JUDGE JAMES L. ROBART

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

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

NOTE ON MOTION CALENDAR:
September 2, 2016

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

INTRODUCTION

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 (collectively, "Movants") respectfully move for leave to file a brief as *amici curiae* in support of Plaintiff Microsoft Corporation's opposition to Defendants' motion to dismiss. Movants affirm that no counsel for a party has authored this brief in whole or in part and that no person other than movants, their counsel, and their members made a monetary contribution to its preparation or submission. Movants have conferred with counsel for Plaintiff and Defendants, and both have consented to the granting of this motion for leave to file Movant's proposed *amici curiae* brief. The proposed *amici curiae* brief is attached hereto as Exhibit A; a proposed order granting leave is attached as Exhibit B.

IDENTITY AND INTEREST OF *AMICI*

Movants are organizations representing businesses and individuals who use cloud-computing services as well as individual companies that use these services. Because the Court's decision in this case could significantly affect the ability of businesses and individuals to maintain the privacy of their most confidential information, *amici* have a substantial interest in this proceeding. The proposed *amici curiae* brief explains the nature of cloud computing and its importance to the U.S. economy, and why the statutory provisions at issue in this case, if permitted to stand, will harm U.S. business and societal interests.

The proposed *amici* are:

- The Chamber of Commerce of the United States of America ("Chamber") is the world's largest business federation representing 300,000 direct members and indirectly representing an underlying membership of more than three million businesses and organizations of every size, in every industry sector, and from every region of the country. A central function of the Chamber is to represent the interests

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

of its members in matters before Congress, the Executive Branch, and the courts.

- The Center for Democracy and Technology ("CDT") is a nonprofit advocacy organization that works to ensure that the human rights we enjoy in the physical world are realized online and that technology continues to serve as an empowering force for people worldwide. Integral to this work is CDT's representation of the individual and public interest in the creation of an open, innovative, and decentralized Internet that promotes the constitutional and democratic values of free expression, privacy, and individual liberty.
- The National Association of Manufacturers ("NAM") is the largest manufacturing association in the United States, representing small and large manufacturers in every industrial sector and in all 50 states. Manufacturing employs nearly 12 million men and women, contributes more than $2 trillion to the U.S. economy annually, has the largest economic impact of any major sector, and accounts for two-thirds of private-sector research and development. The NAM is the voice of the manufacturing community and the leading advocate for a policy agenda that helps manufacturers compete in the global economy and create jobs across the United States.
- Alaska Airlines, Inc. is a leading U.S. airline headquartered in Seattle, Washington. Alaska and its regional partners fly approximately 32 million passengers annually to over 110 destinations with an average of 970 daily flights throughout the United States, including Hawaii, Canada, Costa Rica and Mexico.
- Archive360, Inc. is a global software technology company that provides next generation email archive migration software solutions and cloud-based storage for regulatory compliance, legal, and low touch data.
- AvePoint is the leader in Microsoft Cloud solutions, providing software and services that migrate, manage, and protect Office 365 and SharePoint data for 15,000 organizations and 5 million cloud users.
- BP America Inc., is part of the BP group of companies which is a global leader in

the energy industry. Since 2006, BP has invested more than $90 billion in U.S. oil, gas, and renewable as well as the technology to produce them safely.

- Delta Air Lines, Inc., is a leader in the airline industry, offering service to over 300 destinations in 62 countries on six continents. Delta serves nearly 180 million customers each year and employs 80,000 people worldwide.
- Eli Lilly and Company is a global healthcare leader that unites caring with discovery to make life better for people around the world. Lilly was founded more than a century ago by a man committed to creating high-quality medicines that meet real needs, and today Lilly remains true to that mission in all its work. Across the globe, Lilly employees work to discover and bring life-changing medicines to those who need them, improve the understanding and management of disease, and give back to communities through philanthropy and volunteerism.
- Getty Images (US), Inc., is among the world's leading creators and distributors of award-winning still imagery, video, music, and multimedia products, as well as other forms of premium digital content, available through its trusted house of brands, including iStock and Thinkstock. With its advanced search and image recognition technology, Getty Images (US), Inc., serves business customers in more than 100 countries and is the first place creative and media professionals turn to discover, purchase and manage images and other digital content.
- GlaxoSmithKline LLC is a Delaware limited liability company and the US operating company for GlaxoSmithKline, a science-led global healthcare company that researches and develops a broad range of innovative products in three primary areas of pharmaceuticals, vaccines and consumer healthcare.
- H5 is a leading eDiscovery company that specializes in the expert use of advanced technology combined with scientific expertise in search and information analysis to find the documents that matter in high profile litigation and investigations and help corporations and law firms meet litigation discovery, compliance and information

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

management objectives. H5's client list includes some of the nation's largest corporations and most prominent law firms.

