EXHIBIT A

The Honorable James L. Robart

UNITED STATES DISTRICT COURT FOR THE
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.

No. 2:16-cv-00538-JLR

[PROPOSED] BRIEF OF *AMICI CURIAE* LAW PROFESSORS IN SUPPORT OF PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

NOTE ON MOTIONS CALENDAR:
SEPTEMBER 2, 2016

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

TABLE OF CONTENTS

Page

INTRODUCTION 1

ARGUMENT 2

I. THE GOVERNMENT'S USE OF SECTION 2705(b) VIOLATES HISTORICAL UNDERSTANDINGS OF THE FIRST AND FOURTH AMENDMENTS. 2

A. English and Colonial Law Favoring Notice of a Search Was Carried into the Fourth Amendment. 3

B. The Fourth Amendment Was Enacted to Bar Unreasonable Searches that Were Used to Inhibit Freedom of Expression. 4

II. THE GOVERNMENT'S USE OF SECTION 2705(b) CONTRAVENES MODERN FIRST AND FOURTH AMENDMENT JURISPRUDENCE. 6

A. More than Ever, Section 2705(b) Is Unconstitutional Because It Bars Provider Speech about Law Enforcement Demands and Deprives Individuals of Notice. 6

B. Finding 2705(b) Unconstitutional Follows Historical Practice of Preserving Core Constitutional Protections as Technology Evolves. 9

CONCLUSION 12

APPENDIX OF *AMICI CURIAE* LAW PROFESSORS A1

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

TABLE OF AUTHORITIES

Page(s)

Cases

In re App. of United States,
620 F.3d 304 (3d Cir. 2010).....11

Atwater v. City of Lago Vista,
532 U.S. 318 (2001).....1, 4

Berger v. New York,
388 U.S. 41 (1967).....9

Boyd v. United States,
116 U.S. 616 (1886).....2, 3, 5

Butterworth v. Smith,
494 U.S. 624 (1990).....8

City of Ontario v. Quon,
130 S.Ct. 2619 (2010).....9, 10

Clapper v. Amnesty Int'l USA,
133 S.Ct. 1138 (2013).....8

Entick v. Carrington,
95 Eng.Rep. 807 (K.B. 1765).....5

Gentile v. State Bar of Nevada,
501 U.S. 1030 (1991).....7, 8

Globe Newspaper Co. v. Superior Court,
457 U.S. 596 (1982).....5, 9

In re Grand Jury Subpoena,
2016 WL 3745541 (9th Cir. July 13, 2016).....11

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

In re Grand Jury Subpoena to Facebook,
No. 16-mc-1300, Mem. and Order (E.D.N.Y. May 12, 2016).....11

Katz v. United States,
389 U.S. 347 (1967).....10

Ker v. California,
374 U.S. 23 (1963).....3

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

Klayman v. Obama,
957 F. Supp. 2d 1 (D.D.C. 2013). 11

Kyllo v. United States,
533 U.S. 27 (2001) 10

Marcus v. Search Warrants,
367 U.S. 717 (1961) 1, 5

Merrill v. Lynch,
151 F. Supp. 3d 342 (S.D.N.Y. 2015) 10

Microsoft v. United States,
2016 WL 3770056 (2d Cir. July 14, 2016) 11

Mills v. Alabama,
384 U.S. 214 (1966) 5

In re Nat'l Sec. Letters,
No. 11-cv-2173, slip op. (N.D. Cal. Mar. 29, 2016) 10

Olmstead v. United States,
277 U.S. 438 (1928) 1, 10

Powers v. Ohio,
499 U.S. 400 (1991) 8

Reno v. ACLU,
521 U.S. 844 (1997) 10

Richmond Newspapers, Inc. v. Virginia,
448 U.S. 555 (1980) 5, 6

Riley v. California,
134 S.Ct. 2473 (2014) 1, 10, 11, 12

In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders,
562 F. Supp. 2d 876 (S.D. Tex. 2008) 8

In re Search of Google Email Accounts Identified in Attachment A,
92 F. Supp. 3d 944 (D. Alaska 2015) 11

In re Search of Premises Known as: Three Hotmail Email Accounts,
2016 WL 1239916 (D. Kan. Mar. 28, 2016) 11

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

United States v. Freitas,
800 F.2d 1451 (9th Cir. 1986) 9, 12

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

United States v. Graham,
824 F.3d 421 (4th Cir. 2016) 11

United States v. Jones,
132 S.Ct. 945 (2012) 10, 11, 12

United States v. Playboy Entm't Grp.,
529 U.S. 803 (2000) 10

United States v. Villegas,
899 F.2d 1324 (2d Cir. 1990) 9

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 11

Wilkes v. Wood,
98 Eng.Rep. 489 (C.P. 1763) 5

Wilson v. Arkansas,
514 U.S. 927 (1995) 1, 3, 4, 9

Constitutional Provisions

U.S. Const. amend. IV 2

Statutes

18 U.S.C. § 2705(b) ..... *passim*

Other Authorities

Samuel Beckett,
Waiting for Godot (1953) 9

G. Robert Blakey,
The Rule of Announcement and Unlawful Entry: Miller v. United States *and*
Ker v. California, 112 U. Pa. L. Rev. 499 (1964) 3, 4

