The Honorable James L. Robart

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

Microsoft Corporation,

Plaintiff,

v.

The United States Department of Justice, and Loretta Lynch, in her official capacity as Attorney General of the United States,

Defendants.

No. 2:16-cv-00538-JLR

FIRST AMENDED 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 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

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

government increasingly seeks (and obtains) secrecy orders under Section 2705(b). This statute violates both the Fourth Amendment, which affords people and businesses the right to know if the government searches or seizes their property, and the First Amendment, which enshrines Microsoft's rights to talk to its customers and to discuss how the government conducts its investigations—subject only to restraints narrowly tailored to serve compelling government interests. People do not give up their rights when they move their private information from physical storage to the cloud. Microsoft therefore asks the Court to declare that Section 2705(b) is unconstitutional, both on its face and as applied to Microsoft and its customers. Microsoft also asks the Court to declare that 18 U.S.C. § 2703 is unconstitutional, both on its face and as applied, to the extent it permits the government to conduct warranted searches and seizures without notice to the target of the warrant.

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

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

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

4. The government, however, has exploited the transition to cloud computing as a means of expanding its power to conduct secret investigations. As individuals and businesses have moved their most sensitive information to the cloud, the government has increasingly adopted the tactic of obtaining the private digital documents of cloud customers not from the customers themselves, but through legal process directed at online cloud providers like Microsoft. At the same time, the government seeks secrecy orders under 18 U.S.C. § 2705(b) to prevent Microsoft from telling its customers (or anyone else) of the government's demands. These secrecy orders generally assert that abiding by the centuries-old requirement of seeking evidence directly from its owner would jeopardize the government's investigation. Most of the time, these secrecy orders prohibit notification for unreasonably long (or even unlimited) periods of time, which Section 2705(b) permits whenever a court has "reason to believe" any of several adverse consequences might otherwise ensue—including any time notice would "seriously jeopardiz[e] an investigation or unduly delay[] a trial"—without requiring any case-specific showing to support the belief.

5. Over a 20-month period ending in May 2016, federal courts issued more than 3,250 secrecy orders silencing Microsoft from speaking about the government's legal demands for Microsoft customers' data; of those secrecy orders, nearly two-thirds contained no fixed end date. Further, more than 650 of those secrecy orders accompanied search warrants, and roughly 70 percent of those orders were of indefinite duration. (In fact, the dozens of secrecy orders issued to Microsoft in this District almost without exception contain no time limit.) These twin developments—the increase in government demands for online data and the simultaneous increase in secrecy—have combined to undermine confidence in the privacy of the cloud and have impaired Microsoft's right to be transparent with its customers, a right guaranteed by the First Amendment.

6. There may be exceptional circumstances when the government's interest in investigating criminal conduct justifies an order temporarily barring a provider from notifying a customer that the government has obtained the customer's private communications and data.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

But Section 2705(b) sweeps too broadly. That antiquated law (passed decades before cloud computing existed) allows courts to impose prior restraints on speech about government conduct—the very core of expressive activity the First Amendment is intended to protect—even if other approaches could achieve the government's objectives without burdening the right to speak freely. The statute sets no limits on the duration of secrecy orders, and it permits prior restraints any time a court has "reason to believe" adverse consequences would occur if the government were not allowed to operate in secret. Under the statute, the assessment of adverse consequences need not be based on the specific facts of the investigation, and the assessment is made ***only*** at the time the government applies for the secrecy order, with no obligation on the government to later justify continued restraints on speech even if circumstances change because, for instance, the investigation is closed or the subject learns of it by other means. It also permits those restraints based on the application of purely subjective criteria, such as a finding that notice would "jeopardiz[e] an investigation" in unspecified ways or "unduly delay a trial." Section 2705(b) is therefore facially overbroad under the First Amendment, since it does not require the government to establish that the continuing restraint on speech is narrowly tailored to promote a compelling interest applicable to the specific secrecy order**.** Further, because Microsoft has been subjected to non-disclosure orders entered pursuant to Section 2705(b) without adherence to the requisite constitutional standards, Section 2705(b) is also unconstitutional under the First Amendment as applied to Microsoft.

