THE HONORABLE JAMES L. ROBART

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

Microsoft Corporation,

Plaintiff,

v.

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

Defendants.

American Civil Liberties Union and American Civil Liberties Union Foundation,

Plaintiffs–Intervenors,

v.

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

Defendants in Intervention.

No. 2:16-cv-00538-JLR

OPPOSITION TO MOTION TO DISMISS

NOTE ON MOTION CALENDAR:
September 23, 2016

Oral Argument Requested

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

TABLE OF CONTENTS

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

TABLE OF AUTHORITIES

Cases

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

Statutes

Other Authorities

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

The American Civil Liberties Union and the American Civil Liberties Union Foundation (together, the "ACLU" or "Intervenors") are customers of Microsoft who have moved to intervene in this action to defend their Fourth Amendment right to notice from the government if and when the government acquires their constitutionally protected information from Microsoft. The ACLU moved to intervene in this lawsuit on May 26, 2016. ECF No. 13. That motion is pending, so the ACLU now files this opposition to the government's motion to dismiss to ensure its participation in the dispositive briefing of the Fourth Amendment questions common to its and Microsoft's complaints. As explained in an earlier belief, the ACLU respectfully urges that the proper course is to resolve the motion to intervene prior to consideration of the motion to dismiss, "to allow all interested parties to present their arguments in a single case at the same time." *100Reporters LLC v. DOJ*, 307 F.R.D. 269, 286–87 (D.D.C. 2014); *see* ACLU Intervention Reply 2.[1]

INTRODUCTION

This case presents the question whether the government may search and seize individuals' constitutionally protected communications without ever telling them that it has done so. The government argues that it need not notify anyone other than Microsoft when it executes a warrant for the emails of one of Microsoft's customers. But the government's rule makes no constitutional sense. The Fourth Amendment entitlement to notice travels with the right to privacy. In other words, when the government intrudes upon an individual's protected privacy interests, it owes *that individual* notice. Both the Ninth Circuit and the Supreme Court have recognized that commonsense principle multiple times. The government's obligation to provide notice is inherent in the warrant requirement, whose founding purpose was to constrain government power by ensuring that individuals whose privacy had been invaded learned of and could challenge the lawfulness of the invasion. The notice requirement has also been a

[1] Should this Court deny its motion to intervene, the ACLU respectfully requests leave to file this brief as *amicus curiae*.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

cornerstone of the Supreme Court's case law assessing the constitutional reasonableness of surreptitious surveillance. And the requirement is just one manifestation of the bedrock command of due process that the government accompany every deprivation of liberty or property with notice.

The government's principal defense of its failure to provide notice to Microsoft's customers relies on an anachronism. Historically, the Fourth Amendment protected property interests, and the traditional manner of providing notice reflects that fact. Leaving a copy of the warrant and an inventory of property seized at the physical location of the invasion satisfied the government's constitutional obligation to provide notice. But as Americans began to rely on third parties to route their sensitive communications, the government acquired the ability to search or seize without physical trespass, raising the specter of widespread invasions of privacy without notice to those directly affected. The Supreme Court responded by ensuring that the right to notice kept pace with evolving technologies. It invalidated an electronic surveillance statute that did not require notice to the government's targets, *see Berger v. New York*, 388 U.S. 41, 60 (1967), and it sustained one that did, *see United States v. Donovan*, 429 U.S. 413, 429 n.19 (1977). In the process, the Court made clear that the individual searched is the one entitled to notice.

The government attempts to insulate its refusal to provide notice from judicial review, arguing that neither Microsoft nor the ACLU has standing to raise these important constitutional questions. By the government's logic, Microsoft does not *ever* have standing to defend its customers' right to notice, and Microsoft's customers, including the ACLU, may not defend their own right to notice until *after* they receive the primary relief they would seek—that is, notice. In the government's view, the only plaintiffs who have standing to sue for notice are those who have already gotten it, and those deprived of notice forever have no ability to seek a remedy at all. That is not the law. Microsoft has third-party standing to assert the Fourth Amendment rights of its customers because of its close relationship to them and, most importantly, because under

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

ECPA, Microsoft's customers cannot protect their own interests—as the government itself has underscored in its opposition to the ACLU's motion to intervene.