2 Wayne R. LaFave,
Search and Seizure: A Treatise on the Fourth Amendment
§ 4.8(a) (5th ed. 2010) 3

Nelson B. Lasson,
The History and Development of the Fourth Amendment to the United States
Constitution (1937) 5

Jonathan Manes,
Online Service Providers and Surveillance Law Transparency,
125 Yale L.J. F. 343 (2016) 7

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

Roger Roots,
The Originalist Case for the Fourth Amendment Exclusionary Rule,
45 Gonz. L. Rev. 1 (2010) 4, 5

Mag. Judge Stephen Wm. Smith,
Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket,
6 Harv. L. & Pol'y Rev. 313 (2012) 7, 8, 9

Daniel J. Steinbock,
Announcement in Police Entries,
80 Yale L.J. 139 (1970) 4

James J. Tomkovicz,
California v. Acevedo*: The Walls Close in on the Warrant Requirement*,
29 Am. Crim. L. Rev. 1103 (1992).....5

Jonathan Witmer-Rich,
The Rapid Rise of Delayed Notice Searches, and the Fourth Amendment "Rule Requiring Notice," 41 Pepp. L. Rev. 509 (2014).....3, 12

9 Writings of James Madison (G. Hunt ed., 1910) 5

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

INTRODUCTION

Amici curiae law professors, whose work focuses on privacy, technology, security, and constitutional law, write to assist the Court by providing important context for the Government's motion to dismiss Microsoft's challenge to secrecy orders under 18 U.S.C. § 2705(b) that accompany digital searches and seizures.[1] That provision of the Electronic Communications Privacy Act ("ECPA"), which authorizes "preclusion of notice," violates historical and modern understandings of the First and Fourth Amendments because it allows the Government to indefinitely bar online service providers from speaking publicly or notifying users about the seizures they effect at the Government's behest. Section 2705(b) is therefore unconstitutional.

The Government's use of Section 2705(b) today decisively departs from the Constitution's historical underpinnings. Under pre-founding law, notice accompanied execution of a warrant in all but extreme circumstances. That common-law rule was incorporated into the Fourth Amendment, which offered protections considered critical to privacy, liberty, and free expression. As the Framers recognized, the right to discuss and criticize government affairs presupposed the right to be free from arbitrary and abusive Government intrusions. The Supreme Court has since repeatedly affirmed—in watershed opinions authored by Justices of all constitutional perspectives—that historical understandings of the Government's search-and-seizure authority guide modern interpretation of the Fourth Amendment. *See, e.g.*, *Riley v. California*, 134 S.Ct. 2473, 2484, 2494-95 (2014) (Roberts, J., for a unanimous court); *Atwater v. City of Lago Vista*, 532 U.S. 318, 326 (2001) (Souter, J.); *Wilson v. Arkansas*, 514 U.S. 927, 931-36 (1995) (Thomas, J., for a unanimous court); *Marcus v. Search Warrants*, 367 U.S. 717, 724-29 (1961) (Brennan, J., for a unanimous court); *Olmstead v. United States*, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting). Here, the historical understandings cannot be squared with Section 2705(b).

The Government's widespread use of Section 2705(b) to impose an indefinite gag order is also incompatible with modern First and Fourth Amendment jurisprudence. The principles underlying the First and Fourth Amendments have remained constant since the Founding. But

[1] The Appendix lists the identity and interest of *amici*, who have filed an unopposed motion for leave to submit this brief. No party or its counsel authored this brief in whole or in part, and no person (including a party or its counsel), other than *amici* or their counsel, contributed money intended to fund preparing or submitting this brief.

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

experience shows the Government will push the limits of those principles, and overstep them, whenever it can. Today, the exponential increase in the depth and breadth of information the Government can easily obtain, in an age where vast troves of personal data are customarily stored in the cloud, requires courts to reconsider how to apply those principles in order to maintain the delicate balance between privacy and security. Section 2705(b) dramatically upsets that balance. It tips the scales far in favor of the Government by indefinitely gagging online service providers, who are uniquely positioned to inform the public about the Government's use and interpretation of its search-and-seizure authority. As a result, Section 2705(b) inhibits public debate regarding the protection of online privacy against Government intrusions, precludes the public from learning the Government has violated an individual's privacy, and prevents individuals from vindicating their constitutional rights, including the right to notice of a search. That must end. This Court should deny the Government's motion to dismiss and hold that Section 2705(b) is unconstitutional.

