

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

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.

No.

COMPLAINT FOR
DECLARATORY JUDGMENT

Microsoft Corporation (“Microsoft”) alleges as follows.

INTRODUCTION

1. Microsoft brings this case because its customers have a right to know when the government obtains a warrant to read their emails, and because Microsoft has a right to tell them. Yet the Electronic Communications Privacy Act (“ECPA”) allows courts to order Microsoft to keep its customers in the dark when the government seeks their email content or other private information, based solely on a “reason to believe” that disclosure might hinder an investigation. Nothing in the statute requires that the “reason to believe” be grounded in the facts of the particular investigation, and the statute contains no limit on the length of time such secrecy orders may be kept in place. 18 U.S.C. § 2705(b). Consequently, as Microsoft’s customers increasingly store their most private and sensitive information in the cloud, the government increasingly seeks (and obtains) secrecy orders under Section 2705(b). This

1 statute violates both the Fourth Amendment, which affords people and businesses the right to
2 know if the government searches or seizes their property, and the First Amendment, which
3 enshrines Microsoft’s rights to talk to its customers and to discuss how the government
4 conducts its investigations—subject only to restraints narrowly tailored to serve compelling
5 government interests. People do not give up their rights when they move their private
6 information from physical storage to the cloud. Microsoft therefore asks the Court to declare
7 that Section 2705(b) is unconstitutional on its face.

8 2. Before the digital age, individuals and businesses stored their most sensitive
9 correspondence and other documents in file cabinets and desk drawers. As computers became
10 prevalent, users moved their materials to local computers and on-premises servers, which
11 continued to remain within the user’s physical possession and control. In both eras, the
12 government had to give notice when it sought private information and communications, except
13 in the rarest of circumstances.

14 3. Cloud computing has spurred another profound change in the storage of private
15 information. Today, individuals increasingly keep their emails and documents on remote
16 servers owned by third parties, i.e., in the cloud, using free web-based services such as
17 Microsoft’s Outlook.com. Businesses have also migrated their information technology
18 infrastructure to servers hosted by providers such as Microsoft, which offer productivity
19 software (e.g., Microsoft’s Office365) and the ability to access correspondence and other
20 documents from any device. But the transition to the cloud does not alter the fundamental
21 constitutional requirement that the government must—with few exceptions—give notice when
22 it searches and seizes the private information or communications of individuals or businesses.

23 4. The government, however, has exploited the transition to cloud computing as a
24 means of expanding its power to conduct secret investigations. As individuals and business
25 have moved their most sensitive information to the cloud, the government has increasingly
26 adopted the tactic of obtaining the private digital documents of cloud customers not from the
27 customers themselves, but through legal process directed at online cloud providers like

1 Microsoft. At the same time, the government seeks secrecy orders under 18 U.S.C. § 2705(b)
2 to prevent Microsoft from telling its customers (or anyone else) of the government’s demands.
3 These secrecy orders generally assert that abiding by the centuries-old requirement of seeking
4 evidence directly from its owner would jeopardize the government’s investigation. Most of the
5 time, these secrecy orders prohibit notification for unreasonably long (or even unlimited)
6 periods of time, which Section 2705(b) permits whenever a court has “reason to believe” any of
7 several adverse consequences might otherwise ensue—including any time notice would
8 “seriously jeopardiz[e] an investigation or unduly delay[] a trial.”

9 5. Over the past 18 months, federal courts have issued nearly 2,600 secrecy orders
10 silencing Microsoft from speaking about warrants and other legal process seeking Microsoft
11 customers’ data; of those, more than two-thirds contained no fixed end date. (In fact, of the
12 twenty-five secrecy orders issued to Microsoft by judges in this District, *none* contained a time
13 limit.) These twin developments—the increase in government demands for online data and the
14 simultaneous increase in secrecy—have combined to undermine confidence in the privacy of
15 the cloud and have impaired Microsoft’s right to be transparent with its customers, a right
16 guaranteed by the First Amendment.