For these reasons and those elaborated below, the government's failure to notify Microsoft's customers of the search or seizure of their communications violates the Fourth Amendment, and Microsoft has third-party standing to defend its customers' right to notice. The Court should therefore deny the government's motion to dismiss Microsoft's Fourth Amendment claims.

BACKGROUND

The Electronic Communications Privacy Act ("ECPA") permits the government to compel service providers to disclose "the contents of a wire or electronic communication," 18 U.S.C. § 2703, in three ways: (1) using a warrant issued under the Federal Rules of Criminal Procedure, 18 U.S.C. § 2703(a), (b)(1)(A); (2) using an administrative, grand-jury, or trial subpoena, *id.* § 2703(b)(1)(B)(i); or (3) using a so-called "2703(d) order" issued by a court under a subpoena-like standard, *id.* § 2703(d).

Under ECPA, the government's statutory obligation to provide notice to those whose communications it acquires turns on the particular authority the government relies on to compel disclosure. If the government relies on a subpoena or 2703(d) order, it must provide "prior notice" to the subscriber or customer, although it may delay that notification for renewable 90-day periods upon a judicial finding of exigency. *Id.* § 2705(a). If the government obtains a warrant, however, it may compel disclosure "without required notice to the subscriber or customer," *id.* § 2703(b)(1)(A), even when there is no exigency justifying secrecy. ECPA also permits the government to apply for a court order prohibiting a service provider from notifying anyone of the existence of the disclosure order that the provider has received. *Id.* § 2705(b). In some cases, these "gag orders" last indefinitely.

Today, the government ordinarily uses a warrant when it seeks individuals' electronic communications from third-party service providers. *See* Intervenors' Compl. ¶ 20, ECF No. 13-

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

1; Gov't MTD Br. 4 n.3. ECPA does not require the government to provide notice when it relies on a warrant, and so the government now routinely searches and seizes individuals' electronic communications without providing any notice—delayed or otherwise—to those whose private information it has obtained. Compl. ¶ 21. According to Microsoft's Complaint, nearly half of the federal demands it has received under ECPA in the last eighteen months were accompanied by gag orders, the majority of which contained no time limit. Microsoft Am. Compl. ¶ 16, ECF No. 28. Accordingly, a substantial portion of the individuals whose electronic communications the government demands from Microsoft receive no notice whatsoever, from either the government or Microsoft.

In this lawsuit, Microsoft challenges the constitutionality of the ECPA, arguing that 18 U.S.C. § 2705(b) restricts Microsoft's speech in violation of the First Amendment and that sections 2705(b) and 2703 violate the Fourth Amendment rights of Microsoft's customers to receive notice of the search and seizure of their communications. On May 26, 2016, the ACLU moved for leave to intervene, as a customer of Microsoft, to protect its Fourth Amendment right to receive notice from the government of the search and seizure of its communications. The ACLU's motion is still pending. The government has now filed a motion to dismiss Microsoft's claims, but it has not addressed the ACLU's proposed complaint. The ACLU files this opposition, however, to ensure its participation in dispositive briefing of the Fourth Amendment questions common to its and Microsoft's complaints.

LEGAL STANDARD

The ACLU agrees with Microsoft's articulation of the legal standard that applies to the government's motion to dismiss.

ARGUMENT

The Court should deny the government's motion to dismiss Microsoft's Fourth Amendment claims (and, by implication, the ACLU's complementary claims) because the government's failure to provide notice to Microsoft's customers of the search or seizure of their

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

communications violates the Fourth Amendment and because Microsoft has third-party standing to assert that claim.

I. The government's failure to provide notice to those whose private communications it obtains under ECPA violates the Fourth Amendment.

