

THE HONORABLE JAMES L. ROBERT

**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**

**TABLE OF CONTENTS**

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

Table of Authorities ..... iii

Introduction..... 1

Background.....3

Legal Standard ..... 4

Argument ..... 4

    I.    The government’s failure to provide notice to those whose private  
communications it obtains under ECPA violates the Fourth Amendment. ....5

        A.    The Fourth Amendment requires notice. .... 5

        B.    The notice required is to those whose Fourth Amendment interests are  
invaded. .... 9

        C.    The government’s search and seizure of communications under ECPA  
without notice is unconstitutional. .... 12

    II.    Microsoft has third-party standing to assert its customers’ right to notice. ....13

Conclusion ..... 15

**TABLE OF AUTHORITIES**

**Cases**

*100Reporters LLC v. DOJ*, 307 F.R.D. 269 (D.D.C. 2014) ..... 1

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

*Craig v. Boren*, 429 U.S. 190 (1976) ..... 13

*Dalia v. United States*, 441 U.S. 238 (1979) ..... 7, 10, 11

*Doe v. Bolton*, 410 U.S. 179 (1973)..... 13

*Eisenstadt v. Baird*, 405 U.S. 438 (1972) ..... 15

*Enterline v. Pocono Medical Ctr.*, 751 F. Supp. 2d 782 (M.D. Pa. 2008)..... 13

*Franks v. Delaware*, 438 U.S. 154 (1978) ..... 8

*Groh v. Ramirez*, 540 U.S. 551 (2004) ..... 8

*In re Grand Jury Subpoena*, No. 15-35434, 2016 WL 3745541 (9th Cir. July 13, 2016) ..... 8, 12

*In re Horowitz*, 482 F.2d 72 (2d Cir. 1973) ..... 12

*In re Verizon Internet Servs., Inc.*, 257 F. Supp. 2d 244 (D.D.C. 2003) ..... 13

*Katz v. United States*, 389 U.S. 347 (1967) ..... 6, 7, 10, 11

*Kowalski v. Tesmer*, 543 U.S. 125 (2004) ..... 13

*Malley v. Briggs*, 475 U.S. 335 (1986) ..... 8

*Mathews v. Eldridge*, 424 U.S. 319 (1976)..... 9

*McVicker v. King*, 266 F.R.D. 92 (W.D. Pa. 2010) ..... 13

*Mills v. United States*, 742 F.3d 400 (9th Cir. 2014) ..... 13

*Nat’l Cottonseed Prods. Ass’n v. Brock*, 825 F.2d 482 (D.C. Cir. 1987) ..... 14

*Newfield v. Ryan*, 91 F.2d 700 (5th Cir. 1937) ..... 12

*Rakas v. Illinois*, 439 U.S. 128 (1978) ..... 14

*Riley v. California*, 134 S. Ct. 2473 (2014) ..... 8

1 *Rothner v. City of Chicago*, 929 F.2d 297 (7th Cir. 1991) ..... 13

2 *SEC v. O’Brien*, 467 U.S. 735 (1984)..... 12

3 *Trawinski v. Doe*, No. A-0312-14T1, 2015 WL 3476553 (N.J. Super. Ct. App.

4 Div. June 3, 2015)..... 13

5 *United States v. Bansal*, 663 F.3d 634 (3d Cir. 2011) ..... 12

6 *United States v. Chun*, 503 F.2d 533 (9th Cir. 1974)..... 6, 11

7 *United States v. Donovan*, 429 U.S. 413 (1977)..... 2, 6, 7, 11

8 *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008)..... 12

9 *United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986)..... 5, 7, 10, 12

10 *United States v. James Daniel Good Real Property*, 510 U.S. 43 (1993) ..... 9

11 *United States v. Johns*, 851 F.2d 1131 (9th Cir. 1988)..... 7

12 *United States v. Pangburn*, 983 F.2d 449 (2d Cir. 1993) ..... 12

13 *United States v. Salvucci*, 448 U.S. 83 (1980) ..... 14

14 *United States v. Scully*, 108 F. Supp. 3d 59 (E.D.N.Y. 2015) ..... 12

15 *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010)..... 12

16 *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570 (3d Cir. 1980)..... 15