17 6. There may be exceptional circumstances when the government’s interest in
18 investigating criminal conduct justifies an order temporarily barring a provider from notifying a
19 customer that the government has obtained the customer’s private communications and data.
20 But Section 2705(b) sweeps too broadly. That antiquated law (passed decades before cloud
21 computing existed) allows courts to impose prior restraints on speech about government
22 conduct—the very core of expressive activity the First Amendment is intended to protect—
23 even if other approaches could achieve the government’s objectives without burdening the right
24 to speak freely. The statute sets no limits on the duration of secrecy orders, and it permits prior
25 restraints any time a court has “reason to believe” adverse consequences would occur if the
26 government were not allowed to operate in secret. Under the statute, the assessment of adverse
27 consequences need not be based on the specific facts of the investigation, and the assessment is

1 made *only* at the time the government applies for the secrecy order, with no obligation on the
2 government to later justify continued restraints on speech even if circumstances change
3 because, for instance, the investigation is closed or the subject learns of it by other means. It
4 also permits those restraints based on the application of purely subjective criteria, such as a
5 finding that notice would “jeopardiz[e] an investigation” in unspecified ways or “unduly delay
6 a trial.” Section 2705(b) is therefore facially overbroad under the First Amendment, since it
7 does not require the government to establish that the continuing restraint on speech is narrowly
8 tailored to promote a compelling interest.

9 7. The statute also violates the Constitution’s protection against unreasonable
10 searches and seizures. The Fourth Amendment’s requirement that government engage only in
11 “reasonable” searches necessarily includes a right for people to know when the government
12 searches or seizes their property. *See Wilson v. Arkansas*, 514 U.S. 927, 934 (1995). For
13 example, if the government comes into a person’s home to seize her letters from a desk drawer
14 or computer hard drive, that person in almost all circumstances has the right to notice of the
15 government’s intrusion. The same is true when the government executes a search of a business
16 to seize emails from the business’s on-site server. But Section 2705(b) subjects Microsoft’s
17 cloud customers to a different standard merely because of how they store their communications
18 and data: the statute provides a mechanism for the government to search and seize customers’
19 private information *without* notice to the customer, based upon a constitutionally insufficient
20 showing. In so doing, Section 2705(b) falls short of the intended reach of Fourth Amendment
21 protections, which do not depend on the technological medium in which private “papers and
22 effects” are stored.

23 8. For these reasons, Microsoft asks the Court to declare that Section 2705(b) is
24 unconstitutional on its face.

25 PARTIES

26 9. *Microsoft.* Microsoft is a corporation organized and existing under the laws of
27 the State of Washington, with its principal place of business at One Microsoft Way, Redmond,

1 Washington 98052. Microsoft has standing to bring this action because of the repeated
2 invasion of its First Amendment rights through the issuance of indefinite and insufficiently
3 substantiated secrecy orders, its interest in upholding its public commitment to safeguard the
4 privacy of its customers' sensitive emails and documents without violating court orders, its
5 right to invoke the Fourth Amendment rights of its customers (who have no practical means of
6 enforcing those rights), and its interest in avoiding findings of contempt.

7 10. ***The United States Department of Justice.*** The United States Department of
8 Justice is an agency of the executive branch of the federal government, employees of which
9 regularly apply for secrecy orders under 18 U.S.C. § 2705(b) and serve those secrecy orders on
10 providers, including Microsoft.

11 11. ***Loretta Lynch.*** Loretta Lynch, sued in her official capacity only, is the Attorney
12 General of the United States. Attorney General Lynch has ultimate authority over the United
13 States Department of Justice, employees of which regularly apply for secrecy orders under 18
14 U.S.C. § 2705(b) and serve those secrecy orders on providers, including Microsoft.

15 JURISDICTION AND VENUE

16 12. ***Jurisdiction.*** This Court has jurisdiction over this action pursuant to 28 U.S.C.
17 § 1331 because the action concerns federal questions, and pursuant to 28 U.S.C. §§ 2201 and
18 2202 because this is a civil action for a declaratory judgment.