The Fourth Amendment requires the government to provide notice to those whose privacy interests it invades. The ACLU is a customer of Microsoft and has a reasonable expectation of privacy in the contents of its communications stored on Microsoft's servers. The ACLU is therefore entitled, as are all of Microsoft's customers, to government notice of any search or seizure of its communications. The government's failure to provide such notice violates the Fourth Amendment, as does ECPA to the extent it authorizes that practice.

A. The Fourth Amendment requires notice.

The Supreme Court and the Ninth Circuit have long recognized that the Fourth Amendment requires notice. Notice is central to the purpose of the warrant requirement, and it is essential to the Fourth Amendment reasonableness of any surreptitious surveillance authority.

In *United States v. Freitas*, the Ninth Circuit held that notice is a presumptive Fourth Amendment requirement. 800 F.2d 1451 (9th Cir. 1986). There, the court considered the constitutionality of a surreptitious search of a home based on a warrant that failed to provide for any notice whatsoever. The court explained that while "the Fourth Amendment does not prohibit all surreptitious entries," the "absence of any notice requirement in the warrant casts strong doubt on its constitutional adequacy." *Id.* at 1456. "[R]esolv[ing] those doubts," the court held that the warrant at issue "was constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry." *Id.* The court based its holding on the line of Supreme Court cases discussed below and on the commonsense observation that "surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment." *Id.*[2]

[2] Although *Freitas* appears to be the Ninth Circuit's clearest articulation of the right to notice, the court recognized the right as early as 1974. *See United States v. Chun*, 503 F.2d 533, 536 (9th

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

The Supreme Court has also, time and again, recognized the constitutional necessity of notice. In *Berger v. New York*, 388 U.S. 41, 60 (1967), the Supreme Court struck down a New York eavesdropping statute, in part because "the statute's procedure . . . has no requirement for notice as do conventional warrants." A few months later, in *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court invalidated the practice of warrantless wiretapping and, in the process, again discussed the requirement of notice. In setting out a framework for Congress to consider in crafting a constitutional wiretapping scheme, *see id.* at 354–56, the Court suggested that even if wiretapping targets were not constitutionally entitled to *advance* notice (as a "conventional warrant" ordinarily provides), the government could not dispense with notice altogether. *See id.* at 355 n.16 ("In omitting any requirement of advance notice, the federal court that authorized electronic surveillance in *Osborn* simply recognized, as has this Court, that officers need not announce their purpose before conducting an otherwise authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence.").

A year after *Katz*, Congress enacted Title III, the still-operative federal wiretapping law, which obligates the government to provide notice to wiretap targets, subject to court-authorized delay. 18 U.S.C. § 2518(8)(d). In two cases addressing Title III, the Supreme Court has made even clearer what it said in *Berger* and *Katz*. First, in *United States v. Donovan*, 429 U.S. 413 (1977), the Court considered the proper statutory construction of Title III's delayed-notice provision but also briefly addressed its constitutionality. It approvingly quoted Congress's summary of *Berger* and *Katz*: "The *Berger* and *Katz* decisions established that notice of surveillance is a constitutional requirement of any surveillance statute." *Donovan*, 429 U.S. at 430 (quoting 114 Cong. Rec. 14485–86 (1968)). And in a footnote citing those same decisions,

---

Cir. 1974) ("In *Berger v. New York*, 388 U.S. 41, 87 S. Ct. 1873, 18 L. Ed. 2d 1040 (1967), the Supreme Court enunciated certain constitutional standards which a valid wiretapping statute must contain. Among those standards were notice procedures and procedures for a return on the warrant."); *see also United States v. Donovan*, 429 U.S. 413, 431 (1977) (expressly agreeing with *Chun*'s analysis of the related question of Title III notice to non-targets).

