		Page(s)
1	<i>ECPA Reform and the Revolution in Cloud Computing: Hearing before the</i>	
2	<i>Subcomm. on the Constitution of the H. Comm. on the Judiciary, 111th</i>	
	<i>Cong. (2011).....</i>	5, 6
3	Jared A. Harshbarger, <i>Cloud Computing Providers and Data Security Law</i> , 16 J.	
4	Tech. L. & Pol’y 229 (2011)	2, 5
5	Orin S. Kerr, <i>The Next Generation Communications Privacy Act</i> , 162 U. Pa. L.	
6	Rev. 373 (2014).....	4
7	Nancy J. King & V.T. Raja, <i>What Do They Really Know About Me in the</i>	
8	<i>Cloud?</i> , 50 Am. Bus. L.J. 413 (2013)	5
9	Mary Madden, <i>Public Perceptions of Privacy and Security in the Post-Snowden</i>	
10	<i>Era</i> , Pew Research Center (Nov. 12, 2014), http://goo.gl/ivNYHD	6, 7
11	James Manyika et al., McKinsey Global Institute, <i>Disruptive Technologies:</i>	
12	<i>Advances That Will Transform Life, Business, and the Global Economy</i>	
13	(2013), http://goo.gl/p0EuC6	5
14	Paul Ohm, <i>The Fourth Amendment in a World Without Privacy</i> , 81 Miss. L.J.	
15	1309 (2012)	4
16	Lee Rainie & Shiva Maniam, <i>Americans Feel the Tensions between Privacy and</i>	
17	<i>Security Concerns</i> , Pew Research Center (Feb. 19, 2016),	
18	http://goo.gl/zfetT5	6
19	Kevin Werbach, <i>The Network Utility</i> , 60 Duke L.J. 1761 (2011).....	5

INTEREST OF AMICI CURIAE

Amici curiae are organizations representing users of remote computing services and individual users of such services: the Chamber of Commerce of the United States of America; the Center for Democracy and Technology; the National Association of Manufacturers; Alaska Airlines, Inc.; Archive360, Inc.; AvePoint; BP America Inc.; Delta Air Lines, Inc.; Eli Lilly and Company; Getty Images (US), Inc.; GlaxoSmithKline LLC; H5; the Information Coalition; Onsupport; and Wipfli LLP. A description of each *amicus* appears in the motion accompanying this brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

The authority to conduct surreptitious searches conferred by the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. §§ 2703(b) & 2705(b), is invoked routinely by the government to bar third-party service providers, such as Microsoft, Google, or Apple, from notifying their customers that the government has sought access to the customer’s electronic data—such as e-mails, photos, and documents—stored by the customer with the service provider. *See* First Amend. Compl. ¶ 16

Prior to the technological advances that today permit storage of data “in the cloud” through the use of third-party providers, individuals and businesses kept important, private information on their own premises, either in physical form or in their own computer systems. If the government wanted access to that information, it had to serve a warrant on the individual or business—and the individual or business could contest the government’s demand.

The government’s extensive use of ECPA gag orders thus leverages a new technology—the storage and manipulation of data “in the cloud” on remote servers, rather than on the customer’s own devices—to significantly reduce privacy protections. Before the use of this technology, the customer would have known of the government’s demand for private information and had an opportunity to contest the government’s request, because the data was in the customer’s possession. The government’s view of ECPA means that, because of this fortuitous technological development, it may obtain the information without the customer’s

1 knowledge and without an opportunity for the customer to challenge the government's action.

2 Cloud computing has already provided significant economic and societal benefits, and it
3 could produce even greater rewards. But if the government's view of ECPA's gag order
4 authority prevails, individuals and businesses will have reason to be reluctant to take advantage
5 of remote computing technology—because of the diminished privacy protection—and society
6 may lose the substantial cost-saving and efficiency gains resulting from this new technology.

7 ECPA's gag order provisions not only portend adverse consequences for cloud
8 computing; they also violate the Constitution. By prohibiting companies like Microsoft from
9 speaking about an issue of public concern—government surveillance of their customers—the
10 gag orders constitute content-based restrictions on speech and prior restraints. They are
11 permissible only if the strict scrutiny standard is satisfied, but ECPA's "reason to believe"
12 standard allows gag orders based on a much lesser showing.