- The Information Coalition advances best practices in enterprise information and information governance. The Information Coalition represents the interests of a broad base of practitioners and vendors by providing collaborative, hands-on resources that enable organizations to best reduce risk and increase value of their information and processes.
- Onsupport is a leader in the healthcare industry, providing security risk analysis, technology consulting, and cloud hosting services to covered entities and their business associates. Onsupport helps businesses ranging from single practicioners to large, hospital networks secure and protect ePHI (Electronic Protected Healthcare Information).
- Wipfli LLP ranks among the top 20 accounting and business consulting firms in the nation, with more than 1,700 associates located in 37 offices in the United States and two offices in India. For over 86 years, Wipfli has provided private and publicly held companies with industry-focused assurance, accounting, tax and consulting services to help clients overcome their business challenges today and plan for tomorrow.

Following Federal Rule of Civil Procedure 7.1, the Movants make the following corporate disclosure statements:

- Alaska Airlines, Inc. is wholly owned by its parent corporation Alaska Air Group, Inc. Apart from that relationship, no public company owns more than 10% of the stock of Alaska Airlines, Inc.
- BP America Inc., is a wholly owned indirect subsidiary of BP plc, which is a publicly traded company. No publicly traded company owns 10% or more of BP plc.
- Getty Images (US), Inc., is a wholly owned subsidiary of Getty Images, Inc.,

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

which is wholly owned by other entities that are not publicly traded. A majority of those not publicly traded entities is indirectly held by an affiliate of The Carlyle Group LP, which is a publicly traded Delaware limited partnership.

- GlaxoSmithKline LLC is owned, through several levels of wholly-owned subsidiaries, by GlaxoSmithKline plc, a publicly-traded public limited company organized under the laws of England. GlaxoSmithKline plc has no parent company. To the knowledge of GlaxoSmithKline LLC and GlaxoSmithKline plc, none of the shareholders of GlaxoSmithKline plc beneficially owns ten percent or more of its outstanding shares. However, Bank of New York Mellon ("BNYM") acts as Depositary in respect to Ordinary Share American Depositary Receipts ("ADRs") representing shares in GlaxoSmithKline plc. In that capacity, BNYM is the holder, but not the beneficial owner, of more than ten percent of the outstanding shares in GlaxoSmithKline plc on behalf of the ADR owners who are the beneficial owners of these shares, none of whom to GlaxoSmithKline plc's knowledge own ten percent or more of its outstanding shares.
- None of the other proposed *amici* has a parent company, and no publicly held company owns 10% or more of the stock of the other proposed *amici*.

AUTHORITY

District courts have "broad discretion to appoint amici curiae." *Hoptowit v. Ray*, 682 F.2d 1237, 1260 (9th Cir. 1982). "An amicus brief should normally be allowed . . . when the amicus has unique information or perspective that can help the court beyond the help that the lawyers for the parties are able to provide." *Community Ass'n for Restoration of the Env't v. Deruyter Brothers Dairy*, 54 F. Supp. 2d 974, 975 (E.D. Wash. 1999) (citing *Miller-Wohl Co. v. Commissioner of Labor & Indus.*, 694 F.2d 203, 204 (9th Cir. 1982)).

Movants offer a unique perspective. They explain that remote computing services—the storage "in the cloud" of individuals' and companies' most confidential information embodied

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

in emails, documents, photographs, and other materials—substitute for the storage of such information on users' own premises, either in physical form or in their own computer systems. That technology provides substantial benefits to individuals, businesses, and the entire U.S. economy—in the form of reduced cost, increased efficiency, and greater protection against hackers and other unauthorized intruders.

Those benefits are threatened, however, by the government's extensive use of gag orders issued pursuant to the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2703(b) & 2705(b). When information was stored in an individual's home or on a business's premises, the government had to serve a warrant on the individual or business in order to obtain the information—and the individual or business could contest the government's demand.