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

the Supreme Court held that Title III's "notice and return provisions satisfy constitutional requirements." *Id.* at 429 n.19. Two years later, in *Dalia v. United States*, 441 U.S. 238 (1979), the Court considered the constitutionality of surreptitious entry for the purpose of installing a surveillance device. Even as the Court dismissed the argument that the Fourth Amendment prohibits all surreptitious entries, it reaffirmed its holding in *Donovan* "that Title III provided a *constitutionally adequate* substitute for advance notice by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance." *Dalia*, 441 U.S. at 248 (emphasis added) (citing *Donovan*, 429 U.S. at 429 n.19). The Court held that "[t]here is no reason why the same notice [as approved in *Donovan*] is not equally sufficient with respect to electronic surveillances requiring covert entry." *Id.*

In short, the Supreme Court and the Ninth Circuit have held that the Fourth Amendment requires notice. The Supreme Court has invalidated a scheme lacking notice, affirmed a scheme requiring it, and permitted postponement, but never the wholesale elimination, of notice. The Ninth Circuit has followed suit in holding that notice is a presumptive constitutional requirement.

The government argues that the notice obligation recognized by the Ninth Circuit in *Freitas* applies only to physical searches of the home. Gov't MTD Br. 23. But that argument ignores more recent Ninth Circuit precedent extending *Freitas* to a remote storage unit. *See United States v. Johns*, 851 F.2d 1131 (9th Cir. 1988). And even setting *Johns* aside, the government's argument cannot be squared with the logic of *Freitas* itself, which based its holding on *Berger*—a case involving eavesdropping on conversations in offices, not homes. *Freitas*, 800 F.2d at 1456; *see Berger*, 388 U.S. at 45. Nor can it be squared with *Katz* or *Donovan*, which recognized the right to notice in the context of electronic surveillance, and which did not involve physical searches of the home. *See Katz*, 389 U.S. at 348 (listening device attached to exterior of a public telephone booth); *Donovan*, 429 U.S. at 417 (wiretapping of several phones). Moreover, as *Berger* expressly recognized, the protections of the notice requirement are even "more important" in the context of eavesdropping—not less, as the government suggests—because of the "inherent dangers" associated with surreptitious spying.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

See Berger, 388 U.S. at 60 ("Such a showing of exigency, in order to avoid notice would appear more important in eavesdropping, with its inherent dangers, than that required when conventional procedures of search and seizure are utilized."); *id.* at 63 ("Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."). More recently, the Supreme Court and the Ninth Circuit have similarly recognized that electronic invasions can be every bit as intrusive as searches of the home—and even more so. As the Ninth Circuit reiterated only a few weeks ago, "[p]ersonal email can, and often does, contain all the information once found in the 'papers and effects' mentioned explicitly in the Fourth Amendment." *In re Grand Jury Subpoena*, No. 15-35434, 2016 WL 3745541, at *5 (9th Cir. July 13, 2016); *accord Riley v. California*, 134 S. Ct. 2473, 2491 (2014) ("Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house.").

Underlying these cases is the basic notion that with the power to search and seize comes the duty to notify. By affording those searched an opportunity to respond, notice fulfills the warrant requirement's basic aim of ensuring that the government's searches are both lawfully authorized and lawfully executed.[3] Contrary to the government's claim, Gov't MTD Br. 22, courts have long recognized that the one-sided process that accompanies the issuance of a warrant cannot, on its own, protect against error and overreach.[4] Notice ensures that targets of government surveillance may challenge the basis of the government's search or seizure of their papers and effects, that they may seek compensation for unjustified invasions, and that they may seek the return of property or information unlawfully held. *See, e.g.*, S. Rep. 90-1097, 1968 U.S.C.C.A.N. 2112, 2194 (Pursuant to Title III's notice requirement, "all authorized

[3] Notice conveys at least four basic facts about a search: (1) it tells the aggrieved person that a search has occurred; (2) it describes what the government was authorized to take; (3) it identifies what was actually taken; and (4) it identifies the legal authority the government relied upon.