7. Further, ECPA violates the Constitution's protection against unreasonable searches and seizures. The Fourth Amendment's requirement that government engage only in "reasonable" searches necessarily includes a right for people to know when the government searches or seizes their property. *See Wilson v. Arkansa*s, 514 U.S. 927, 934 (1995). For example, if the government comes into a person's home to seize her letters from a desk drawer or computer hard drive, that person in almost all circumstances has the right to notice of the government's intrusion. The same is true when the government executes a search of a business to seize emails from the business's on-site server. But 18 U.S.C. § 2703 combines with Section

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

2705(b) to subject Microsoft's cloud customers to a different standard merely because of how they store their communications and data: Section 2703 allows the government to search and seize customers' private information without providing any notice to the customer, while Section 2705(b) permits the government to obtain an order gagging the cloud services provider based upon a constitutionally insufficient showing. Section 2703, to the extent it authorizes warranted searches and seizures without notice to the warrant's target, and Section 2705(b) together fall short of the intended reach of Fourth Amendment protections, which do not depend on the technological medium in which private "papers and effects" are stored.

8. For these reasons, Microsoft asks the Court to declare that Section 2703, to the extent it permits the government to conduct warranted searches and seizures without notice to the target, and Section 2705(b) are unconstitutional on their face and as applied.

PARTIES

9. ***Microsoft.*** Microsoft is a corporation organized and existing under the laws of the State of Washington, with its principal place of business at One Microsoft Way, Redmond, Washington 98052. Microsoft has standing to bring this action because of the repeated invasion of its First Amendment rights through the issuance of indefinite and insufficiently substantiated secrecy orders, its interest in upholding its public commitment to safeguard the privacy of its customers' sensitive emails and documents without violating court orders, its right to invoke the Fourth Amendment rights of its customers (who have no practical means of protecting those rights), and its interest in avoiding findings of contempt.

10. ***The United States Department of Justice.*** The United States Department of Justice is an agency of the executive branch of the federal government, employees of which regularly apply for secrecy orders under 18 U.S.C. § 2705(b), serve those secrecy orders on providers, including Microsoft, and obtain the contents of electronic communications without notice to affected Microsoft customers under 18 U.S.C. § 2703.

11. ***Loretta Lynch***. Loretta Lynch, sued in her official capacity only, is the Attorney General of the United States. Attorney General Lynch has ultimate authority over the United

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

States Department of Justice, employees of which regularly apply for secrecy orders under 18 U.S.C. § 2705(b), serve those secrecy orders on providers, including Microsoft, and obtain the contents of electronic communications without notice to affected Microsoft customers under 18 U.S.C. § 2703.

JURISDICTION AND VENUE

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

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

MICROSOFT'S CLOUD SERVICES

14. ***Cloud Computing.*** As they migrate their communications and documents to the cloud, individuals and businesses have increasingly entrusted Microsoft and other providers with their most private information—what the Supreme Court has referred to as a "cache of sensitive personal information." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). A customer that stored paper documents in file cabinets or emails on on-site servers would generally know contemporaneously about the execution of a warrant by law enforcement—and would be able to assert any rights concerning any documents or data seized during the search. A customer storing documents and emails remotely in the cloud should be in the same position. That is, cloud customers should be able to trust they will know if they become the targets of warrants or other legal process authorizing the seizure of sensitive information.

15. ***Secrecy Orders.*** Secrecy orders issued under Section 2705(b) combine with the government's ability to obtain electronic communications and data without notice to the target under Section 2703 to give the government a double-barreled weapon, allowing it to seek electronic communications and other private data under a veil of prolonged (or even indefinite)

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

secrecy. The government's use of legal process directed at cloud providers such as Microsoft, when combined with accompanying secrecy orders, amounts to a substantial expansion of law enforcement's ability to engage in secret search and seizure activity, adversely affecting both Microsoft's right to communicate with its customers and the customers' privacy interests—simply because customers have moved their information to the cloud.