19 13. ***Venue.*** Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2)
20 because Microsoft has its headquarters and principal place of business in this District and
21 because Microsoft's speech, in the absence of a secrecy order, would emanate in substantial
22 part from this District.

23 MICROSOFT'S CLOUD SERVICES

24 14. ***Cloud Computing.*** As they migrate their communications and documents to the
25 cloud, individuals and businesses have increasingly entrusted Microsoft and other providers
26 with their most private information—what the Supreme Court has referred to as a “cache of
27 sensitive personal information.” *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). A customer

1 that stored paper documents in file cabinets or emails on on-site servers would generally know
2 contemporaneously about the execution of a warrant by law enforcement—and would be able
3 to assert any rights concerning any documents or data seized during the search. A customer
4 storing documents and emails remotely in the cloud should be in the same position. That is,
5 cloud customers should be able to trust they will know if they become the targets of warrants or
6 other legal process authorizing the seizure of sensitive information.

7 15. **Secrecy Orders.** Secrecy orders issued under Section 2705(b) allow the
8 government to seek electronic communications and other private data under a veil of prolonged
9 (or even indefinite) secrecy. The government’s use of legal process directed at cloud providers
10 such as Microsoft, when combined with accompanying secrecy orders, amounts to a substantial
11 expansion of law enforcement’s ability to engage in secret search and seizure activity,
12 adversely affecting both Microsoft’s right to communicate with its customers and the
13 customers’ privacy interests—simply because customers have moved their information to the
14 cloud.

15 16. **The Frequency of Secrecy Orders.** Between September 2014 and March 2016,
16 Microsoft received 5,624 federal demands for customer information or data. Of those, nearly
17 half—2,576—were accompanied by secrecy orders, forbidding Microsoft from telling the
18 affected customers that the government was looking at their information. The vast majority of
19 these secrecy orders related to consumer accounts and prevent Microsoft from telling affected
20 individuals about the government’s intrusion into their personal affairs; others prevent
21 Microsoft from telling business customers that the government has searched and seized the
22 emails of individual employees of the customer. Further, 1,752 of these secrecy orders
23 contained no time limit, meaning that Microsoft could *forever* be barred from telling the
24 affected customer about the government’s intrusion. The government has used this tactic in
25 this District. Since September 2014, Microsoft received 25 secrecy orders issued in this
26 District, none of which contained any time limit. These secrecy orders prohibit Microsoft from
27 speaking about the government’s specific demands to *anyone* and forbid Microsoft from ever

1 telling its customers whose documents and communications the government has obtained. The
2 secrecy orders thus prevent Microsoft’s customers and the public at large from ever learning
3 the full extent of government access to private, online information.

4 **STATUTORY OVERVIEW**

5 17. **Section 2705(b).** Congress enacted Section 2705(b) as part of the Electronic
6 Communications Privacy Act of 1986 (“ECPA”). Section 2705(b) provides, in its entirety:

7 **(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL**
8 **ACCESS.**—A governmental entity acting under section 2703,
9 when it is not required to notify the subscriber or customer under
10 section 2703(b)(1), or to the extent that it may delay such notice
11 pursuant to subsection (a) of this section, may apply to a court for
12 an order commanding a provider of electronic communications
13 service or remote computing service to whom a warrant,
14 subpoena, or court order is directed, for such period as the court
15 deems appropriate, not to notify any other person of the existence
16 of the warrant, subpoena, or court order. The court shall enter
17 such an order if it determines that there is reason to believe that
18 notification of the existence of the warrant, subpoena, or court
19 order will result in—

- 14 (1) endangering the life or physical safety of an individual;
- 15 (2) flight from prosecution;
- 16 (3) destruction of or tampering with evidence;
- 17 (4) intimidation of potential witnesses; or
- 18 (5) otherwise seriously jeopardizing an investigation or unduly
19 delaying a trial.