13 ECPA's provisions categorically prohibiting customers from receiving notice about
14 government searches of their intimate and private data also impinge on Fourth Amendment
15 rights. Users' data is protected by the Fourth Amendment, and notice is an essential ingredient
16 of the Fourth Amendment's reasonableness analysis. ECPA authorizes surreptitious searches
17 without the strong justification for withholding notice that the Fourth Amendment requires.

18 ARGUMENT

19 I. ECPA'S AUTHORIZATION OF SURREPTITIOUS SEARCHES WILL 20 IMPEDE REALIZATION OF THE VERY SUBSTANTIAL BENEFITS OF 21 CLOUD COMPUTING SERVICES.

22 "Cloud computing is the capacity of Internet-connected devices to display data stored
23 on remote servers rather than on the device itself." *Riley v. California*, 134 S. Ct. 2473, 2491
24 (2014). These technologies, also known generically as Internet-based data services, permit the
25 user to conduct a wide range of data storage or processing operations that until recently were
26 performed on the user's desktop computer or local server. The physical hardware that performs
27 those tasks is owned by the data services provider and accessed via the Internet, but the user
does not perceive any difference in his or her experience. Jared A. Harshbarger, *Cloud*

1 *Computing Providers and Data Security Law*, 16 J. Tech. L. & Pol’y 229, 232 (2011). Indeed,
 2 as the Supreme Court has recognized, “users often may not know whether particular
 3 information is stored on the device or in the cloud.” *Riley*, 134 S. Ct. at 2491.

4 Cloud computing makes sophisticated services available to all users, individuals and
 5 also businesses of all sizes. And it promises to provide very substantial benefits to the
 6 economy, in terms of increased productivity. Internet-based data services also promise very
 7 substantial societal benefits and will provide significant incentives for further innovation.

8 Those benefits will not be fully realized if the decision to use cloud computing carries
 9 with it a very significant reduction in privacy rights—particularly protection against
 10 government surveillance. But that is the inevitable consequence of allowing the government to
 11 continue obtaining gag orders of indefinite duration under ECPA.

12 **A. Business and Individual Users of Internet-Based Data Services Entrust**
 13 **Their Most Intimate, Confidential, and Valuable Information to Third-**
Party Providers.

14 In *Riley v. California*, a unanimous Supreme Court described the highly personal
 15 information that individuals store in electronic form:

16 First, a cell phone collects in one place many distinct types of information—an
 17 address, a note, a prescription, a bank statement, a video—that reveal much
 18 more in combination than any isolated record. Second, a cell phone’s capacity
 19 allows even just one type of information to convey far more than previously
 20 possible. *The sum of an individual’s private life can be reconstructed* through a
 thousand photographs labeled with dates, locations, and descriptions Third,
 the data on a phone can date back to the purchase of the phone, or even earlier.
 . . . Finally, there is an element of pervasiveness that characterizes [information
 contained in] cell phones.

21 134 S. Ct. at 2489-90 (emphasis added).

22 *Riley* addressed this question in the context of information stored on cell phones, but the
 23 Court recognized that all of this information may be stored securely “in the cloud” rather than
 24 in the cell phone itself. 134 S. Ct. at 2491. And the “immense storage capacity” of modern cell
 25 phones emphasized in *Riley*, *id.* at 2489, is dwarfed by the essentially limitless storage
 26 accessible through cloud computing. Individuals can store in the cloud *all* of their email
 27 messages, *all* of their photographs and videos, and *all* of their personal financial and health

1 data. Indeed, modern communication and storage devices “are so pervasive that some persons
2 may consider them to be essential means or necessary instruments for self-expression, even
3 self-identification.” *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010).

4 Prior to the advent of remote data services technologies, this broad swath of information
5 would not have been stored with a third party—individuals would have kept it in their homes.
6 Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 Miss. L.J. 1309, 1316
7 (2012). This shift in personal and business practices is the result of dramatic reductions in the
8 cost of storing digital data. In 1984—that is, two years prior to ECPA’s enactment—it cost
9 \$85,000 to store a single gigabyte of data; by 2011, that price had dropped to approximately
10 five cents. Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev.
11 373, 391 (2014). In the mid to late 1990s, when free email services first became available,
12 those services “generally came with about 2 megabytes of storage space. In contrast, today’s
13 popular free Gmail service comes with fifteen *gigabytes* (GB) of storage space, about seventy-
14 five hundred times more storage than was common a decade ago.” *Id.* at 392 (emphasis added).

