The Honorable James L. Robart

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

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

CORPORATE DISCLOSURE STATEMENT

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

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

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

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

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

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

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

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

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

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

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

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

TABLE OF CONTENTS

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

TABLE OF AUTHORITIES

Page(s)

CASES:

STATUTES:

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

STATEMENT OF INTEREST

Amazon.com, Box, Cisco Systems, Dropbox, Evernote, Google, LinkedIn, Pinterest, Salesforce, Snapchat, and Yahoo respectfully submit this brief as *amici curiae*[1] in support of Microsoft Corporation.

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

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

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

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

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

[1] No party or counsel for a party authored or paid for this brief in whole or in part, or made a monetary contribution 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.

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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

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

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

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

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

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

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

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

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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

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

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

---

[2] *See, e.g.*, Amazon, *Information Requests*, https://aws.amazon.com/compliance/amazon-information-requests/; Cisco, *Trust and Transparency Center*, 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 Report for 2015*, https://evernote.com/legal/transparency; Google, *Transparency Report*, https://www.google.com/transparencyreport/userdatarequests/US/; LinkedIn, *Our Transparency Report*, https://www.linkedin.com/legal/transparency; Pinterest, *Transparency Report*, https://help.pinterest.com/en/articles/transparency-report; Snapchat, *Transparency Report*, https://www.snapchat.com/transparency; Yahoo, *Transparency Report*, https://transparency.yahoo.com/government-data-requests/country/United%20States**/31/?tid=31.

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

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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

INTRODUCTION

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

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

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

[4] *See, e.g.*, Quentin Hardy, *The Era of Cloud Computing*, N.Y. Times (June 11, 2014).

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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

ARGUMENT

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

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

> [S]urreptitious searches . . . strike at the very heart of the interests protected by the Fourth Amendment. The mere thought of strangers walking through and visually examining the center of our privacy interest, our home, arouses our passion for freedom as does nothing 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).

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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

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

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

[5] A judge may "postpone[]" the required notice upon a finding of good cause to do so. 18 U.S.C. § 2518(8)(d).

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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

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

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

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

[6] See the transparency reports cited *supra* note 2.

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

- 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.
- 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.
- 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.

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

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

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

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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

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

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

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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

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

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

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

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

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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

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

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

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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

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

CONCLUSION

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

DATED: September 2, 2016

HOGAN LOVELLS US LLP

By: s/ Neal Kumar Katyal
Neal Kumar Katyal
Attorney for *Amici Curiae*

HOGAN LOVELLS US LLP
555 THIRTEENTH STREET, N.W.
WASHINGTON, DC 20004
(202) 637-5600 FAX: (202) 637-5910

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*