20 18. **Effect of Statute.** Microsoft is a “provider of electronic communications
21 service or remote computing service” as those terms are used in the statute. Under the plain
22 terms of Section 2705(b), a court therefore may order Microsoft “not to notify **any other**
23 **person** of the existence” of a legal demand for its customer’s emails and documents. A court
24 may issue such an order “for such period as the court deems appropriate,” without any
25 requirement that the government advise the court of any change in circumstances bearing upon
26 the government’s initial asserted need for nondisclosure. Thus, for example, a secrecy order
27 may prevent Microsoft from informing a customer of the intrusion even after the government’s

1 investigation ends or becomes public through other means. Under the statute, a court is not
2 required to consider whether a secrecy order is narrowly tailored to further the government’s
3 asserted interests and whether there are less restrictive alternatives. Indeed, the statute
4 contemplates that the court “shall enter such an order” without weighing whether less
5 restrictive alternatives are available. Further, Section 2705(b) allows the court to issue a
6 secrecy order whenever it finds “reason to believe” that any of five adverse results would
7 otherwise occur, including when notification “will result in ... otherwise seriously jeopardizing
8 an investigation or unduly delaying a trial.”

9 19. ***Comparison to Section 2705(a).*** Section 2705(b) is notably different from its
10 parallel provision, Section 2705(a), which applies to certain forms of legal process issued under
11 ECPA, 18 U.S.C. § 2703(b)(1)(B). When the government requires a provider to disclose
12 information under this provision, the government itself has an affirmative obligation to notify
13 the customer. Section 2705(a) permits the government to delay its notice when “there is reason
14 to believe” notification will trigger the same five adverse results listed in Section 2705(b). But
15 even though Section 2705(a) relies on exactly the same government interests as Section
16 2705(b) to justify withholding notice, Section 2705(a) authorizes a delay of only a definite and
17 fixed duration—90 days—and requires the government to justify any further delays in
18 notification. In other words, in Section 2705(a), Congress determined that withholding notice
19 for no more than 90 days satisfied the five government interests enumerated in both Section
20 2705(a) and Section 2705(b), subject only to the government’s right to renew the period of
21 delayed upon making a further showing.

22 20. ***Searches in the Physical World.*** By allowing the government to operate behind
23 a veil of secrecy, Section 2705(b) also differs from similar forms of process in the physical
24 world. For example, although 18 U.S.C. § 3103a authorizes so-called “sneak and peek”
25 warrants for secret searches—the only permissible means of executing search warrants of
26 physical documents without notice—that provision presumptively requires the government to
27 notify the target of the search “within a reasonable period not to exceed 30 days after the date

1 of its execution.” 18 U.S.C. § 3103a(b)(3). The statute permits extensions of this deferred
2 notice, but “subject to the condition that extensions should only be granted upon an updated
3 showing of the need for further delay and that each additional delay should be limited to
4 periods of 90 days or less.” 18 U.S.C. § 3103a(c). While these provisions permit delays of
5 longer than 30 and 90 days “if the facts of the case justify a longer period of delay,” the statute
6 imposes temporal baselines lacking in Section 2705(b).

7 **COUNT I**

8 **REQUEST FOR DECLARATORY RELIEF –**

9 **INVALIDITY OF SECTION 2705(b) UNDER THE FIRST AMENDMENT**

10 21. ***Overbreadth Doctrine.*** “When the Government restricts speech, the
11 Government bears the burden of proving the constitutionality of its actions.” *Comite de*
12 *Jornaleros de Redondo Beach v. City of Redondo Beach*, 657 F.3d 936, 944 (9th Cir. 2011)
13 (“*Comite de Jornaleros*”) (internal quotation marks omitted). “In a facial challenge to a law’s
14 validity under the First Amendment, the law may be invalidated as overbroad if a substantial
15 number of its applications are unconstitutional, judged in relation to the statute’s plainly
16 legitimate sweep.” *Id.* (internal quotation marks omitted).