17 **Statutes**

18 18 U.S.C. § 2518..... 6, 9, 11

19 18 U.S.C. § 2520..... 9

20 18 U.S.C. § 2703..... 3

21 18 U.S.C. § 2705..... 3

22 18 U.S.C. § 3103a..... 9

23 Fed. R. Crim. P. 41 ..... 9, 10, 11

24 N.Y. Crim. Pro. Code § 803 (1881)..... 10

25

26 **Other Authorities**

27 114 Cong. Rec. 14485 (1968)..... 6

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

H. R. Rep. 65 (1917)..... 10  
S. Rep. 90-1097, 1968 U.S.C.C.A.N. 2112 ..... 8, 11

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

### 13 INTRODUCTION

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

---

25  
26 <sup>1</sup> Should this Court deny its motion to intervene, the ACLU respectfully requests leave to file  
27 this brief as *amicus curiae*.

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

5         The government’s principal defense of its failure to provide notice to Microsoft’s  
6 customers relies on an anachronism. Historically, the Fourth Amendment protected property  
7 interests, and the traditional manner of providing notice reflects that fact. Leaving a copy of the  
8 warrant and an inventory of property seized at the physical location of the invasion satisfied the  
9 government’s constitutional obligation to provide notice. But as Americans began to rely on third  
10 parties to route their sensitive communications, the government acquired the ability to search or  
11 seize without physical trespass, raising the specter of widespread invasions of privacy without  
12 notice to those directly affected. The Supreme Court responded by ensuring that the right to  
13 notice kept pace with evolving technologies. It invalidated an electronic surveillance statute that  
14 did not require notice to the government’s targets, *see Berger v. New York*, 388 U.S. 41, 60  
15 (1967), and it sustained one that did, *see United States v. Donovan*, 429 U.S. 413, 429 n.19  
16 (1977). In the process, the Court made clear that the individual searched is the one entitled to  
17 notice.

18         The government attempts to insulate its refusal to provide notice from judicial review,  
19 arguing that neither Microsoft nor the ACLU has standing to raise these important constitutional  
20 questions. By the government’s logic, Microsoft does not *ever* have standing to defend its  
21 customers’ right to notice, and Microsoft’s customers, including the ACLU, may not defend their  
22 own right to notice until *after* they receive the primary relief they would seek—that is, notice. In  
23 the government’s view, the only plaintiffs who have standing to sue for notice are those who  
24 have already gotten it, and those deprived of notice forever have no ability to seek a remedy at  
25 all. That is not the law. Microsoft has third-party standing to assert the Fourth Amendment rights  
26 of its customers because of its close relationship to them and, most importantly, because under  
27

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

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

### 8 **BACKGROUND**

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

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

25 Today, the government ordinarily uses a warrant when it seeks individuals’ electronic  
26 communications from third-party service providers. *See* Intervenor’s Compl. ¶ 20, ECF No. 13-  
27



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

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

### 20 LEGAL STANDARD

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

### 23 ARGUMENT

24 The Court should deny the government's motion to dismiss Microsoft's Fourth  
25 Amendment claims (and, by implication, the ACLU's complementary claims) because the  
26 government's failure to provide notice to Microsoft's customers of the search or seizure of their  
27

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

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

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

11 **A. The Fourth Amendment requires notice.**

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

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

---

26 <sup>2</sup> Although *Freitas* appears to be the Ninth Circuit’s clearest articulation of the right to notice,  
27 the court recognized the right as early as 1974. See *United States v. Chun*, 503 F.2d 533, 536 (9th  
INTS.’ OPPOSITION TO MOT. TO DISMISS - 5