15 Today, a government search of the information stored by an individual using cloud
16 technology “would typically expose to the government far *more* than the most exhaustive
17 search of a house”—not just “many sensitive records previously found in the home” but also “a
18 broad array of private information never found in a home in any form.” *Riley*, 134 S. Ct. at
19 2491. The same conclusion applies to electronic information stored by businesses. A
20 company’s most confidential business information—proprietary technology, financial data,
21 intellectual property, business plans, manufacturing processes, acquisition plans and
22 negotiating strategy, customer data, privileged and confidential legal advice regarding pending
23 lawsuits and other sensitive matters—will be embodied in the emails, documents, and other
24 electronic information stored with the company’s cloud services provider.

25 **B. Cloud Computing Technology Promises Dramatic Economic and Societal**
26 **Benefits.**

27 Cloud computing is “one of the most significant technical advances for global business

1 in this decade—as important as PCs were to the 1970s.” Nancy J. King & V.T. Raja, *What Do*
 2 *They Really Know About Me in the Cloud?*, 50 Am. Bus. L.J. 413, 418 (2013). It provides
 3 significant practical benefits to the businesses and individuals that use these services.

4 *First*, the ability to access data from a remote data center creates significant economies
 5 of scale, resulting in reduced costs for businesses and individual customers. A cloud computing
 6 provider can provide data backup services, business continuity, security, and other data
 7 operation functions far more efficiently than individual businesses. Kevin Werbach, *The*
 8 *Network Utility*, 60 Duke L.J. 1761, 1821-22 (2011). In addition, because “companies share
 9 virtual capacity in massive clouds,” large remote data centers provide a better solution to
 10 fluctuating demand. *Id.* at 1822. Cloud service providers offer a pool of servers to customers
 11 who then can rapidly harness those servers’ collective computing power when needed (“scaling
 12 up”), and then rapidly release that power when the desired task is completed (“scaling down”).
 13 Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the*
 14 *Cloud*, 73 Md. L. Rev. 313, 325 (2013).

15 These enhanced capabilities and reduced costs will increase productivity by hundreds of
 16 billions of dollars. James Manyika et al., McKinsey Global Institute, *Disruptive Technologies:*
 17 *Advances That Will Transform Life, Business, and the Global Economy* at 65 (2013),
 18 <http://goo.gl/p0EuC6>. And by lowering the barriers to entry for small companies, cloud
 19 computing creates new opportunities for innovation across the economy. *ECPA Reform and the*
 20 *Revolution in Cloud Computing: Hearing before the Subcomm. on the Constitution of the H.*
 21 *Comm. on the Judiciary*, 111th Cong. 30 (2011) [hereinafter *The Revolution in Cloud*
 22 *Computing*] (statement of Michael Hintze, Microsoft Corp.).

23 *Second*, cloud computing providers’ greater scale enables them to direct vastly greater
 24 resources into protecting against hacks and other unlawful intrusions than a business,
 25 university, or government (particularly state and local government) attempting to manage its
 26 own computer systems in-house. Harshbarger, 16 J. Tech. L. & Pol’y at 234. Moreover,
 27 Internet-based computing provides businesses with disaster recovery services on a much more

1 cost-efficient basis. *See* Lee Badger et al., *Recommendations of the Nat'l Inst. of Standards &*
 2 *Tech., U.S. Dep't of Commerce, NIST Special Publication 800-146: Cloud Computing Synopsis*
 3 *and Recommendations*, at Sec. 5-4 (2012), <http://goo.gl/KNlaJM>.

4 *Third*, allowing users to access their devices from any location in the world that has
 5 Internet access also enhances seamless data portability—the user can create a document on a
 6 home laptop, edit it on a tablet, review it on a desktop computer at work, and then share it with
 7 colleagues around the world. *See The Revolution in Cloud Computing*, 14-15 (statement of
 8 Edward W. Felten, Dir., Ctr. For Info. Tech. Policy, Princeton Univ.).