17 22. ***Presumptive Invalidity of Prior Restraints.*** A secrecy order “imposes a prior
18 restraint on speech.” *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F.
19 Supp. 2d 876, 882 (S.D. Tex. 2008) (“*In re Sealing*”). Any prior restraint “bear[s] heavy
20 presumption against its constitutional validity,” and the government has a “heavy burden of
21 showing justification for the imposition of such a restraint.” *Capital Cities Media, Inc. v.*
22 *Toole*, 463 U.S. 1303, 1305 (1983). Thus, because Section 2705 on its face authorizes the
23 issuance of secrecy orders that operate as a prior restraint on Microsoft’s speech, the
24 government’s burden of justifying the restraint is particularly heavy. The statute authorizes
25 secrecy orders that prohibit, *ex ante*, providers such as Microsoft from engaging in core
26 protected speech under the First Amendment, i.e., speech about the government’s access to
27 customers’ sensitive communications and documents and its increased surveillance on the

1 Internet. “Whatever differences may exist about interpretations of the First Amendment, there
2 is practically universal agreement that a major purpose of that Amendment was to protect the
3 free discussion of governmental affairs.” *Mills v. Alabama*, 384 U.S. 214, 218 (1971).

4 23. ***Content-Based Speech Restrictions.*** Secrecy orders issued under
5 Section 2705(b) also function as content-based restrictions on speech, as “they effectively
6 preclude speech on an entire topic—the [accompanying] order and its underlying criminal
7 investigations.” *In re Sealing*, 562 F. Supp. 2d at 881. Like prior restraints, “[c]ontent-based
8 regulations are presumptively invalid” and subject to strict scrutiny. *R.A.V. v. City of St. Paul*,
9 505 U.S. 377, 382 (1992). They may be upheld only if they are “narrowly tailored to promote a
10 compelling Government interest.” *United States v. Playboy Entm’t Group, Inc.*, 529 U.S. 803,
11 813 (2000). “If a less restrictive alternative would serve the Government’s purpose, the
12 legislature must use that alternative.” *Id.*

13 24. ***Presumptive Openness of Government Records.*** Secrecy orders also
14 improperly inhibit the public’s right of access to search warrants under both the common law
15 and the First Amendment. Upon application by a party, the press, or the public, search
16 warrants generally must be unsealed after investigations are concluded. *See United States v.*
17 *Bus. of Custer Battlefield Museum & Store*, 658 F.3d 1188, 1194-95 (9th Cir. 2011) (access to
18 search warrant materials may be denied only where “compelling reasons” outweigh
19 presumption of disclosure). But when a search warrant is accompanied by an indefinite secrecy
20 order, the public and the press—like the affected customer—may have no idea a warrant has
21 been issued. As a result, even after the government concludes an investigation, the public and
22 the press may have no effective way to learn about, discuss, and debate the government’s
23 actions.

24 25. ***Overbreadth of Section 2705(b).*** Section 2705(b) facially violates the First
25 Amendment because a substantial number of its applications are unconstitutional under these
26 standards, when judged in relation to the statute’s legitimate sweep. This overbreadth
27 manifests itself in at least three ways.

1 26. ***Indefinite Duration.*** First, Section 2705(b) is unconstitutional because it
2 permits secrecy orders “for such period as the court deems appropriate.” Because this language
3 at least allows a court to issue secrecy orders of a prolonged duration, and has been understood
4 by dozens of courts (including this one) to authorize indefinite secrecy orders, the statute
5 violates the First Amendment because it is not narrowly tailored to satisfy a compelling
6 government interest. Even when circumstances initially justify a secrecy order as the narrowest
7 means available to satisfy a compelling government interest, the First Amendment demands
8 that the provider be free to engage in truthful speech about the government’s activities as soon
9 as secrecy is no longer required to satisfy that interest. *In re Sealing*, 562 F. Supp. 2d at 895
10 (“As a rule, sealing and non-disclosure of electronic surveillance orders must be neither
11 permanent nor, what amounts to the same thing, indefinite.”); *In Matter of Search Warrant for*
12 *[Redacted]@hotmail.com*, 74 F. Supp. 3d 1184, 1185 (N.D. Cal. 2014) (reading Section
13 2705(b) to require a fixed end date on any secrecy order; observing the “First Amendment
14 rights of both Microsoft and the public” were affected by such an order); *In the Matter of the*
15 *Grand Jury Subpoena for: [Redacted]@yahoo.com*, 79 F. Supp. 3d 1091, 1091 (N.D. Cal.,
16 2015) (denying government’s application for indefinite order under Section 2705(b) because it
17 would “amount to an undue prior restraint of Yahoo!’s First Amendment right to inform the
18 public of its role in searching and seizing its information”). A secrecy order of a prolonged or
19 indefinite duration will apply beyond the point when a compelling government interest requires
20 it. As a result, to the extent it authorizes issuance of secrecy orders of prolonged or indefinite
21 duration, Section 2705(b) violates the First Amendment on its face. *See Butterworth v. Smith*,
22 494 U.S. 624, 635-36 (1993) (state statute indefinitely banning witnesses from disclosing
23 testimony given before a grand jury violates the First Amendment).