ARGUMENT

I. THE GOVERNMENT'S USE OF SECTION 2705(b) VIOLATES HISTORICAL UNDERSTANDINGS OF THE FIRST AND FOURTH AMENDMENTS.

The Fourth Amendment secures individual liberty and privacy from arbitrary governmental searches and seizures. *See, e.g.*, *Boyd v. United States*, 116 U.S. 616, 624-27 (1886). Although the Fourth Amendment does not mention notice, there is compelling historical evidence that notice is implicit in its prohibition of "unreasonable searches and seizures." U.S. Const. amend. IV.

When America was founded, English law required notice for most governmental searches and seizures. Notice was regularly provided in the American colonies, and that practice was carried into the Constitution. In addition, history reveals that restrictions on the search-and-seizure power were understood to be critical to ensuring freedom of speech—the ability to speak about government (mis)conduct presupposed protection from unreasonable intrusions, and protection from unreasonable intrusions presupposed the ability to speak about government (mis)conduct. The Government's modern-day reliance on Section 2705(b) to prevent service providers from informing the public and users about the Government's exercise of its ECPA authority conflicts with these founding-era understandings that inform whether a practice is constitutional today.

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

A. English and Colonial Law Favoring Notice of a Search Was Carried into the Fourth Amendment.

The Fourth Amendment resulted from "a centuries-long history of legal, political, and popular opposition to expansive and abusive search powers." Jonathan Witmer-Rich, *The Rapid Rise of Delayed Notice Searches, and the Fourth Amendment "Rule Requiring Notice,"* 41 Pepp. L. Rev. 509, 565 (2014). In particular, the Framers reacted to the English practice of using "writs of assistance"—general warrants that failed to describe with particularity what officers were authorized to search and seize. *See, e.g.*, *Boyd*, 116 U.S. at 625-26. Writs of assistance empowered English officers to use "discretion" to search "suspected places" for illegal goods—a practice described during the colonial era as "'the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book.'" *Id.* at 625 (citation omitted). The detested writs allowed officers to enter homes at will and indiscriminately seize personal papers, one's "'dearest property.'" *Id.* at 628 (citation omitted).

Despite the awesome power of a writ of assistance, colonial officers were nonetheless required to give notice when executing one. 2 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 4.8(a) (5th ed. 2010). The notice requirement was part of English common law centuries before the establishment of the American colonies. *See Wilson*, 514 U.S. at 932 n.2. As early as 1603, English courts recognized that except in exigent circumstances a government officer "'ought to signify the cause of his coming, and to make request to open doors,'" when "'execut[ing] the King's process.'" *Id.* at 931 (citation omitted). And officers actually made such requests. "[P]rominent founding-era commentators agreed" that the "'constant practice'" was for officers to "'first signify to those in the house the cause of his coming, and request them to give him admittance'" before exercising search-and-seizure authority. *Id.* at 932-33 (citation omitted).[2] The English tradition of providing notice of a search was adopted in the colonies. "It was firmly established long before the adoption of the Bill of Rights that the fundamental liberty of the individual includes protection against unannounced police entries." *Ker v. California*, 374 U.S. 23, 47, 52 (1963) (Brennan, J., dissenting) ("[G]eneral warrants and writs of assistance [were]

[2] *See* G. Robert Blakey, *The Rule of Announcement and Unlawful Entry:* Miller v. United States *and* Ker v. California, 112 U. Pa. L. Rev. 499, 500-02 (1964) (discussing the history of the notice requirement in English law).

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

usually preceded at least by some form of notice."); Daniel J. Steinbock, *Announcement in Police Entries*, 80 Yale L.J. 139, 142-44 (1970) ("American colonial experience with announcement prior to entrance was parallel to England's: execution of all warrants was made with notice.").

The notice requirement, a critical feature of searches and seizures in Colonial America, was implicitly carried into the Constitution. Although the Fourth Amendment's text does not specifically mention notice, the common-law notice requirement "forms a part of" the Fourth Amendment's "reasonableness inquiry," which is "guided by the meaning ascribed to it by the Framers." *Wilson*, 514 U.S. at 929, 931; *see also Atwater*, 532 U.S. at 326 (considering "'traditional protections against unreasonable searches and seizures afforded … at the time of the framing,'" because such "'common-law understanding of an officer's authority'" shows "'what the Framers of the Amendment might have thought to be reasonable'"). It would make little sense to interpret the Fourth Amendment differently. Why would the Founders have considered non-exigent searches *without* notice to be reasonable if even the hated writs of assistance that inspired their revolution were executed *with* notice? *See* Steinbock, *supra*, at 145 n.29. And why would the Founders have required in the Fourth Amendment that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized" if they were comfortable with warrants that provided targets no notice about the scope of an officer's search-and-seizure authority? *See* Roger Roots, *The Originalist Case for the Fourth Amendment Exclusionary Rule*, 45 Gonz. L. Rev. 1, 38-39 & nn.241, 248 (2010). The obvious answer is that they did not. This conclusion is reinforced by multiple 19th century decisions that presumed, consistent with historical understanding of the Government's search-and-seizure authority, that officers must give notice when executing a warrant. *See* Blakey, *supra* note 2, at 507-08; *Wilson*, 514 U.S. at 933-34. The Government's use of Section 2705(b) to avoid providing constitutionally required notice of searches, including those effected under ECPA, sharply contrasts with this longstanding tradition.