1           The Supreme Court has also, time and again, recognized the constitutional necessity of  
2 notice. In *Berger v. New York*, 388 U.S. 41, 60 (1967), the Supreme Court struck down a New  
3 York eavesdropping statute, in part because “the statute’s procedure . . . has no requirement for  
4 notice as do conventional warrants.” A few months later, in *Katz v. United States*, 389 U.S. 347  
5 (1967), the Supreme Court invalidated the practice of warrantless wiretapping and, in the  
6 process, again discussed the requirement of notice. In setting out a framework for Congress to  
7 consider in crafting a constitutional wiretapping scheme, *see id.* at 354–56, the Court suggested  
8 that even if wiretapping targets were not constitutionally entitled to *advance* notice (as a  
9 “conventional warrant” ordinarily provides), the government could not dispense with notice  
10 altogether. *See id.* at 355 n.16 (“In omitting any requirement of advance notice, the federal court  
11 that authorized electronic surveillance in *Osborn* simply recognized, as has this Court, that  
12 officers need not announce their purpose before conducting an otherwise authorized search if  
13 such an announcement would provoke the escape of the suspect or the destruction of critical  
14 evidence.”).

15           A year after *Katz*, Congress enacted Title III, the still-operative federal wiretapping law,  
16 which obligates the government to provide notice to wiretap targets, subject to court-authorized  
17 delay. 18 U.S.C. § 2518(8)(d). In two cases addressing Title III, the Supreme Court has made  
18 even clearer what it said in *Berger* and *Katz*. First, in *United States v. Donovan*, 429 U.S. 413  
19 (1977), the Court considered the proper statutory construction of Title III’s delayed-notice  
20 provision but also briefly addressed its constitutionality. It approvingly quoted Congress’s  
21 summary of *Berger* and *Katz*: “The *Berger* and *Katz* decisions established that notice of  
22 surveillance is a constitutional requirement of any surveillance statute.” *Donovan*, 429 U.S. at  
23 430 (quoting 114 Cong. Rec. 14485–86 (1968)). And in a footnote citing those same decisions,

---

24  
25 Cir. 1974) (“In *Berger v. New York*, 388 U.S. 41, 87 S. Ct. 1873, 18 L. Ed. 2d 1040 (1967), the  
26 Supreme Court enunciated certain constitutional standards which a valid wiretapping statute  
27 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).

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

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

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

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

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

---

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

25 <sup>4</sup> *See, e.g., Franks v. Delaware*, 438 U.S. 154, 169 (1978) (“[T]he hearing before the  
 26 magistrate not always will suffice to discourage lawless or reckless misconduct.”); *Malley v.*  
 27 *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).

1 interceptions must eventually become known at least to the subject,” so that he “can then seek  
2 appropriate civil redress for example, under [18 U.S.C. § 2520], if he feels that his privacy has  
3 been unlawfully invaded.”); Fed. R. Crim. P. 41(g). In this way, the requirement of notice  
4 mirrors the bedrock due-process requirement that the government provide notice of (and an  
5 opportunity to respond to) any deprivation of liberty. *See Mathews v. Eldridge*, 424 U.S. 319  
6 (1976); *United States v. James Daniel Good Real Property*, 510 U.S. 43, 55 (1993).<sup>5</sup>

7 On the other hand, the government has no legitimate interest in withholding notice  
8 forever. While investigators may have an interest in delaying notice of a search in certain  
9 circumstances, those justifications eventually expire—for instance, when an investigation is  
10 closed for lack of evidence of wrongdoing, when the suspect learns of the investigation, or when  
11 the investigation results in prosecution. *See* 18 U.S.C. § 3103a(b)(1) (permitting delayed notice  
12 of surreptitious searches only where “the court finds reasonable cause to believe that providing  
13 immediate notification of the execution of the warrant may have an adverse result”); *id.*  
14 § 2518(8)(d) (requiring notice of wiretap within 90 days except where government shows “good  
15 cause” for postponement).

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

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

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

---

24 <sup>5</sup> Indeed, if the Fourth Amendment did not itself require notice, the Fifth Amendment clearly  
25 would. The government must provide notice at some point of every deprivation of liberty, and an  
26 invasion of constitutionally protected privacy unquestionably constitutes a deprivation of liberty.  
27 *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).