[4] *See, e.g.*, *Franks v. Delaware*, 438 U.S. 154, 169 (1978) ("[T]he hearing before the magistrate not always will suffice to discourage lawless or reckless misconduct."); *Malley v. Briggs*, 475 U.S. 335, 338–39 (1986) (permitting damages suit against officers where arrest warrant and supporting affidavit allegedly failed to establish probable cause); *Groh v. Ramirez*, 540 U.S. 551, 554 (2004) (finding that magistrate judge signed facially defective warrant).

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

interceptions must eventually become known at least to the subject," so that he "can then seek appropriate civil redress for example, under [18 U.S.C. § 2520], if he feels that his privacy has been unlawfully invaded."); Fed. R. Crim. P. 41(g). In this way, the requirement of notice mirrors the bedrock due-process requirement that the government provide notice of (and an opportunity to respond to) any deprivation of liberty. *See Mathews v. Eldridge*, 424 U.S. 319 (1976); *United States v. James Daniel Good Real Property*, 510 U.S. 43, 55 (1993).[5]

On the other hand, the government has no legitimate interest in withholding notice forever. While investigators may have an interest in delaying notice of a search in certain circumstances, those justifications eventually expire—for instance, when an investigation is closed for lack of evidence of wrongdoing, when the suspect learns of the investigation, or when the investigation results in prosecution. *See* 18 U.S.C. § 3103a(b)(1) (permitting delayed notice of surreptitious searches only where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result"); *id.* § 2518(8)(d) (requiring notice of wiretap within 90 days except where government shows "good cause" for postponement).

The balance of these interests makes clear what the Supreme Court and the Ninth Circuit have already held: that electronic searches and seizures carried out without any requirement for notice are unreasonable under the Fourth Amendment.

B. The notice required is to those whose Fourth Amendment interests are invaded.

Simply put, the right to notice travels with the right to privacy. The government argues otherwise, maintaining that the Fourth Amendment requires that the government notify only *Microsoft* of the search and seizure of its customers' communications. Gov't MTD Br. 22–23.

[5] Indeed, if the Fourth Amendment did not itself require notice, the Fifth Amendment clearly would. The government must provide notice at some point of every deprivation of liberty, and an invasion of constitutionally protected privacy unquestionably constitutes a deprivation of liberty. *See, e.g.*, *Wolf v. People of the State of Colo.*, 338 U.S. 25, 27–28 (1949), *overruled on other grounds by Mapp v. Ohio*, 367 U.S. 643 (1961).

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

But that rule ignores *Freitas*, *Berger*, *Donovan*, and *Dalia*, all of which described a constitutional right to notice held by the same individual whose privacy the government had invaded. Any other understanding would render the right to notice meaningless. If Microsoft's customers possess a protected Fourth Amendment interest in their communications (which they do, *see* Part I.C), then notifying *Microsoft alone* of the search or seizure of those communications accomplishes little with respect to the parties actually holding the right. It would, instead, operate solely to require notice to a party that, the government claims, cannot even assert the Fourth Amendment rights at issue. This is not the law.

The government's argument conflates a historical anachronism with a constitutional principle. The government is correct that officers traditionally provided Fourth Amendment notice at the physical site of the intrusion. But that is so because, for the first 175 years of the Fourth Amendment's application, it was understood to cover primarily physical trespasses. *See Katz*, 389 U.S. at 353. As a result, notice provided at the site of the intrusion *was* notice to the individual whose Fourth Amendment rights were at stake. It is no surprise, therefore, that Federal Rule of Criminal Procedure 41 reflects that historical context. Under Rule 41(f), an officer executing a warrant must "give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken or leave a copy of the warrant and receipt at the place where the officer took the property." Fed. R. Crim. P. 41 (f)(1)(C). This provision was first enacted as Section 12, Title 11 of the Espionage Act, 18 U.S.C. § 622 (1917),[6] which in turn was drawn directly from Section 803 of the New York Code of Criminal Procedure, set out at least as early as 1881.[7] H. R. Rep. 65 at 20 (1917). In 1881,

[6] "When the officer takes property under the warrant, he must give a copy of the warrant together with a receipt for the property taken (specifying it in detail) to the person from whom it was taken by him, or in whose possession it was found; or, in the absence of any person, he must leave it in the place where he found the property."