9 For all of these reasons, businesses, universities, and governments are choosing to
 10 outsource their data storage and computing functions to third-party providers in order to reduce
 11 cost, enhance flexibility, and improve security.

12 **C. Many Individuals And Businesses Will Be Reluctant To Use Cloud**
 13 **Computing Services If, As The Government Asserts, Their Private**
 14 **Information Receives Significantly Diminished Legal Protection.**

15 Individuals and businesses are increasingly concerned about maintaining the
 16 confidentiality of the electronically-stored data that contains their most private information. If
 17 moving that information from a desktop computer (or a cell phone) to the cloud means that it
 18 will have reduced legal protection, then companies and individuals naturally will be more
 19 reluctant to use this new technology.

20 “[P]eople now are more anxious about the security of their personal data and are more
 21 aware that greater and greater volumes of data are being collected about them.” Lee Rainie &
 22 Shiva Maniam, *Americans Feel the Tensions between Privacy and Security Concerns*, Pew
 23 Research Center (Feb. 19, 2016), <http://goo.gl/zfetT5>. Eighty percent of adults “agree” or
 24 “strongly agree” that Americans should be concerned about government monitoring of phone
 25 calls and internet communications. Mary Madden, *Public Perceptions of Privacy and Security*
 26 *in the Post-Snowden Era*, Pew Research Center (Nov. 12, 2014), <http://goo.gl/ivNYHD>.

27 These concerns have been heightened by the revelations by Edward Snowden about
 U.S. government access to personal information. “Americans’ lack of confidence in” the

1 privacy of information communicated electronically “tracks closely with how much they have
 2 heard about government surveillance programs.” *Id.* Many technology companies responded by
 3 announcing they would provide customers with greater security for their personal information.
 4 *See, e.g.,* Berkman Center for Internet & Society at Harvard University, *Don’t Panic: Making*
 5 *Progress on the “Going Dark” Debate*, at 3-4 (2016), <http://goo.gl/98KaEc>.

6 Moreover, the ability of U.S. companies to compete in the cloud computing market is
 7 injured by users’ perceptions that privacy protections are reduced because of greater
 8 government surveillance in the United States. A recent report found that damage to U.S.
 9 providers due to perceptions of U.S. government surveillance practices “will likely far exceed”
 10 \$35 billion. Daniel Castro and Alan McQuinn, *Beyond the USA Freedom Act: How U.S.*
 11 *Surveillance Still Subverts U.S. Competitiveness* at 1 (2015), <http://goo.gl/Ob21Jn>; *see also*
 12 Elizabeth Dwoskin and Frances Robinson, *NSA Internet Spying Sparks Race to Create*
 13 *Offshore Havens for Data Privacy*, Wall St. J. (Sept. 27, 2013), <http://goo.gl/i2NLss>
 14 (explaining that foreign countries “are seeking to use data-privacy laws as a competitive
 15 advantage—a way to boost domestic companies that long have sought an edge over Google,
 16 Microsoft Corp. and other U.S. tech giants”).

17 ECPA’s gag orders conceal previously-available information regarding the scope of
 18 governmental access to private information, thus reducing transparency and further eroding the
 19 privacy of users’ information vis-à-vis the government. Because, prior to the advent of cloud
 20 services, that information was stored on the premises of businesses and in individuals’ homes,
 21 either in physical or electronic form, the government had to obtain a warrant and serve the
 22 owner of the information. ECPA thus works a significant change in individuals’ ability to know
 23 whether the government is searching their information—and how frequently the government
 24 searches information of businesses and individuals. If the statute is upheld, there is a significant
 25 prospect of reduced (or foregone) use of cloud technology, the corresponding loss of economic
 26 and societal benefits, and the disadvantaging of U.S. businesses in comparison to foreign
 27 competitors.

II. SECTION 2705(B)'S BROAD GAG ORDER AUTHORIZATION VIOLATES THE CONSTITUTION.

A. The First Amendment Prohibits Restriction of Speech Based on a Mere “Reason to Believe” that Adverse Consequences Would Occur.

