American University Law Review

Volume 66 | Issue 3 Article 6

2017

Cloudy with a Chance of Abused Privacy Rights: Modifying Third-Party Fourth Amendment Standing Doctrine Post-Spokeo

Sarah E. Pugh

Cloudy with a Chance of Abused Privacy Rights: Modifying Third-Party Fourth Amendment Standing Doctrine Post-Spokeo

Keywords
The Stored Communications Act, SCA, privacy, Electronic communications, cloud

CLOUDY WITH A CHANCE OF ABUSED PRIVACY RIGHTS: MODIFYING THIRD-PARTY FOURTH AMENDMENT STANDING DOCTRINE POST-*SPOKEO*

SARAH E. PUGH*

The Stored Communications Act (SCA) provides various privacy protections for electronic communications; however, the statute has failed to keep up with technological advances, and the application of third-party Fourth Amendment standing doctrine has whittled away privacy protections. Microsoft is bringing a Fourth Amendment challenge to sections 2703 and 2705 of the SCA, which—when used in combination—permit the government to use "no-notice warrants" and secrecy orders to access a cloud user's communications and data from the electronic communications provider without the cloud user's knowledge.

The greater problem is that these actions may go unchallenged in court. As the U.S. Supreme Court's standing jurisprudence currently provides, Fourth Amendment rights may not be raised vicariously. However, where Microsoft's cloud customers are entirely unaware that a search has taken place, they lack the knowledge to bring a claim and assert their own rights. Moreover, there is the secondary problem of establishing whether Microsoft's customers have suffered a sufficient harm from this invasion of privacy by the government. New case law suggests that the improper sharing of personal information might not satisfy the "injury in fact" requirement for standing. If the Court extends this case to the Fourth Amendment and requires evidence that the

* Junior Staff Member, *American University Law Review*, Volume 66; J.D. Candidate, May 2018, *American University Washington College of Law*; B.A., Political Science, 2015, *Northeastern University*. I would like to express my gratitude to my colleagues on the *Law Review*—particularly, Morgan Creamer and Sarah West, my Note & Comment Editors—for their considerable time and effort editing and providing feedback. I would also like to thank Professor Jennifer Daskal for sharing her invaluable knowledge and perspective on this topic. Finally, I am eternally grateful to my parents, friends, and family for their continued and unwavering love and support.

search had a concrete negative impact, Microsoft's customers may not have suffered a legally cognizable harm.

This Comment advocates adopting a modified and relaxed third-party standing doctrine to permit electronic communications service providers to defend their customers' privacy interests and raise Fourth Amendment claims on their behalf where they are unable to do so themselves. This approach would also require the court to expressly identify an improper search and seizure of electronic communications and data as a sufficient "injury in fact" to confer standing, minimizing the impact of Spokeo, Inc. v. Robins.

TABLE OF CONTENTS

INTRODUCTION

"[J]ust as the Internet has opened up the world for each and every one of us, it has also opened up each and every one of us to the world. And increasingly, the price we're being asked to pay for all of this connectedness is our privacy."
—Gary Kovacs[1]

The American people have significantly valued their privacy since colonial times, and there has been a continual battle to safeguard this privacy.[2] During the American Revolutionary War, people were

1. *Tracking Our Online Trackers*, TED TALKS (May 2012), https://www.ted.com/talks/gary_kovacs_tracking_the_trackers/transcript?language=en.

2. Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY, PLI, 1-1, § 1:2, at 1–4 (2006), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications (noting that the colonists were "afforded unprecedented privacy" in America).

concerned about general warrants that often resulted in law enforcement ransacking people's homes and belongings;[3] today, privacy concerns are still grounded in a fear of excessive government intrusion into spaces that the people have generally regarded as private and secure.[4] Because Americans value individual privacy so highly, Congress has passed many laws protecting our privacy and personal information.[5]

However, laws seeking to protect privacy have often proven inadequate, in keeping pace with significant technological progress.[6] This was true of the 1968 Wiretap Act,[7] which was ultimately amended by the Electronic Communications Privacy Act of 1986 (ECPA).[8] Now, as technology continues to develop and progress,[9] the validity of the ECPA is being called into question.

---

3. *Id.* § 1:2, at 1–5 (highlighting the preservation of privacy in the Third, Fourth, and Fifth Amendments in the Bill of Rights).

The Fourth Amendment guarantees that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

4. *See* Solove, *supra* note 2, § 1:4.2, at 1–23 ("The increasing computerization of information and the burgeoning repositories of personal data in federal agencies continued to be a topic of importance.").