B. The Fourth Amendment Was Enacted to Bar Unreasonable Searches that Were Used to Inhibit Freedom of Expression.

History also demonstrates that restricting the Government's search-and-seizure power was critical to securing the freedom of speech guaranteed by the First Amendment. For centuries

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

English authorities used freewheeling searches and seizures to suppress free speech—rummaging and ransacking in search of supposedly seditious and libelous papers. *Marcus*, 367 U.S. at 724-29. In *Wilkes v. Wood*, 98 Eng.Rep. 489 (C.P. 1763), and *Entick v. Carrington*, 95 Eng.Rep. 807 (K.B. 1765), English courts rejected warrants that authorized general searches for papers by writers and publishers who criticized the government. *See* Nelson B. Lasson, *The History and Development of the Fourth Amendment to the United States Constitution* 43-48 (1937). "It may be confidently asserted" that those cases "were in the minds of those who framed the fourth amendment … and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures." *Boyd*, 116 U.S. at 626-27; *see, e.g.*, Roots, *supra*, at 38-39 (*Wilkes* and *Entick* are "universally acknowledged" as "the most famous search and seizure cases known to the drafters of the Fourth Amendment"). The Fourth Amendment was therefore "fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression." *Marcus*, 367 U.S. at 728-29; *see* James J. Tomkovicz, California v. Acevedo*: The Walls Close in on the Warrant Requirement*, 29 Am. Crim. L. Rev. 1103, 1148 (1992) ("The Framers understood that privacy was a critical premise of free speech.").

To ensure liberty was not stifled, the Framers rejected limits on speech about how government exercises its authority: "Whatever differences may exist about interpretations of the First Amendment, there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs. This of course includes discussions of … structures and forms of government, [and] the manner in which government is operated or should be operated[.]" *Mills v. Alabama*, 384 U.S. 214, 218-19 (1966). As James Madison put it, "a people who mean to be their own Governors, must arm themselves with the power which knowledge gives." 9 Writings of James Madison 103 (G. Hunt ed., 1910). The First Amendment ensures that knowledge can flow freely. It "prohibit[s] government from limiting the stock of information from which members of the public may draw." *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 576 (1980). And it is designed to "ensure that … constitutionally protected 'discussion of governmental affairs,' is an informed one." *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 605 (1982). By contrast, Section 2705(b) allows the Government to

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

indefinitely restrict notice of and speech about its search-and-seizure practices with only a generalized showing of need. That violates the First Amendment, and in turn undermines the Fourth Amendment's role in guaranteeing free discussion of government affairs.

II. THE GOVERNMENT'S USE OF SECTION 2705(b) CONTRAVENES MODERN FIRST AND FOURTH AMENDMENT JURISPRUDENCE.

Section 2705(b) as it operates today violates historical understandings of the First and Fourth Amendments, and also conflicts with their modern application. Section 2705(b) violates the First Amendment by stifling speech about Government practices by online service providers who are uniquely positioned to increase the universe of information that the public may draw from to inform its debate about the proper balance between civil liberties and security. And Section 2705(b) violates the Fourth Amendment by allowing notice of a search to be withheld in perpetuity, thereby preventing a user from ever learning about the Government's conduct and insulating that conduct from public scrutiny and an adversarial challenge in the courts.

History, once again, resolves any doubt on this score. The way that constitutional law developed in response to emerging technology in the past strongly supports invalidating Section 2705(b) today. Time and again courts have tested the Government's then-contemporary practices against the foundational principles embodied in the First and Fourth Amendments and rejected those practices as unconstitutional. The Supreme Court and lower courts have recently done so as to a wide variety of the Government's digital search-and-seizure practices. This Court should do the same as to Section 2705(b) by concluding that the Government's routine reliance on Section 2705(b) to cloak its electronic search activities encroaches too deeply upon individual liberty.

A. More than Ever, Section 2705(b) Is Unconstitutional Because It Bars Provider Speech about Law Enforcement Demands and Deprives Individuals of Notice.

In curtailing providers' freedom to speak about the orders they receive, Section 2705(b) undermines the core First Amendment right to engage in informed discussion of government activities. Just as the First Amendment protected speech about government activity historically, it continues to do so today. *See, e.g.*, *Richmond*, 448 U.S. at 571-72, 580. And today that protection is especially critical when technology companies—like Microsoft—are the speakers.