ECPA gag orders restrain speech of great interest to providers’ customers—both those who learn of government access to their information and those whose information is not sought but who learn of the extent to which the government searches or seizes information held by their provider. The speech restrained by these orders also relates to a topic of general public interest and grave concern: government surveillance of electronic data. *See supra* at p. 6 .

1. A gag order must satisfy the strict scrutiny standard.

These gag orders are “content-based” speech restrictions because they target “speech with a particular content,” *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 564 (2011)—the identities of customers whose information is sought by the government. These gag orders also are a prior restraint on speech, among “the most serious and least tolerable infringement on First Amendment rights.” *Nebraska Press Ass’n v. Stuart*, 427 U.S. 539, 559 (1976). “Any system of prior restraints of expression comes . . . bearing a heavy presumption against its constitutional validity.” *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963).

Content-based restrictions on speech and prior restraints each are subject to strict scrutiny review. *See Sorrell*, 564 U.S. at 565-66 (content-based restrictions); *Levine v. United States Dist. Court for the Cent. Dist. of Cal.*, 764 F.2d 590, 595 (9th Cir. 1985) (prior restraints). Gag orders therefore must be “narrowly tailored to promote a compelling Government interest.” *United States v. Playboy Entm’t Group, Inc.*, 529 U.S. 803, 813 (2000).

2. The statutory guidelines for issuing a gag order do not satisfy strict scrutiny.

Section 2705(b) authorizes a gag order if the court “determines that there is *reason to believe*” that disclosure of the warrant would result in one of five specified “adverse result[s].” 18 U.S.C. § 2705(b) (emphasis added). The standard established by the “reason to believe” test is not clear from the face of the statute. It could be satisfied by any reason to believe, no matter

1 how remote—which would fall far short of the compelling interest required by strict scrutiny.

2 Alternatively, “reason to believe” might be interpreted as equivalent to the reasonable
3 belief or fair probability required to establish probable cause. *In re: National Security Letters*,
4 Nos. 11-cv-02173-SI, *et al.*, at 29 (N.D. Cal. Mar. 29, 2016) (interpreting the standard in the
5 national security letter context to require the government to set forth specific facts showing a
6 “reasonable likelihood” that the adverse consequences would occur) (Doran Decl. [Dkt. 45],
7 Ex. B); *see also Florida v. Harris*, 133 S. Ct. 1050, 1055 (2013) (defining probable cause);
8 *United States v. Gorman*, 314 F.3d 1105, 1110 (9th Cir. 2002) (stating in related context that
9 “reason to believe” “embodies the same standard of reasonableness inherent in probable
10 cause”). Significantly, however, the government’s motion to dismiss studiously avoids this
11 position, presumably because—as Microsoft’s allegations and the cases interpreting Section
12 2705(b) indicate—the government’s practice has been to rely on mere boilerplate, *not* case-
13 specific probable cause. First Amend. Compl. ¶ 29; *In re Fifteen Subpoenas*, No. 16-MC-1300,
14 at 2-3, 8 n.7 (E.D.N.Y. May 12, 2016) (Doran Decl. [Dkt. 45], Ex. E).

15 In any event, probable cause falls far short of what is required to satisfy strict scrutiny.
16 *Hopper v. City of Pasco*, 241 F.3d 1067, 1074-75 (9th Cir. 2001) (distinguishing strict scrutiny
17 from “more lenient” reasonableness test). That construction therefore could not save the statute.

18 Section 2705(b) further authorizes a gag order of indefinite duration without providing
19 for ongoing review to ensure that the speech may continue to be restrained. “An indefinite non-
20 disclosure order is tantamount to a permanent injunction of prior restraint.” *In re Sealing and*
21 *Non-Disclosure of Pen/Trap/2703(D)*, 562 F. Supp. 2d 876, 886 (S.D. Tex. 2008); *see also In*
22 *Matter of Search Warrant for [redacted]@hotmail.com*, 74 F. Supp. 3d 1184 (N.D. Cal. 2014).
23 Section 2703(b) fails strict scrutiny for the independent reason that it does not require that the
24 gag order be lifted when the threat of adverse consequences has abated.