24 27. ***“Reason to Believe.”*** Second, Section 2705(b) is unconstitutionally overbroad
25 because it permits a court to issue a secrecy order whenever it has “reason to believe”
26 notification would result in one of five listed adverse results. But the statute does not require
27 that the “reason to believe” be grounded in the specific facts of a particular investigation, as

1 distinct from the government’s overall experiences or other unspecified considerations.
2 Further, the statute offers no guidance as to the evidentiary burden the government bears in
3 showing a “reason to believe” sufficient to justify a secrecy order. And the “reason to believe”
4 standard fails to require that a secrecy order be the least restrictive means available to further
5 the government’s interest in avoiding the specified adverse results, as the First Amendment
6 requires to justify this sort of restraint. The “reason to believe” standard therefore falls far
7 short of the “heavy burden” the First Amendment imposes when the government seeks to
8 impose a prior restraint on speech.

9 28. ***The Overbroad Catchall.*** Third, Section 2705(b) allows a court to issue secrecy
10 orders whenever it finds “reason to believe” notification of the target would “otherwise
11 seriously jeopardiz[e] an investigation or unduly delay[] a trial.” This subjective and vaguely-
12 defined provision allows the issuance of secrecy orders in the absence of any compelling
13 interest sufficient to justify a prior restraint or a content-based restriction on speech. There may
14 be compelling circumstances not captured within the “adverse results” specifically enumerated
15 in Section 2705(b)(1)-(4) that would justify a restraint on the provider’s speech, but this
16 catchall provision is substantially broader than necessary to account for those circumstances
17 and provides no meaningful constraints. It therefore violates the First Amendment.

18 29. ***Facial Overbreadth.*** Because Section 2705(b) is overbroad in each of the ways
19 described in the previous paragraphs, the government cannot overcome the presumption that
20 the provision on its face violates the First Amendment.

21 30. ***Judicial Declaration.*** A judicial declaration that Section 2705(b) violates the
22 First Amendment is necessary and appropriate so Microsoft may ascertain its obligations under
23 law. Absent such a declaration, the government will continue to seek, and courts will continue
24 to issue, secrecy orders that impermissibly restrict the First Amendment rights of Microsoft and
25 similarly situated providers. And although Microsoft has the right to challenge individual
26 orders (as it has done), the need for Microsoft repeatedly to expend time and effort challenging
27

1 orders issued pursuant to a constitutionally flawed statute places an impermissible burden on its
2 First Amendment rights.

3
4 **COUNT II**

5 **REQUEST FOR DECLARATORY RELIEF—**

6 **INVALIDITY OF SECTION 2705(b) UNDER THE FOURTH AMENDMENT**

7 31. ***Notice under the Fourth Amendment.*** Notice to an owner whose property is
8 being searched or seized “is an element of the reasonableness inquiry under the Fourth
9 Amendment.” *Wilson v. Arkansas*, 514 U.S. 927, 934 (1995); *see also United States v. Freitas*,
10 800 F.2d 1451, 1456 (9th Cir. 1986).