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

Online service providers operate at the intersection of technology, privacy, and security. They make possible the global communication system that can simultaneously be used as a tool by those who favor democracy and justice as well as those with criminal intent. This puts providers "in a special position" to inform the important public discussion about balancing civil liberties and the Government's needs, because those providers "are privy to information that the rest of [the] public is not: they know what kinds of information the government demands of them." Jonathan Manes, *Online Service Providers and Surveillance Law Transparency*, 125 Yale L.J. F. 343, 344 (2016); Mag. Judge Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 Harv. L. & Pol'y Rev. 313, 330 (2012) (providers are in the "best position to challenge ECPA orders"). Simply put, that public discussion *depends* on those companies being able to speak freely about their relationship and experience with the Government. Without that speech, the public cannot understand what the Government is doing. And if the public cannot understand what the Government is doing, it can neither ensure the Government's searches and seizures are reasonable nor assess whether the legal barriers protecting online privacy are too low or too high.

Yet in practice Section 2705(b) bars exactly this type of bedrock First Amendment speech about government affairs. A Section 2705(b) gag order forbids service providers from revealing when they are conscripted to search and seize their customers' information and disclose it to the Government. It prevents the public from grasping or evaluating the extent of the Government's online investigative activities, the type or scope of alleged criminal activity it targets, and the justification for the Government's intrusions. It even obscures the very existence—and the substance—of the massive shadow ECPA docket in courthouses across the country. *See* Judge Smith, *supra*, at 313-22. These harms erode trust in government at a crucial moment when public and legal institutions are actively deliberating about how to adapt core protections for liberty and privacy to the cloud computing era. Section 2705(b) therefore cannot be squared with the First Amendment. *Gentile v. State Bar of Nev.*, 501 U.S. 1030, 1034 (1991) ("[S]peech critical of the exercise of the State's power lies at the very center of the First Amendment.").

Courts across the country have recognized that, by silencing service providers, Section 2705(b) may unconstitutionally inhibit public scrutiny of government conduct. For example, one

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

court rejected the Government's application for an open-ended Section 2705(b) order because such orders "cannot stand" in "an era of increasing public demand for transparency about the extent of government demands for data from providers." *Matter of Grand Jury Subpoena for: [Redacted]@yahoo.com*, 79 F. Supp. 3d 1091, 1095 (N.D. Cal. 2015). Another court pointedly observed that Section 2705(b)'s "pernicious effects of concealing even lawful conduct should not be overlooked" because "these secret orders, issued by the thousands year after year by court after court around the country, may conceal from the public the actual degree of government intrusion that current legislation authorizes." *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 886 (S.D. Tex. 2008). These decisions rest comfortably on longstanding precedent highlighting the importance of transparency and rejecting efforts to shield government conduct from public review. *See, e.g.*, *Gentile*, 501 U.S. at 1035; *Butterworth v. Smith*, 494 U.S. 624, 632, 636 (1990) (invalidating statute barring disclosure of "information relating to alleged governmental misconduct," which is "at the core of the First Amendment," because it could be used "to silence those who know of unlawful conduct or irregularities on the part of public officials"). But these district court rulings, rightly decided, are not binding elsewhere. This Court should build on them by invalidating Section 2705(b) whenever the Government tries to use it.

Section 2705(b) also insulates the Government's actions from judicial and public scrutiny. When the Government seizes an individual's data from a service provider, and bars the provider from disclosing that seizure, the individual cannot mount a challenge. How could she contest a search that she doesn't know (or can't reasonably allege) happened? *See Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1148-49 (2013). A gagged provider could sue as a third party to vindicate its users' rights. *See Powers v. Ohio*, 499 U.S. 400, 410-11 (1991). But a provider cannot reasonably be expected to file or fully prosecute *tens of thousands* of lawsuits each year to do so, especially given the Government's mistaken view (MTD 11-12) that providers lack standing to challenge the search the Government compelled *them* to perform (often under threat of criminal contempt). *See also* Judge Smith, *supra* at 327-31 (lamenting difficulty of appealing ECPA cases). And the public benefit from such suits is mitigated because the proceedings would likely be under seal—frustrating the public's constitutional right of access that "ensure[s] that the individual

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

citizen can effectively participate in and contribute to" civic affairs. *Globe*, 457 U.S. at 604. In other words, the Government's misguided interpretation of Section 2705(b) enables it to impose a speech restriction (itself unconstitutional) to undermine First Amendment rights and to avoid Fourth Amendment scrutiny. That is incredibly dangerous for civil liberties. It cannot be the law.