[7] *See* N.Y. Crim. Pro. Code § 803 (1881), *available at* https://archive.org/stream/codecriminalpro08stagoog#page/n223/mode/2up.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

when the government searched or seized an individual's property, notice at the site of the intrusion constituted notice to the owner of the property.

Technology overtook this historical practice with the advent of wiretapping. With wiretapping, the government gained the ability to search and seize without physical trespass—and the Supreme Court responded by ensuring that the core protections of the Fourth Amendment continued to apply. Since *Berger* and *Katz*, the Supreme Court has consistently held that the constitutionality of surreptitious spying regimes turns, in part, on whether they give effect to the right to notice. And the notice contemplated has always been to those whose Fourth Amendment interests are at stake. In *Berger* itself, the Court invalidated an eavesdropping statute that did not require notice to the government's surveillance target. 388 U.S. at 60. And in *Donovan*, the Court held (as explained in *Dalia*) "that Title III provided a constitutionally adequate substitute for advance notice by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on *those subjected to surveillance*." *Dalia*, 441 U.S. at 248 (emphasis added).[8] The Supreme Court has never suggested that Title III is constitutional because it requires notice to, for example, AT&T or Verizon, on whose property the government conducts its wiretaps. That would make little sense. Yet the government relies on that flawed logic here.

The other cases the government cites in support of its argument are unavailing. Gov't MTD Br. 22–23. Those cases: (1) concern records in which the court found no Fourth

[8] When Congress enacted Title III, it not only acknowledged that notice to the target was constitutionally required, *see* S. Rep 90-1097 at 74 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2161–62, but expressly stated that Title's III's notice requirement was intended to replicate the notice provided by conventional search warrants under Rule 41. *Id.* at 105, *as reprinted in* 1968 U.S.C.C.A.N. at 2194 ("Subparagraph (d) places on the judge the duty of causing an inventory to be served by the law enforcement agency on the person named in an order authorizing or approving an interception. This reflects existing search warrant practice." (citing Fed. R. Crim. P. 41, *Berger*, and *Katz*)); *Chun*, 503 F.2d at 537 ("To compensate partially for the loss of prior notice, which is traditionally available in the use of conventional search warrants . . . post-use notice is also required [by Title III]."); *id.* at 539 ("Congress intended § 2518(8)(d) to . . . reflect the inventory and notice system for conventional search warrants contained in Rule 41").

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

Amendment protection at all, and so had no Fourth Amendment foundation upon which to require notice,[9] (2) rely on a Second Circuit decision that expressly distinguished its view of notice from the Ninth Circuit's decision in *Freitas*,[10] or (3) concern only the meaning of Rule 41 rather than the requirements of the Fourth Amendment.[11]

For these reasons, the Fourth Amendment requires the government to provide notice to the persons whose Fourth Amendment interests it invades.

C. The government's search and seizure of communications under ECPA without notice is unconstitutional.

The ACLU has a reasonable expectation of privacy in the electronic communications it stores on Microsoft's servers. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008); *In re Grand Jury Subpoena*, 2016 WL 3745541, at *5. The government does not dispute this fact. *See* Gov't MTD Br. 9–10 (disputing expectation of privacy only in "most non-content records and information").[12] Because the ACLU—and, indeed, all Microsoft customers—have a reasonable expectation of privacy in their communications, they are entitled to notice when the government searches or seizes those communications. Notice may be delayed in exceptional circumstances, but it may not be withheld forever. *See Freitas*, 800 F.2d at 1456.