ECPA's broad gag order authority, therefore, has the effect of significantly reducing the privacy protection for individuals and businesses that use cloud services. Users will be reluctant to store information in the cloud if their privacy protection is diminished, and society will lose the substantial cost-saving and efficiency gains of this emerging technology.

Proposed *amici* further argue that ECPA's gag order provisions violate the Constitution. In a variety of contexts, the Supreme Court has held that constitutional protections should not be diluted by the use of new technologies. *See Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *Kyllo v. United States*, 533 U.S. 27 (2001). The same result is warranted here.

First, by prohibiting companies like Microsoft from speaking about an issue of public concern—namely, government surveillance of their customers—the gag orders constitute content-based restrictions on speech and prior restraints. Such limitations are permissible only if the strict scrutiny standard is satisfied, but ECPA's "reason to believe" standard allows gag orders based on a much lesser showing.

Second, ECPA's provisions prohibiting customers from receiving notice about government searches of their most intimate and private data also violate the Fourth Amendment. Users' data is protected by the Fourth Amendment, and notice is an essential

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

ingredient of the Fourth Amendment's reasonableness analysis. ECPA authorizes surreptitious searches without the strong justification for withholding or delaying notice that the Fourth Amendment requires.

For these reasons, Movants respectfully request that the Court grant this unopposed motion for leave to file a brief as *amici curiae*.

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.*

EXHIBIT A

JUDGE JAMES L. ROBART

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

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

TABLE OF CONTENTS

Page

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

TABLE OF AUTHORITIES

Page(s)

CASES

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

Page(s)

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

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

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

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

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

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

ARGUMENT

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

"Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley v. California*, 134 S. Ct. 2473, 2491 (2014). These technologies, also known generically as Internet-based data services, permit the user to conduct a wide range of data storage or processing operations that until recently were performed on the user's desktop computer or local server. The physical hardware that performs 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*

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

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

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

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

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

> First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously 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.

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

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

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

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

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

B. Cloud Computing Technology Promises Dramatic Economic and Societal Benefits.

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

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

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

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

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

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

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

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

B. ECPA's Warrant Authority Violates The Fourth Amendment.

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

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

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

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.

Notice is important in assessing the permissibility of government actions under the Fourth Amendment. In *Wilson v. Arkansas*, 514 U.S. 927 (1995), the Supreme Court addressed "whether the common-law knock and announce principle forms a part of the Fourth Amendment reasonableness inquiry." *Id.* at 930. After finding that this notice principle existed in England under the common law and "was woven quickly into the fabric of early American law," *id.* at 933, the Court concluded that notice was an essential part of the reasonableness 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.

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

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

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.

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

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

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

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

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

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

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

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.*

EXHIBIT B

THE HONORABLE JAMES L. ROBART

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION, Plaintiff, v. THE UNITED STATES DEPARTMENT OF JUSTICE, and LORETTA LYNCH, in her official capacity as Attorney General of the United States, Defendants.	Case No. 2:16-cv-00538-JLR **(PROPOSED) ORDER GRANTING MOTION OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA, THE CENTER FOR DEMOCRACY AND TECHNOLOGY, THE NATIONAL ASSOCIATION OF MANUFACTURERS, *ET AL*. FOR LEAVE TO FILE AN *AMICI CURIAE* BRIEF IN SUPPORT OF MICROSOFT CORPORATION'S OPPOSITION TO DEFENDANT'S MOTION TO DISMISS** **NOTE ON MOTION CALENDAR:** September 2, 2016

ORDER

The Court has reviewed the Unopposed Motion of 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 for Leave to File an *Amicus Curiae* Brief in Support of Microsoft Corporation's Opposition to Defendant's Motion to Dismiss. The

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107

Court ORDERS that the motion is GRANTED. The Clerk is directed to accept for filing the *Amicus Curiae* Brief attached as Exhibit A to the Unopposed Motion for Leave to File filed by 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.

Dated this _____ day of _____, 2016.

_____
HON. JAMES L. ROBART
United States District Judge

Presented by:

LANE POWELL PC

By *s/ Ryan P. McBride*
Ryan P. McBride, WSBA No. 33280
Telephone: 206.223.7000
Facsimile: 206.223.7107
Email: mcbrider@lanepowell.com
Attorneys 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.

LANE POWELL PC
1420 FIFTH AVENUE, SUITE 4200
P.O. BOX 91302
SEATTLE, WA 98111-9402
206.223.7000 FAX: 206.223.7107