Section 2705(b) is not rescued by its reference to "delayed notice." The indefinite "delay" is, in practice, typically *perpetual*. "[T]emporary sealing orders almost always become permanent" because "judges almost never have occasion to revisit these cases, so the 'further order' lifting the seal rarely arrives." Judge Smith, *supra*, at 325. This leaves the provider at the Government's mercy, waiting and wondering when, if ever, the Government will permit the provider to speak. As one court explained in rejecting an application for a Section 2705(b) order: "The problem is that the government does not seek to gag Microsoft for a day, a month, a year, or some other fixed period. … [I]t wants Microsoft gagged for … well, forever." *In re Search Warrant for: [Redacted]@hotmail.com*, 74 F. Supp. 3d 1184, 1185 (N.D. Cal. 2014); *cf.* Samuel Beckett, *Waiting for Godot*, Act I (1953). Even if delay is not perpetual, it can still violate the Constitution. *See, e.g.*, *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (mandating notice "within a reasonable, but short, time subsequent to [a] surreptitious" search, usually seven days); *United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) (same). Fourth Amendment "reasonableness" may be flexible, but the pervasive modern application of Section 2705(b) to bar targets from ever learning about a search bends the Fourth Amendment well beyond the breaking point. *See Berger v. New York*, 388 U.S. 41, 60 (1967) (rejecting wiretapping statute that had "no requirement for notice as do conventional warrants"); *cf. Wilson*, 514 U.S. at 934 (finding notice of a search is part of the Fourth Amendment's "reasonableness inquiry").

B. Finding 2705(b) Unconstitutional Follows Historical Practice of Preserving Core Constitutional Protections as Technology Evolves.

Rejecting Section 2705(b) is consistent with the arc of First and Fourth Amendment jurisprudence. Fourth Amendment "reasonableness" is meant to evolve to fit modern times. But this evolution happens slowly. By necessity, the law lags behind technology; the former responds cautiously, case by case, as the latter develops. *See, e.g.*, *City of Ontario v. Quon*, 560 U.S. 746,

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

759-60 (2010). But the law eventually catches up. When the time is right, courts strike down previously approved Government practices that can no longer be reconciled with first principles.

Many examples illustrate this point. In the Fourth Amendment context, the Supreme Court initially held "surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution." *Katz v. United States*, 389 U.S. 347, 353 (1967) (citing *Olmstead*, 277 U.S. at 457, 464-66 (majority op.)). The Court later rejected that "narrow view," because it "ignore[d] the vital role that the public telephone has come to play in private communication." *Id.* at 352-53; *see Kyllo v. United States*, 533 U.S. 27, 36 (2001) ("[T]he rule we adopt must take account of more sophisticated systems that are already in use or in development."). In the First Amendment context, the Court has similarly recognized that what might pass for a permissibly tailored speech restriction one day may be impermissibly broad the next, due to advancing technology. *United States v. Playboy Entm't Grp.*, 529 U.S. 803, 807-08, 814 (2000); *Reno v. ACLU*, 521 U.S. 844, 891 (1997) (O'Connor, J., concurring and dissenting in part) ("[W]e must evaluate" a statute "as it applies to the Internet as it exists today" not as it might develop).

Following this trend, courts are adapting constitutional law to account for ubiquitous technology and the reality that personal information previously stored on premises is now routinely stored in the cloud operated by online service providers. Courts have thus extended First Amendment protection to online providers who wish to speak about government investigative practices, invalidating and narrowing gag orders analogous to Section 2705(b) orders even in the context of national security investigations. *See Merrill v. Lynch*, 151 F. Supp. 3d 342, 344-46 (S.D.N.Y. 2015); *In re Nat'l Sec. Letters*, No. 11-cv-2173, slip op. 2-17 (N.D. Cal. Mar. 29, 2016).

The Supreme Court has also been refreshing Fourth Amendment doctrine to ensure that it provides as much protection in the digital age as it did in the analog and mechanical ones. In myriad contexts, the Court has emphasized the importance of "assur[ing] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34; *see also Riley*, 134 S.Ct. at 2495 ("[T]echnology … does not make the information any less worthy of the protection for which the Founders fought."); *United States v. Jones*, 132 S.Ct. 945, 949-51 & n.3 (2012); *Quon*, 560 U.S. at 759-60. Lower courts have followed

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

suit ad hoc, rejecting the Government's expansive interpretation of its authority to obtain digital evidence, including evidence stored in the cloud.[3] Justices and circuit judges have also questioned the scope of the third-party doctrine—which exempts information disclosed to third parties from Fourth Amendment protection—because the doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 132 S.Ct. at 957 (Sotomayor, J., concurring); *accord id.* at 963-64 (Alito, J., concurring) (using new technology to conduct previously impossible searches may "impinge[] on expectations of privacy").[4] As Judge Leon summarized in evaluating NSA's bulk metadata collection, "present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between" the Government and service providers—are "so thoroughly unlike those considered" by courts in the past that fresh scrutiny is required. *Klayman v. Obama*, 957 F. Supp. 2d 1, 30-32 & n.42 (D.D.C. 2013).