25 ECPA gag orders restrain speech of enormous public significance. The nation is
26 debating the proper reach of government’s power to intrude into the private information held by
27 electronic communications providers; that debate has depended on disclosures to the press

1 revealing details of the scale of government electronic surveillance. The government “carries a
 2 heavy burden of showing justification for the imposition of such a restraint.” *Organization for*
 3 *a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971). That burden remains unsatisfied so long as
 4 the government can restrain electronic service providers’ speech indefinitely and without
 5 proving that restricting public debate is necessary to protect an overriding interest.

6 **B. ECPA’s Warrant Authority Violates The Fourth Amendment.**

7 Notice is critical under the Fourth Amendment because it enables the affected
 8 individual to take action to protect his or her constitutional rights and because it is a touchstone
 9 element of whether the search is reasonable under the Fourth Amendment.

10 ECPA specifically relieves the government of any obligation to provide notice to a
 11 customer. 18 U.S.C. § 2703(b)(1)(A). That provision, in combination with ECPA’s
 12 authorization for gag orders prohibiting service providers from giving their customers notice,
 13 effectively precludes *all* notice to the individual whose Fourth Amendment rights are violated.

14 Searches performed under this categorical “no notice” regime violate the Fourth
 15 Amendment. The only way such searches may be upheld, therefore, is if the government in a
 16 particular case demonstrates a sufficiently weighty justification for prohibiting notice—and
 17 ECPA fails to impose such an obligation on the government.

18 ***1. The Fourth Amendment generally requires contemporaneous notice to***
 19 ***the owner of property to be searched or seized, absent a strong***
 20 ***justification for withholding notice.***

21 Notice is important in assessing the permissibility of government actions under the
 22 Fourth Amendment. In *Wilson v. Arkansas*, 514 U.S. 927 (1995), the Supreme Court addressed
 23 “whether the common-law knock and announce principle forms a part of the Fourth
 24 Amendment reasonableness inquiry.” *Id.* at 930. After finding that this notice principle existed
 25 in England under the common law and “was woven quickly into the fabric of early American
 26 law,” *id.* at 933, the Court concluded that notice was an essential part of the reasonableness
 27 analysis. *Id.* at 936. This was true even though certain limited circumstances—such as a threat
 of physical violence—may justify an unannounced entry. *See id.* at 935-36.

1 Similarly, in *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986), the Ninth Circuit
 2 stated, in relation to a warrant that authorized surreptitious entry to a home, that “the absence of
 3 any notice requirement in the warrant casts strong doubt on its constitutional adequacy.” *Id.* at
 4 1456. That is “because surreptitious searches and seizures strike at the very heart of the
 5 interests protected by the Fourth Amendment.” *Id.* The court held that the warrant violated the
 6 Fourth Amendment and directed that warrants should “provide explicitly for notice within a
 7 reasonable, but short, time subsequent to the surreptitious entry. Such time should not exceed
 8 *seven days* except upon a *strong* showing of *necessity*.” *Id.* (emphases added).

9 ECPA does not satisfy that standard. Far from requiring the government to make a
 10 “strong showing of necessity,” ECPA eliminates government notice in all cases, prohibits
 11 notice by the provider based on a mere “reason to believe,” and allows the lack of notice to last
 12 indefinitely. That falls far short of the requirements of *Wilson* and *Freitas*.

13 **2. The Fourth Amendment’s protection of users’ confidential personal**
 14 **and business information is not vitiated because users store that**
information with third-party providers.

15 Information protected by the Fourth Amendment if stored on the user’s premises in
 16 physical form or on a user’s laptop or smart phone does not lose that protection merely because
 17 the user chooses instead to store that information with a third party. Indeed, “[c]ell phone users
 18 often may not know whether particular information is stored on the device itself or in the
 19 cloud” as it “generally makes little difference” to the user. *Riley*, 134 S. Ct. at 2491.

20 The Supreme Court has made clear that technological advances should not by
 21 themselves reduce Fourth Amendment rights. The Court has instead sought to “preserv[e] th[e]
 22 degree of privacy against government that existed when the Fourth Amendment was adopted.”
 23 *Kyllo v. United States*, 533 U.S. 27, 34 (2001). That is why *Kyllo v. United States* held that the
 24 police needed a search warrant to use a thermal-imaging device that revealed details of a
 25 home’s interior. *Id.* (“To withdraw protection of this minimum expectation [of privacy within
 26 the home] would be to permit police technology to erode the privacy guaranteed by the Fourth
 27 Amendment.”). The Court followed the same approach in *Riley* when it rejected application of

1 the search-incident-to-arrest doctrine to modern smart phones. 134 S. Ct. at 2495.