---

[9] *See SEC v. O'Brien*, 467 U.S. 735, 743 (1984) (no Fourth Amendment rights with respect to financial records held by financial firm); *Newfield v. Ryan*, 91 F.2d 700, 704 (5th Cir. 1937) ("[T]he sender of messages has no rights, either of substance or of procedure, for such a demand invades no privacy of his . . . ."); *In re Horowitz*, 482 F.2d 72 (2d Cir. 1973) (subpoena for records).

[10] *See United States v. Scully*, 108 F. Supp. 3d 59, 84 (E.D.N.Y. 2015) (citing *United States v. Pangburn*, 983 F.2d 449 (2d Cir. 1993), which is inconsistent, in part, with *Freitas*).

[11] *See United States v. Bansal*, 663 F.3d 634, 662 (3d Cir. 2011).

[12] Intervenors disagree with the government about the extent of Fourth Amendment protection for non-content information stored on Microsoft's servers. But for purposes of this filing, they focus solely on communications and other content, which the Ninth Circuit has already recognized are protected by the Fourth Amendment.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

Under section 2703, the government routinely acquires electronic communications without ever providing notice to those whose communications it acquires. *See* Gov't MTD Br. 4 n.3. That practice is unconstitutional, and section 2703 is unconstitutional to the extent it authorizes it.

II. Microsoft has third-party standing to assert its customers' right to notice.

Microsoft's Fourth Amendment challenge overcomes the prudential limits on third-party standing because (1) Microsoft has a close relationship with its customers, who hold the Fourth Amendment right to notice, and (2) Microsoft's customers are unable to protect their own interests independently. *See Mills v. United States*, 742 F.3d 400, 407 (9th Cir. 2014) (citing *Kowalski v. Tesmer*, 543 U.S. 125, 130 (2004)). The ACLU agrees with Microsoft's explanation of its third-party standing and makes here only two brief points.

First, Microsoft has a sufficiently close relationship to its customers to assert their privacy interests under the Fourth Amendment. Courts have routinely recognized third-party standing in cases involving vendors and service providers, *see Craig v. Boren*, 429 U.S. 190, 195 (1976); *Doe v. Bolton*, 410 U.S. 179, 188 (1973); *Rothner v. City of Chicago*, 929 F.2d 297, 300–01 (7th Cir. 1991). Moreover, in the specific context of a communications service provider, "[t]he trend among courts which have been presented with this question is to hold that entities such as newspapers, internet service providers, and website hosts may, under the principle of *jus tertii* standing, assert the rights of their readers and subscribers." *McVicker v. King*, 266 F.R.D. 92, 95 (W.D. Pa. 2010).[13] Indeed, the government itself has acknowledged that technology

[13] *See also, e.g.*, *Enterline v. Pocono Medical Ctr.*, 751 F. Supp. 2d 782, 786 (M.D. Pa. 2008) (holding that a newspaper had standing to assert the First Amendment rights of anonymous commentators on its online forums); *Trawinski v. Doe*, No. A-0312-14T1, 2015 WL 3476553, at *5 (N.J. Super. Ct. App. Div. June 3, 2015) (same); *In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244, 258 (D.D.C. 2003) ("The relationship between an Internet service provider and its subscribers is the type of relationship courts have found will ensure that issues will be 'concrete and sharply presented.' Verizon has a vested interest in vigorously protecting its subscribers' First Amendment rights, because a failure to do so could affect Verizon's ability to maintain and broaden its client base."), *rev'd on other grounds sub nom. Recording Indus. Ass'n of Amer., Inc. v. Verizon*, 351 F.3d 1229 (D.C. Cir. 2003).