16. ***The Frequency of Secrecy Orders.*** Between September 2014 and May 2016, Microsoft received more than 6,000 federal demands for customer information or data. Of those demands, more than 3,250 were accompanied by secrecy orders (including more than 650 secrecy orders served with search warrants), forbidding Microsoft from telling the affected customers that the government was looking at their information. The vast majority of these secrecy orders related to consumer accounts and prevent Microsoft from telling affected individuals about the government's intrusion into their personal affairs; others prevent Microsoft from telling business customers that the government has searched and seized the emails of individual employees of the customer. Further, more than 2,000 of these federal secrecy orders (including more than 450 secrecy orders accompanying search warrants) contained no time limit, meaning that Microsoft could ***forever*** be barred from telling the affected customer about the government's intrusion. The government has used this tactic in this District. Since September 2014, Microsoft received at least 63 secrecy orders issued in this District pursuant to Section 2705(b), which almost without exception contained no time limit. These secrecy orders prohibit Microsoft from speaking about the government's specific demands to ***anyone*** and forbid Microsoft from ever telling its customers whose documents and communications the government has obtained. The secrecy orders thus prevent Microsoft's customers and the public at large from ever learning the full extent of government access to private, online information.

STATUTORY OVERVIEW

17. ***Section 2703***. Congress enacted Section 2703 as part of the Electronic Communications Privacy Act of 1986 ("ECPA"). Section 2703 authorizes the government to

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

obtain the contents of electronic communications pursuant to a warrant without the government providing notice to the person whose communications are being seized and searched.

18. ***Section 2705(b).*** Congress also enacted Section 2705(b) as part of ECPA. Section 2705(b) provides, in its entirety:

> **(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—**A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—
>
> (1) endangering the life or physical safety of an individual;
>
> (2) flight from prosecution;
>
> (3) destruction of or tampering with evidence;
>
> (4) intimidation of potential witnesses; or
>
> (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

19. ***Effect of Statute.*** Microsoft is a "provider of electronic communications service or remote computing service" as those terms are used in ECPA. Under the plain terms of Section 2705(b), a court therefore may order Microsoft "not to notify ***any other person*** of the existence" of a legal demand for its customer's emails and documents. A court may issue such an order "for such period as the court deems appropriate," without any requirement that the government advise the court of any change in circumstances bearing upon the government's initial asserted need for nondisclosure. Thus, for example, a secrecy order may prevent Microsoft from informing a customer of the intrusion even after the government's investigation ends or becomes public through other means. And under Section 2703, the government itself

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

has no obligation to provide notice when it seizes and searches the contents of electronic communications pursuant to a warrant.

20. ***Grounds for Secrecy Order under Section 2705(b).*** Section 2705(b) does not require a court to consider whether a secrecy order is narrowly tailored to further the government's asserted interests in a particular case and whether there are less restrictive alternatives in that case. Indeed, the statute contemplates that the court "shall enter such an order" without weighing whether less restrictive alternatives are available. Further, Section 2705(b) allows the court to issue a secrecy order whenever it finds "reason to believe" that any of five adverse results would otherwise occur, including when notification "will result in … otherwise seriously jeopardizing an investigation or unduly delaying a trial." Nothing in Section 2705(b) requires a court to base its finding of a "reason to believe" on a showing of specific facts applicable to the particular request for secrecy.

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

22. ***Searches in the Physical World.*** By allowing the government to operate behind a veil of secrecy, Sections 2703 and 2705(b) also differ from similar forms of process in the

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

physical world. For example, although 18 U.S.C. § 3103a authorizes so-called "sneak and peek" warrants for secret searches—the only permissible means of executing search warrants of physical documents without notice—that provision presumptively requires the government to notify the target of the search "within a reasonable period not to exceed 30 days after the date of its execution." 18 U.S.C. § 3103a(b)(3). The statute permits extensions of this deferred notice, but "subject to the condition that extensions should only be granted upon an updated showing of the need for further delay and that each additional delay should be limited to periods of 90 days or less." 18 U.S.C. § 3103a(c). While these provisions permit delays of longer than 30 and 90 days "if the facts of the case justify a longer period of delay," the statute imposes temporal baselines lacking in Sections 2703 and 2705(b).