11 32. ***Failure to Provide Notice.*** A statute is facially unconstitutional under the
12 Fourth Amendment if the “applications of the statute in which it actually authorizes or prohibits
13 conduct” are unconstitutional. *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2451 (2015).
14 Section 2705(b) is facially unconstitutional because, as discussed above, it permits secrecy
15 orders that prohibit providers from telling customers when the government has accessed their
16 private information and data, without requiring constitutionally sufficient proof of the existence
17 of a compelling government interest and without temporally limiting the prohibition to the least
18 restrictive period sufficient to satisfy the government’s compelling interests. The constitutional
19 injury is exacerbated by the fact that, under 18 U.S.C. § 2703(b)(1)(A), the government need
20 not give **any** notice to a customer whose content it obtains by warrant. The interaction of these
21 provisions means the government can access a customer’s most sensitive information without
22 the customer having any way to learn about, or challenge, the government’s intrusion. This
23 result flouts fundamental Fourth Amendment principles.

24 33. ***Standards for Physical Search.*** Section 2705(b)’s Fourth Amendment
25 deficiency is underscored by comparison to the limits on the government’s authority to conduct
26 a search and seizure in the physical world. It has been established for centuries that, absent
27 exigent circumstances, law enforcement must provide contemporaneous notice when

1 conducting a search or seizure. “The common-law principle that law enforcement officers must
2 announce their presence and provide residents an opportunity to open the door is an ancient
3 one.” *Michigan v. Hudson*, 547 U.S. 586, 589 (2006). Even when exigent circumstances exist
4 and thus allow law enforcement to conduct a search before providing notice, the government
5 may delay notice only for a limited period of time. *See* 18 U.S.C. § 3103a; Fed. R. Crim. P.
6 41(f)(1)(C). As a result, if an individual or business elects to maintain its emails on premises,
7 the government could not execute a search warrant for those emails without the customer
8 learning about it and having the ability to assert any rights or privileges it may have. “[W]hen
9 law enforcement seizes property pursuant to a warrant, due process requires them to take
10 reasonable steps to give notice that the property has been taken so the owner can pursue
11 available remedies for its return.” *City of West Covina v. Perkins*, 525 U.S. 234, 240 (1999);
12 *Lavan v. City of Los Angeles*, 693 F.3d 1022, 1032 (9th Cir. 2012) (“[T]he government may not
13 take property like a thief in the night; rather, it must announce its intentions and give the
14 property owner a chance to argue against the taking.”) (internal quotation marks and citation
15 omitted).

16 34. ***Privacy in the Cloud.*** Here, Microsoft’s customers have decided to store their
17 information and data with Microsoft in the cloud rather than on computers at their own
18 premises. This technological fortuity, however, does not weaken the privacy interests at stake.
19 *See Riley*, 134 S. Ct. at 2494-95 (“The fact that technology now allows an individual to carry
20 in his hand” a cell phone that contains the “privacies of life,” including thousands of
21 photographs and records of all his communications, “does not make the information any less
22 worthy of the protection for which the Founders fought[.]”). Nevertheless, relying on Section
23 2705(b), the government seeks and executes warrants for electronic communications far more
24 frequently than it sought and executed warrants for physical documents and communications—
25 apparently because it believes it can search and seize those documents and communications
26 under a veil of secrecy. But providing less protection to information stored in the cloud than to
27 information stored in a local server or papers stored in a file cabinet would ignore the Supreme

1 Court’s admonition not to let “technology [] erode the privacy guaranteed by the Fourth
2 Amendment” and its caution to, when confronted with new technologies, “assure[] preservation
3 of that degree of privacy against government that existed when the Fourth Amendment was
4 adopted.” *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

5 35. **Standards for Standing.** When the government serves a warrant on Microsoft
6 seeking a customer’s private information and data, the Fourth Amendment rights described
7 above belong to the customer, whose “papers and effects” are the target of the government’s
8 legal process. But Microsoft has third-party standing to vindicate its customers’ Fourth
9 Amendment rights to notice, particularly when customers lack sufficient knowledge to
10 challenge government action because of the government’s tactic of operating behind a veil of
11 secrecy. *See Powers v. Ohio* 499 U.S. 400, 410–11 (1991) (permitting third-party standing
12 where: (1) the litigant has constitutional standing (i.e., the litigant has suffered an “injury in
13 fact,” giving him or her a “sufficiently concrete interest” in the outcome of the issue in
14 dispute); (2) the litigant has a “close relation to the third party”; and (3) there is some hindrance
15 to the third party’s ability to protect his or her own interests) (internal quotation marks and
16 citations omitted).