2 In *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), the Sixth Circuit correctly
 3 concluded that e-mails in the possession of third parties are protected by the Fourth
 4 Amendment and invalidated portions of ECPA permitting warrantless searches of e-mails.
 5 Recognizing that “the Fourth Amendment must keep pace with the inexorable march of
 6 technological progress[] or its guarantees will wither and perish,” *id.* at 285, the court reasoned
 7 that “[e-]mail is the technological scion of tangible mail, and . . . plays an indispensable part in
 8 the Information Age,” *id.* at 286. An internet service provider is the “functional equivalent of a
 9 post office”; just as “the police may not storm the post office and intercept a letter . . . unless
 10 they get a warrant,” *id.*, so, too, must they obtain a warrant to search a user’s e-mail account.

11 The user “enjoys a reasonable expectation of privacy in the contents of emails that are
 12 stored with, or sent or received through, a commercial [internet service provider],” and to the
 13 extent “[ECPA] purports to permit the government to obtain such emails warrantlessly, [ECPA]
 14 is unconstitutional.” *Id.* at 288; *accord In re Grand Jury Subpoena*, __ F.3d __, 2016 WL
 15 3745541, at *5 (9th Cir. July 13, 2016) (a user’s “claim to a reasonable expectation of privacy
 16 in the contents of the emails is . . . not undermined by [third party’s] possession of the emails”);
 17 *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (“doubt[ing] that
 18 people would accept without complaint the warrantless disclosure to the Government of a list
 19 of every Web site they had visited in the last week, or month, or year”).

20 The Fourth Amendment thus protects the information that is the subject of these
 21 warrants. If the information sought by the government under ECPA were in physical form
 22 inside an individual’s home or a business’s office, notice would generally be required. *Riley*,
 23 *Kyllo*, and *Warshak* make clear that advances in technology cannot relieve the government of
 24 that obligation. Failing to provide notice for an indefinite—potentially infinite—period violates
 25 the Fourth Amendment in the absence of proof by the government of sufficiently weighty,
 26 case-specific justifications. Section 2703(b)(1)(A) therefore violates the Fourth Amendment.

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

CONCLUSION

The Defendants' motion to dismiss should be denied.

DATED this 2nd day of September, 2016.

LANE POWELL PC

By s/Ryan P. McBride
Ryan P. McBride, WSBA No. 33280
Email: mcbrider@lanepowell.com
1420 Fifth Avenue, Suite 4200
P O Box 91302
Seattle, WA 98111
Telephone: 206-223-7000
Facsimile: 206-223-7107

Andrew J. Pincus*
Travis Crum*
MAYER BROWN LLP
1999 K Street NW
Washington, DC 20006
Telephone: 202-263-3000

Attorneys for Amici Curiae

* Application for Leave to Appear Pro Hac Vice
Pending

CERTIFICATE OF SERVICE

Pursuant to RCW 9A.72.085, the undersigned certifies under penalty of perjury under the laws of the State of Washington, that on the 2nd day of September, 2016, the document attached hereto was presented to the Clerk of the Court for filing and uploading to the CM/ECF system. In accordance with their ECF registration agreement and the Court's rules, the Clerk of the Court will send e-mail notification of such filing to those attorneys of record registered on the CM/ECF system.

Executed on the 2nd day of September, 2016, at Seattle, Washington.

s/Ryan P. McBride

Signature of Attorney

WSBA No. 33280

Typed Name: Ryan P. McBride

Address: 1420 Fifth Avenue, Suite 4200

P.O. Box 91302

Seattle, WA 98111-9402

Telephone: 206.223.7000

Fax: 206.223.7107

E-mail: mcbrider@lanepowell.com

Attorney(s) For: Amici Curiae The Chamber of Commerce of the United States of America, the Center for Democracy and Technology, the National Association of Manufacturers, *et al.*