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

companies are an "effective proxy for defending [their customers' privacy] rights." At a House Judiciary Committee hearing in 2011, a congressman asked a senior Department of Justice representative "why [a service provider] would have an incentive to hire lawyers to protect [its subscribers' privacy] rights." The Department's representative responded that "Internet service providers take the privacy of their customers and subscribers very seriously and I think are often an effective proxy for defending those rights."[14]

Moreover, the government's argument that "Fourth Amendment rights cannot be vicariously asserted" in any context, Gov't MTD Br. 11, distorts precedent. Third parties may not invoke the *exclusionary rule* of the Fourth Amendment by reference to the privacy interests of others. *See, e.g.*, *Nat'l Cottonseed Prods. Ass'n v. Brock*, 825 F.2d 482, 491 (D.C. Cir. 1987). But that limitation is tied to the particular *remedy* of evidentiary suppression. *See, e.g., United States v. Salvucci*, 448 U.S. 83, 86–89 (1980). Even the government's principal authority for its overbroad proposition—*Rakas v. Illinois*, 439 U.S. 128 (1978) (cited at Gov't MTD Br. 10–11)—explicitly (and solely) concerned the costs and benefits of the exclusionary rule. *See id.* at 137–38 ("Since our cases generally have held that one whose Fourth Amendment rights are violated may successfully suppress evidence obtained in the course of an illegal search and seizure, misgivings as to the benefit of enlarging the class of persons who may invoke that rule are properly considered when deciding whether to expand standing to assert Fourth Amendment violations."). The Court should reject the government's attempt to recast that rule as a bar on Microsoft's Fourth Amendment claim here.

Second, the "more important" factor for assessing third-party standing is whether the individuals whose rights are at stake would be unable to assert their interests independently, and that factor weighs decisively in favor of Microsoft. *See Eisenstadt v. Baird*, 405 U.S. 438, 445

[14] Todd M. Hinnen, Statement of Acting Assistant Attorney General for National Security at the Department of Justice, Hearing on "Permanent Provisions of The PATRIOT Act," House Judiciary Committee, Subcomm. on Crime, Terrorism, and Homeland Security, page 65, March 30, 2011, *available at* https://judiciary.house.gov/_files/hearings/printers/112th/112-15_65486.PDF.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

(1972) ("[M]ore important than the nature of the relationship between the litigant and those whose rights he seeks to assert is the impact of the litigation on the third-party interests. . . . [T]he case for according standing to assert third-party rights is stronger in this regard here than in *Griswold* because [the rights-holders] are denied a forum in which to assert their own rights."). The upshot of the government's arguments in this case is that nobody can challenge its failure to provide notice until the government has already unilaterally chosen to provide it. Indeed, the only instance in which the government allows that an individual could challenge its failure to provide notice is "after arraignment during the discovery process." Gov't Opp'n to Mot. to Intervene 11. But many individuals whose private communications are secretly searched will never be indicted, and thus will never know that they have been injured by the search *or* by the government's failure to provide notice of it. And even those individuals who are indicted and do eventually receive notice will often have little reason, at that point, to challenge the earlier deprivation of notice. In short, when the government obtains an individual's communications without notice, that individual is injured—but she has no knowledge of that injury and therefore is unable to challenge it. Given this predicament, it is unsurprising that few, if any, notice challenges have arisen under ECPA since its passage. Individuals whose communications are searched without notice generally have no avenue to seek relief independently. *See United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 574 (3d Cir. 1980) (recognizing third-party standing where "the absence of any notice to the employees of the subpoena means that no person other than Westinghouse would be likely to raise the privacy claim."). This is precisely the gap that the third-party standing doctrine is intended to fill.

CONCLUSION

For the foregoing reasons, the Court should deny the government's motion to dismiss Microsoft's Fourth Amendment claims.

AMERICAN CIVIL LIBERTIES UNION OF WASHINGTON FOUNDATION
901 FIFTH AVENUE #630
SEATTLE, WA 98164
(206) 624-2184

August 26, 2016

Respectfully submitted,

/s/ Alex Abdo
Alex Abdo (*pro hac vice*)
Patrick Toomey*
Brett Max Kaufman*
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
aabdo@aclu.org
*on the brief

/s/ Emily Chiang
Emily Chiang, WSBA No. 50517
ACLU of Washington Foundation
901 Fifth Avenue, Suite 630
Seattle, WA 98164
(206) 624-2184
echiang@aclu-wa.org

Counsel for Plaintiffs–Intervenors