The Government (once again) misunderstands the scope and power of modern technology when it defends Section 2705(b) as only concealing searches that occur somewhere other than a user's home. *See* MTD 23. In *Riley*, a unanimous Supreme Court chastised the Government for equating "a search of all data stored on a cell phone" with a physical search, because "[t]hat is like saying a ride on horseback is materially indistinguishable from a flight to the moon." 134 S.Ct. at 2488. The same could be said of the Government's contention here. Section 2705(b) allows for secret digital searches that "implicate privacy concerns *far beyond* those implicated by the search" of physical objects, and that "would typically expose to the government *far more* than the most exhaustive search of a house." *Id.* at 2488-89, 2491 (emphasis added). Section 2705(b) permits secret seizures of digital data that are even more a person's "dearest property" than the physical

---

[3] *See, e.g.*, *Microsoft v. United States*, 2016 WL 3770056, at *1-2 (2d Cir. July 14, 2016) (finding Government cannot compel production of data held abroad); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (requiring warrant to obtain email "contents"); *In re Search of Premises Known as: Three Hotmail Email Accounts*, 2016 WL 1239916, at *11-15, *23 (D. Kan. Mar. 28, 2016) (denying warrant for "entire email account" due to "substantial amount of data collected"); *In re Grand Jury Subpoena to Facebook*, No. 16-mc-1300, Mem. & Order (E.D.N.Y. May 12, 2016) (denying non-specific request for Section 2705(b) order); *In re Search of Google Email Accounts Identified in Attachment A*, 92 F. Supp. 3d 944, 953 (D. Alaska 2015) (denying warrant for emails without date restrictions).

[4] *See also In re App. of United States*, 620 F.3d 304, 317-18 (3d Cir. 2010) (declining to apply third-party doctrine to cell site location information ("CSLI")); *United States v. Graham*, 824 F.3d 421, 441 n.2 (4th Cir. 2016) (en banc) (Wynn, J., dissenting) (collecting dissents and concurrences questioning application of third-party doctrine to CSLI).

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

papers that have been protected since before the Founding. That data includes "a cache of sensitive personal information" that is "a digital record of nearly every aspect of [people's] lives—from the mundane to the intimate." *Riley*, 134 S.Ct. at 2490; *see also In re Grand Jury Subpoena*, 2016 WL 3745541, at *5 (9th Cir. July 13, 2016). It "reflects a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations." *Jones*, 132 S.Ct. at 955. The Ninth Circuit's reasons for rejecting clandestine searches of a physical home apply with even greater force to the clandestine searches of a digital home that Section 2705(b) purports to permit.

> [S]urreptitious searches and seizures of intangibles 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.

Freitas, 800 F.2d at 1456. "[T]hat covert searches and surveillance are favorite tools of totalitarian control and repression" reveals that Section 2705(b) poses "very real dangers to privacy, liberty, and dissent." Witmer-Rich, *supra*, at 555. Even in America, "[a]wareness that the Government may be watching chills associational and expressive freedoms." *Jones*, 132 S.Ct. at 956.

Of course the fruits of digital searches could prove useful to the Government. Technology enables those searches to be mind-bogglingly broad—capturing nearly every aspect of modern human existence—and to occur without a target's detection. But just as the Constitution has long guarded against secret government intrusions for even the juiciest evidence in the physical realm, it must protect against such searches in the digital realm. The Government should not get a Fourth Amendment free pass whenever evidence happens to be stored with a third party outside the user's home or business. Privacy and liberty depend on transparency. Service providers must be able to speak about the searches they have been compelled to conduct and the private user data they have been compelled to disclose. Users must also get notice of those actions to enable them to challenge improper Government practices. Section 2705(b) is unconstitutional because it permits the Government to obtain indefinite gag orders—without a compelling case-specific reason—and prevents the target of a search from receiving the notice required by the Fourth Amendment.

CONCLUSION

For the foregoing reasons, this Court should deny the Government's motion to dismiss.

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

DATED: September 2, 2016

Respectfully submitted,

By: /s/ David Freeburg

CORR CRONIN MICHELSON BAUMGARDNER FOGG & MOORE LLP

TODD WILLIAMS, WSBA No. 45032
DAVID FREEBURG, WSBA No. 48935
1001 Fourth Avenue, Suite 3900
Seattle, WA 98154
Tel: (206) 501-3512
twilliams@corrcronin.com
dfreeburg@corrcronin.com

GIBSON, DUNN & CRUTCHER LLP

ALEXANDER H. SOUTHWELL*
GABRIEL K. GILLETT*
200 Park Avenue
New York, New York 10166
Telephone: (212) 351-4000
asouthwell@gibsondunn.com
ggillett@gibsondunn.com

JONATHAN MANES, ESQ.*
University at Buffalo School of Law
The State University of New York
613 O'Brian Hall, North Campus
Buffalo, New York 14260-1100
Telephone: (716) 645-6222
jmmanes@buffalo.edu

*Pro Hac Vice Pending

Attorneys for Amici Law Professors

APPENDIX OF *AMICI CURIAE* LAW PROFESSORS

The following professors, who have a strong interest in this case because their research and teaching focus on privacy, technology, security, and constitutional law, have joined this brief as *amici curiae* to offer the Court their unique perspective and to help the Court decide the issues presented. This brief reflects the views of *amici*, but does not purport to reflect the views (if any) of any institutions that *amici* are affiliated with.