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

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

---

22  
23  
24 <sup>6</sup> "When the officer takes property under the warrant, he must give a copy of the warrant  
25 together with a receipt for the property taken (specifying it in detail) to the person from whom it  
26 was taken by him, or in whose possession it was found; or, in the absence of any person, he must  
27 leave it in the place where he found the property."

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



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

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

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

---

20 <sup>8</sup> When Congress enacted Title III, it not only acknowledged that notice to the target was  
21 constitutionally required, *see* S. Rep 90-1097 at 74 (1968), *as reprinted in* 1968 U.S.C.C.A.N.  
22 2112, 2161–62, but expressly stated that Title’s III’s notice requirement was intended to replicate  
23 the notice provided by conventional search warrants under Rule 41. *Id.* at 105, *as reprinted in*  
24 1968 U.S.C.C.A.N. at 2194 (“Subparagraph (d) places on the judge the duty of causing an  
25 inventory to be served by the law enforcement agency on the person named in an order  
26 authorizing or approving an interception. This reflects existing search warrant practice.” (citing  
27 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”).



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

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

7 **C. The government’s search and seizure of communications under ECPA**  
 8 **without notice is unconstitutional.**

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

18  
 19  
 20 <sup>9</sup> *See SEC v. O’Brien*, 467 U.S. 735, 743 (1984) (no Fourth Amendment rights with respect to  
 21 financial records held by financial firm); *Newfield v. Ryan*, 91 F.2d 700, 704 (5th Cir. 1937)  
 22 (“[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).

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

25 <sup>11</sup> *See United States v. Bansal*, 663 F.3d 634, 662 (3d Cir. 2011).

26 <sup>12</sup> Intervenors disagree with the government about the extent of Fourth Amendment protection  
 27 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.

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

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

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

12 First, Microsoft has a sufficiently close relationship to its customers to assert their  
13 privacy interests under the Fourth Amendment. Courts have routinely recognized third-party  
14 standing in cases involving vendors and service providers, *see Craig v. Boren*, 429 U.S. 190, 195  
15 (1976); *Doe v. Bolton*, 410 U.S. 179, 188 (1973); *Rothner v. City of Chicago*, 929 F.2d 297, 300–  
16 01 (7th Cir. 1991). Moreover, in the specific context of a communications service provider,  
17 “[t]he trend among courts which have been presented with this question is to hold that entities  
18 such as newspapers, internet service providers, and website hosts may, under the principle of *jus*  
19 *tertii* standing, assert the rights of their readers and subscribers.” *McVicker v. King*, 266 F.R.D.  
20 92, 95 (W.D. Pa. 2010).<sup>13</sup> Indeed, the government itself has acknowledged that technology

21  
22 <sup>13</sup> *See also, e.g., Enterline v. Pocono Medical Ctr.*, 751 F. Supp. 2d 782, 786 (M.D. Pa. 2008)  
23 (holding that a newspaper had standing to assert the First Amendment rights of anonymous  
24 commentators on its online forums); *Trawinski v. Doe*, No. A-0312-14T1, 2015 WL 3476553, at  
25 \*5 (N.J. Super. Ct. App. Div. June 3, 2015) (same); *In re Verizon Internet Servs., Inc.*, 257 F.  
26 Supp. 2d 244, 258 (D.D.C. 2003) (“The relationship between an Internet service provider and its  
27 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).

1 companies are an “effective proxy for defending [their customers’ privacy] rights.” At a House  
2 Judiciary Committee hearing in 2011, a congressman asked a senior Department of Justice  
3 representative “why [a service provider] would have an incentive to hire lawyers to protect [its  
4 subscribers’ privacy] rights.” The Department’s representative responded that “Internet service  
5 providers take the privacy of their customers and subscribers very seriously and I think are often  
6 an effective proxy for defending those rights.”<sup>14</sup>