17 36. **Microsoft’s Standing.** Microsoft satisfies each element of the *Powers* test.
18 First, Microsoft has a core business interest in safeguarding its customers’ private
19 correspondence and documents. Section 2705(b)’s violation of Microsoft’s customers’ Fourth
20 Amendment rights therefore injures Microsoft by eroding the customer trust that encourages
21 individuals and businesses to migrate their technological infrastructure to Microsoft’s cloud.
22 Further, the Fourth Amendment harms caused by Section 2705(b) are themselves the subject of
23 Microsoft’s forbidden political speech, speech in which Microsoft cannot engage because of
24 secrecy orders issued pursuant to Section 2705(b); accordingly, the Fourth Amendment
25 violations caused by Section 2705(b) compound Microsoft’s First Amendment injury. Second,
26 courts recognize that providers such as Microsoft have a sufficiently close relationship with
27 their customers to allow providers to assert their customers’ constitutional rights under *Powers*.

1 See *In re Verizon Internet Servs.*, 257 F. Supp. 2d 244, 258 (D.D.C. 2003) (“Verizon’s
2 relationship with its client subscribers is the kind of relationship that warrants allowing Verizon
3 to assert a First Amendment challenge on their behalf.”), *rev’d on other grounds by Recording*
4 *Industry Ass’n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1239 (D.C. Cir.
5 2003)). Third, by design, Section 2705(b) hinders any effort by Microsoft’s customers to
6 protect their own Fourth Amendment rights.

7 37. **Judicial Declaration.** A judicial declaration that Section 2705(b) violates the
8 Fourth Amendment is necessary and appropriate so that Microsoft and the government may
9 ascertain their obligations under law. Absent such a declaration, the government will continue
10 to request and obtain secrecy orders that impermissibly restrict the Fourth Amendment rights of
11 Microsoft’s customers and the customers of other, similarly situated providers.

12 **PRAYER FOR RELIEF**

13 Microsoft prays for an Order and Judgment:

14 (a) Declaring that 18 U.S.C. § 2705(b) is facially unconstitutional under the First
15 Amendment;

16 (b) Declaring that 18 U.S.C. § 2705(b) is facially unconstitutional under the Fourth
17 Amendment;

18 and

19 (c) Granting such other and further equitable or legal relief as the Court deems
20 proper.

1 DATED this 14th day of April, 2016.

2 Davis Wright Tremaine LLP

3
4 By /s/ Stephen M. Rummage
Stephen M. Rummage, WSBA #11168

5 By /s/ Ambika K. Doran
6 Ambika K. Doran, WSBA #38237
1201 Third Avenue, Suite 2200
7 Seattle, WA 98101
Telephone: 206-757-8136
8 Fax: 206-757-7136
E-mail: steverummage@dwt.com,
9 ambikadoran@dwt.com

10 Laura Handman*
11 Davis Wright Tremaine LLP
1919 Pennsylvania Ave NW #800,
12 Washington, DC 20006
Telephone: (202) 973-4200
13 Fax: (202) 973-4429
E-mail: laurahandman@dwt.com

14 James M. Garland*
15 Alexander A. Berengaut*
16 Katharine R. Goodloe*
Covington and Burling LLP
17 One CityCenter
850 10th St., N.W.
18 Washington, DC 20001
Tel: (202) 662-6000
19 Fax: (202) 662-6291
Email: jgarland@cov.com,
20 aberengaut@cov.com, kgoodloe@cov.com

21 Bradford L. Smith
22 David M. Howard
Jonathan Palmer
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

23 *pro hac vice application to be filed

24 Attorneys for Microsoft Corporation