Jonathan Manes is Clinical Assistant Professor and Director of the Civil Liberties and Transparency Clinic at the University at Buffalo School of Law, the State University of New York. He writes, teaches, and directs the Clinic's efforts on issues involving the protection of individual rights and the public's right of access to information in the areas of national security, law enforcement, privacy, and technology.

Derek Bambauer is Professor of Law at the University of Arizona. His research explores freedom of speech, Internet censorship, intellectual property, and cybersecurity.

Jane Bambauer is Associate Professor of Law at the University of Arizona. Her research assesses the social costs and benefits of data, and involves many popular privacy laws.

Jordan "Jody" Blanke is Distinguished Professor of Computer Information Systems and Law at the Stetson School of Business and Economics at Mercer University in Atlanta. He writes about the law and ethics of privacy and technology and teaches courses such as The Law and Ethics of Big Data in a Business Analytics Master's Degree program and Privacy Law in an MBA program.

Catherine Crump is an Assistant Clinical Professor at the University of California, Berkeley School of Law and Associate Director of the Samuelson Clinic for Law, Technology, & Public Policy. Her writing, teaching, and clinical work focus on application of the First and Fourth Amendments to new technologies, in both the law enforcement and national security contexts.

Susan Freiwald is Professor of Law and Dean's Circle Scholar at the University of San Francisco School of Law. She teaches courses on criminal procedure, information privacy and internet law and writes extensively on the Fourth Amendment's application to new technologies and the electronic communications privacy laws.

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

David C. Gray is Professor of Law at the University of Maryland, Francis King Carey School of Law. He teaches courses on criminal procedure and writes extensively on the Fourth Amendment.

Dennis D. Hirsch is Professor of Law at The Ohio State University Moritz College of Law and the Capital University Law School. He also serves as director of the Program on Data and Governance at the Moritz College of Law. His research focuses on information privacy law and governance theory.

Margot E. Kaminski is Assistant Professor of Law at The Ohio State University Moritz College of Law and an Affiliated Fellow of the Yale Information Society Project. She writes on law and technology, with a focus on First Amendment and privacy law and the intersections between the two.

Vivek Krishnamurthy is the Assistant Director of the Cyberlaw Clinic at Harvard University's Berkman-Klein Center for Internet & Society and a Clinical Instructor and Lecturer on Law at Harvard Law School. His clinical teaching and academic research focus on the impacts of internet-based technologies on the human rights to privacy and free expression both here in the United States and around the world.

Yvette Joy Liebesman is Professor of Law at Saint Louis University School of Law. She teaches courses related to intellectual property and her research focuses on the intersection of intellectual property and technology.

Neil Richards is the Thomas & Karole Green Professor of Law at Washington University. He writes and teaches in the areas of First Amendment Law, Fourth Amendment Law, and privacy and technology law.

Jorge R. Roig is Associate Professor of Law at the Charleston School of Law (currently Visiting Associate Professor at the Touro College Jacob D. Fuchsberg Law Center). He writes and teaches on the subjects of Constitutional Law, Internet and Technology Law, and Intellectual Property, with a particular interest in issues regarding freedom of speech and privacy.

Ira Rubinstein is Senior Fellow at the Information Law Institute, New York University School of Law, where he is also an Adjunct Professor of Law. He writes and teaches in the areas

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

of privacy, cybersecurity, national security, voter privacy, and the intersection of privacy law and technical design.

David A. Schulz is Senior Research Scholar in Law and Clinical Lecturer at Yale Law School. His scholarly writing and legal practice focus on the First Amendment, access to information, and newsgathering law.

Adina Schwartz is Professor in the Department of Law, Police Science and Criminal Justice Administration at John Jay College of Criminal Justice, City University of New York. She teaches the required law course for students in the John Jay College Master's Program in Digital Forensics and Cybersecurity, and is Assistant Director of the Cybercrime Studies Center there. She writes on Fourth Amendment law, law and technology, and comparative legal regimes on data protection and national security.

Daniel J. Solove is the John Marshall Harlan Research Professor of Law at George Washington University Law School. His work focuses on information privacy law.

Katherine J. Strandburg is the Alfred B. Engelberg Professor of Law at the New York University School of Law. She teaches in the areas of patent law, innovation policy, and information privacy law, and her research considers the implications of "big data" for privacy law.

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave. New York, NY 10166-0193
Tel 212.351.4000

CERTIFICATE OF SERVICE

I hereby certify that on September 2, 2016, I electronically filed the foregoing [Proposed] Brief of *Amici Curiae* Law Professors in Support of Plaintiff's Opposition to Defendants' Motion to Dismiss with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorneys of record who are registered as such on the CM/ECF system.

Dated: September 2, 2016

/s/ David Freeburg
David Freeburg

GIBSON, DUNN & CRUTCHER LLP
200 Park Ave New York, NY 10166-0193
Tel 212.351.4000