COUNT I

REQUEST FOR DECLARATORY RELIEF –

INVALIDITY OF SECTION 2705(b) UNDER THE FIRST AMENDMENT

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

24. ***Presumptive Invalidity of Prior Restraints.*** A secrecy order "imposes a prior restraint on speech." *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 882 (S.D. Tex. 2008) ("*In re Sealing*"). Any prior restraint "bear[s] a heavy presumption against its constitutional validity," and the government has a "heavy burden of showing justification for the imposition of such a restraint." *Capital Cities Media, Inc. v. Toole*, 463 U.S. 1303, 1305 (1983). Thus, because Section 2705 on its face authorizes the issuance of secrecy orders that operate as a prior restraint on Microsoft's speech, the

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

government's burden of justifying the restraint is particularly heavy. The statute authorizes secrecy orders that prohibit, *ex ante*, providers such as Microsoft from engaging in core protected speech under the First Amendment, i.e., speech about the government's access to customers' sensitive communications and documents and its increased surveillance on the Internet. "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." *Mills v. Alabama*, 384 U.S. 214, 218 (1971).

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

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

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

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

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

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

statute indefinitely banning witnesses from disclosing testimony given before a grand jury violates the First Amendment).

29. ***"Reason to Believe."*** Second, Section 2705(b) is unconstitutionally overbroad because it permits a court to issue a secrecy order whenever it has "reason to believe" notification would result in one of five listed adverse results. But the statute does not require that the "reason to believe" be grounded in the specific facts of the particular investigation, as distinct from the government's overall experiences or other unspecified considerations. Further, the statute offers no guidance as to the evidentiary burden the government bears in showing a "reason to believe" sufficient to justify a secrecy order. And the "reason to believe" standard fails to require that a secrecy order be the least restrictive means available to further the government's interest in avoiding the specified adverse results in the particular case, as the First Amendment requires to justify this sort of restraint. The "reason to believe" standard therefore falls far short of the "heavy burden" the First Amendment imposes when the government seeks to impose a prior restraint on speech.

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

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

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

32. ***Invalidity as Applied to Microsoft.*** For the same reasons that Section 2705(b) is facially invalid, it is also unconstitutional as applied to Microsoft. Of the federal secrecy orders issued to Microsoft in the 20-month period ending in May 2016, more than 2,000 (including more than 450 secrecy orders accompanying search warrants) were indefinite, and all were issued under the deficient "reason to believe" standard, without any statutory requirement for case-specific factual showings. Further, it appears a substantial number of the orders may have relied on the unconstitutionally vague catchall provision to justify the restraint on speech. Almost without exception, the secrecy orders issued in this District pursuant to Section 2705(b) likewise were indefinite in duration, and all were issued pursuant to the defective "reason to believe" standard, without any statutory requirement for a case-specific evidentiary showing, and are therefore constitutionally deficient under these standards.

33. ***Judicial Declaration.*** A judicial declaration that Section 2705(b) violates the First Amendment is necessary and appropriate so Microsoft may ascertain its obligations under law. Absent such a declaration, the government will continue to seek, and courts will continue to issue, secrecy orders that impermissibly restrict the First Amendment rights of Microsoft and similarly situated providers. And although Microsoft has the right to challenge individual orders (as it has done), the need for Microsoft repeatedly to expend time and effort challenging orders issued pursuant to a constitutionally flawed statute places an impermissible burden on its First Amendment rights.