7 Moreover, the government’s argument that “Fourth Amendment rights cannot be  
8 vicariously asserted” in any context, Gov’t MTD Br. 11, distorts precedent. Third parties may  
9 not invoke the *exclusionary rule* of the Fourth Amendment by reference to the privacy interests  
10 of others. *See, e.g., Nat’l Cottonseed Prods. Ass’n v. Brock*, 825 F.2d 482, 491 (D.C. Cir. 1987).  
11 But that limitation is tied to the particular *remedy* of evidentiary suppression. *See, e.g., United*  
12 *States v. Salvucci*, 448 U.S. 83, 86–89 (1980). Even the government’s principal authority for its  
13 overbroad proposition—*Rakas v. Illinois*, 439 U.S. 128 (1978) (cited at Gov’t MTD Br. 10–  
14 11)—explicitly (and solely) concerned the costs and benefits of the exclusionary rule. *See id.* at  
15 137–38 (“Since our cases generally have held that one whose Fourth Amendment rights are  
16 violated may successfully suppress evidence obtained in the course of an illegal search and  
17 seizure, misgivings as to the benefit of enlarging the class of persons who may invoke that rule  
18 are properly considered when deciding whether to expand standing to assert Fourth Amendment  
19 violations.”). The Court should reject the government’s attempt to recast that rule as a bar on  
20 Microsoft’s Fourth Amendment claim here.

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

---

24 <sup>14</sup> Todd M. Hinnen, Statement of Acting Assistant Attorney General for National Security at  
25 the Department of Justice, Hearing on “Permanent Provisions of The PATRIOT Act,” House  
26 Judiciary Committee, Subcomm. on Crime, Terrorism, and Homeland Security, page 65, March  
27 30, 2011, *available at* [https://judiciary.house.gov/\\_files/hearings/printers/112th/112-15\\_65486.PDF](https://judiciary.house.gov/_files/hearings/printers/112th/112-15_65486.PDF).

1 (1972) (“[M]ore important than the nature of the relationship between the litigant and those  
2 whose rights he seeks to assert is the impact of the litigation on the third-party interests. . . .  
3 [T]he case for according standing to assert third-party rights is stronger in this regard here than in  
4 *Griswold* because [the rights-holders] are denied a forum in which to assert their own rights.”).  
5 The upshot of the government’s arguments in this case is that nobody can challenge its failure to  
6 provide notice until the government has already unilaterally chosen to provide it. Indeed, the  
7 only instance in which the government allows that an individual could challenge its failure to  
8 provide notice is “after arraignment during the discovery process.” Gov’t Opp’n to Mot. to  
9 Intervene 11. But many individuals whose private communications are secretly searched will  
10 never be indicted, and thus will never know that they have been injured by the search *or* by the  
11 government’s failure to provide notice of it. And even those individuals who are indicted and do  
12 eventually receive notice will often have little reason, at that point, to challenge the earlier  
13 deprivation of notice. In short, when the government obtains an individual’s communications  
14 without notice, that individual is injured—but she has no knowledge of that injury and therefore  
15 is unable to challenge it. Given this predicament, it is unsurprising that few, if any, notice  
16 challenges have arisen under ECPA since its passage. Individuals whose communications are  
17 searched without notice generally have no avenue to seek relief independently. *See United States*  
18 *v. Westinghouse Elec. Corp.*, 638 F.2d 570, 574 (3d Cir. 1980) (recognizing third-party standing  
19 where “the absence of any notice to the employees of the subpoena means that no person other  
20 than Westinghouse would be likely to raise the privacy claim.”). This is precisely the gap that the  
21 third-party standing doctrine is intended to fill.

## 22 CONCLUSION

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

1 August 26, 2016

Respectfully submitted,

2 /s/ Alex Abdo

Alex Abdo (*pro hac vice*)

3 Patrick Toomey\*

4 Brett Max Kaufman\*

American Civil Liberties Union Foundation

5 125 Broad Street, 18th Floor

New York, NY 10004

6 (212) 549-2500

aabdo@aclu.org

7 \*on the brief

8 /s/ Emily Chiang

9 Emily Chiang, WSBA No. 50517

10 ACLU of Washington Foundation

901 Fifth Avenue, Suite 630

11 Seattle, WA 98164

(206) 624-2184

12 echiang@aclu-wa.org

13 *Counsel for Plaintiffs–Intervenors*