COUNT II

REQUEST FOR DECLARATORY RELIEF—

INVALIDITY OF SECTIONS 2703 AND 2705(b) UNDER FOURTH AMENDMENT

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

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

35. ***Failure to Provide Notice.*** A statute is facially unconstitutional under the Fourth Amendment if the "applications of the statute in which it actually authorizes or prohibits conduct" are unconstitutional. *City of Los Angeles v. Patel*, 135 S. Ct. 2443, 2451 (2015). Section 2703 is facially unconstitutional to the extent it absolves the government of the obligation to give notice to a customer whose content it obtains by warrant, without regard to the circumstances of the particular case. Section 2705(b) exacerbates the constitutional injury because, as discussed above, it permits secrecy orders that prohibit providers from telling customers when the government has accessed their private information and data, without requiring constitutionally sufficient proof of the existence of a compelling government interest and without temporally limiting the prohibition to the least restrictive period sufficient to satisfy the government's compelling interests. The interaction of these provisions means the government can access a customer's most sensitive information without the customer having any way to learn about, or challenge, the government's intrusion. This result flouts fundamental Fourth Amendment principles.

36. ***Standards for Physical Search.*** Sections 2703 and 2705(b)'s Fourth Amendment deficiencies are underscored by comparison to the limits on the government's authority to conduct a search and seizure in the physical world. It has been established for centuries that, absent exigent circumstances, law enforcement must provide contemporaneous notice when conducting a search or seizure. "The common-law principle that law enforcement officers must announce their presence and provide residents an opportunity to open the door is an ancient one." *Michigan v. Hudson*, 547 U.S. 586, 589 (2006). Even when exigent circumstances exist and thus allow law enforcement to conduct a search before providing notice, the government may delay notice only for a limited period of time. *See* 18 U.S.C. § 3103a; Fed. R. Crim. P. 41(f)(1)(C). As a result, if an individual or business elects to maintain its emails on premises, the government could not execute a search warrant for those emails without the customer learning about it and having the ability to assert any rights or privileges it may have. "[W]hen law enforcement agents seize property pursuant to a warrant, due process

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

requires them to take reasonable steps to give notice that the property has been taken so the owner can pursue available remedies for its return." *City of West Covina v. Perkins*, 525 U.S. 234, 240 (1999). "[T]he government may not take property like a thief in the night; rather, it must announce its intentions and give the property owner a chance to argue against the taking." *Lavan v. City of Los Angeles*, 693 F.3d 1022, 1032 (9th Cir. 2012) (internal quotation marks and citation omitted).

37. ***Privacy in the Cloud.*** Here, Microsoft's customers have decided to store their information and data with Microsoft in the cloud rather than on computers at their own premises. This technological fortuity, however, does not weaken the privacy interests at stake. *See Riley*, 134 S. Ct. at 2494-95 ("The fact that technology now allows an individual to carry ... in his hand" a cell phone containing the "privacies of life," including thousands of photographs and records of all his communications, "does not make the information any less worthy of the protection for which the Founders fought[.]") (internal quotation marks and citation omitted). Nevertheless, relying on Sections 2703 and 2705(b), the government seeks and executes warrants for electronic communications far more frequently than it sought and executed warrants for physical documents and communications—apparently because it believes it can search and seize those documents and communications under a veil of secrecy. But providing less protection to information stored in the cloud than to information stored in a local server or papers stored in a file cabinet would ignore the Supreme Court's admonition not to let "technology ... erode the privacy guaranteed by the Fourth Amendment" and its caution to, when confronted with new technologies, "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

38. ***Standards for Standing.*** When the government serves a warrant on Microsoft seeking a customer's private information and data, the Fourth Amendment rights described above belong to the customer, whose "papers and effects" are the target of the government's legal process. But Microsoft has third-party standing to vindicate its customers' Fourth

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

Amendment rights to notice, particularly when customers lack sufficient knowledge to challenge government action because of the government's tactic of operating behind a veil of secrecy. *See Powers v. Ohio* 499 U.S. 400, 410–11 (1991) (permitting third-party standing where: (1) the litigant has "suffered an injury in fact, thus giving him or her a sufficiently concrete interest in the outcome of the issue in dispute"; (2) the litigant has a "close relation to the third party"; and (3) there is "some hindrance to the third party's ability to protect his or her own interests") (internal quotation marks and citations omitted).

39. ***Microsoft's Standing.*** Microsoft satisfies each element of the *Powers* test. First, Microsoft has a core business interest in safeguarding its customers' private correspondence and documents. Sections 2703 and 2705(b)'s violation of Microsoft's customers' Fourth Amendment rights therefore injures Microsoft by eroding the customer trust that encourages individuals and businesses to migrate their technological infrastructure to Microsoft's cloud. Further, the Fourth Amendment harms caused by Sections 2703 and 2705(b) are themselves the subject of Microsoft's forbidden political speech, speech in which Microsoft cannot engage because of secrecy orders issued pursuant to Section 2705(b); accordingly, the Fourth Amendment violations caused by Sections 2703 and 2705(b) compound Microsoft's First Amendment injury. Second, courts recognize that providers such as Microsoft have a sufficiently close relationship with their customers to allow providers to assert their customers' constitutional rights under *Powers*. *See In re Verizon Internet Servs.*, 257 F. Supp. 2d 244, 258 (D.D.C. 2003) ("Verizon's relationship with its client subscribers is the kind of relationship that warrants allowing Verizon to assert a First Amendment challenge on their behalf."), *rev'd on other grounds by Recording Industry Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1239 (D.C. Cir. 2003)). Third, by design, Sections 2703 and 2705(b) combine to thwart any effort by Microsoft's customers to protect their own Fourth Amendment rights.

40. ***Invalidity as Applied***. For the same reasons that Sections 2703 and 2705(b) on their face violate the Fourth Amendment, they are also unconstitutional as applied to Microsoft

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

and its customers. The absence of a government notice obligation, combined with the imposition of secrecy orders on Microsoft, has resulted, and will continue to result, in an unconstitutional delay of notice to Microsoft's customers, in violation of their Fourth Amendment rights.

41. ***Judicial Declaration.*** A judicial declaration that Sections 2703 and 2705(b) violate the Fourth Amendment is necessary and appropriate so that Microsoft and the government may ascertain their obligations under law. Absent such a declaration, the government will continue to request and obtain secrecy orders that impermissibly restrict the Fourth Amendment rights of Microsoft's customers and the customers of other, similarly situated providers.

PRAYER FOR RELIEF

Microsoft prays for an Order and Judgment:

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

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

(c) Declaring that 18 U.S.C. § 2703 is unconstitutional under the Fourth Amendment, at least to the extent it permits warranted searches and seizures without the government providing notice to the person whose communications are being searched and seized;

and

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

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

DATED this 17th day of June, 2016.

Davis Wright Tremaine LLP

By /s/ *Stephen M. Rummage*
Stephen M. Rummage, WSBA #11168
Ambika K. Doran, WSBA #38237
1201 Third Avenue, Suite 2200
Seattle, WA 98101
Telephone: 206-757-8136
Fax: 206-757-7136
E-mail: steverummage@dwt.com,
ambikadoran@dwt.com

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

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

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

*Admitted *pro hac vice*

Attorneys for Microsoft Corporation

CERTIFICATE OF SERVICE

I hereby certify that on June 17, 2016, I electronically filed the foregoing *First Amended Complaint for Declaratory Judgment* 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. I further hereby certify that I have mailed by United States Postal Service the document to the following non CM/ECF participant:

Stephen P. Wallace
1116 Sheffer Road – Apt. F
Aurora, IL 60505

DATED this 17th day of June, 2016.

Davis Wright Tremaine LLP
Attorneys for HAL Defendants

By *s/ Stephen M. Rummage*
Stephen M. Rummage, WSBA #11168
1201 Third Avenue, Suite 2200
Seattle, Washington 98101-3045
Telephone: (206) 622-3150
Fax: (206) 757-7700
E-mail: steverummage@dwt.com