5. *See, e.g.*, Omnibus Crime Control and Safe Streets Act of 1968 ("Wiretap Act"), Pub. L. No. 90-351, §§ 801–804, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2510–2520, 47 U.S.C. § 605 (2012)) (establishing rules that the government must follow to obtain wiretap orders); Fair Credit Reporting Act, Pub. L. No. 91-508, §§ 601–622, 84 Stat. 1114, 1127–36 (1970) (codified as amended at 15 U.S.C. §§ 1681–1681t) (promoting the accuracy, fairness, and privacy of information contained in the records of consumer reporting agencies); Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, § 513, 88 Stat. 484, 571–74 (codified at 20 U.S.C. § 1232g) (granting parents protections regarding information about their children's education records, including report cards, transcripts, disciplinary records, and family contact information); Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a) (governing the collection, maintenance, use, and dissemination of personal information in federal agency records).

6. Russell S. Burnside, Note, *The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies*, 13 RUTGERS COMPUTER & TECH. L.J. 451, 455 (1987).

7. *Id.* at 462–63 (noting that the Wiretap Act only expressly protected against the "unauthorized aural interception of voice communications," thereby excluding developing technologies like email and cell phones from its scope (footnote omitted)).

8. Pub. L. No. 99–508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510–2521, 2701–2710, 3117, 3121–3126 (2012)).

9. *See, e.g.*, Caitlin White, *Cloud Computing Timeline Illustrates Cloud's Past, Predicts Its Future*, TECHTARGET (DEC. 2013), http://searchcloudcomputing.techtarget.com/feat

One such development, the increasing availability of cloud storage solutions, has revolutionized Internet usage.[10] Prior to 1986, when the ECPA was first enacted, very few people outside of the business community had access to the Internet.[11] Individuals and businesses used to maintain physical control over their records by storing documents in filing cabinets or on local hard drives or servers. As personal use of the Internet increased, questions about the adequacy of privacy standards arose, leading to the privacy protections and law enforcement access standards provided for in the ECPA.[12] Today, nearly everyone uses the Internet on a daily basis—whether for communicating by email, storing documents in the cloud, or connecting with friends and colleagues through social media.[13] Both individuals and businesses have become more reliant upon third-party cloud storage solutions, such as the services provided by the Microsoft Corporation ("Microsoft"), because of their efficiency and ease of use.[14]

Because of this increase in Internet usage and shift in storage solutions, Microsoft has suggested that the data privacy standards set

---

ure/Cloud-computing-timeline-illustrates-clouds-past-predicts-its-future (highlighting the history of cloud storage from the dot-com bubble burst in the early 2000s through 2014).

10. Cloud storage is "the storing and accessing of data and programs through the internet, rather than through physical means such as hard drives." Newtek Bus. Servs., Inc., *The Future of the Cloud*, FORBES (July 8, 2015, 9:28 AM) [hereinafter *Future of the Cloud*], http://www.forbes.com/sites/thesba/2015/07/08/the-future-of-the-cloud.

11. MARIA C. PAPADAKIS & EILEEN L. COLLINS, DIV. OF SCI. RESEARCH STUDIES, NAT'L SCI. FOUND., THE APPLICATION AND IMPLICATIONS OF INFORMATION TECHNOLOGIES IN THE HOME: WHERE ARE THE DATA AND WHAT DO THEY SAY? 11 (2001), http://files.eric.ed.gov/fulltext/ED452050.pdf (noting that in 1994, the earliest year for which data is available, only two percent of households had Internet access).

12. Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1558 (2004).

13. *See id.* at 1574–75. For example, Mulligan noted that in 2004, "[o]ver 112 million individuals use[d] the Internet to search for information," and that "[g]aming [and] listening to and downloading music" were "popular activities," unlike when the Electronic Communications Privacy Act was first passed eighteen years earlier. *Id.*; *cf.* Timothy Morey et al., *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV., May 2015, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust ("[C]onsumers are aware that they're under surveillance—even though they may be poorly informed about the specific types of data collected about them . . . .").

14. *See* First Am. Compl. for Declaratory Judgment at para. 3, Microsoft Corp. v. U.S. Dep't of Justice, No. 2:16-cv-00538-JLR, 2016 WL 3381727 (W.D. Wash. June 17, 2016) [hereinafter Am. Compl.]; *see also Future of the Cloud*, *supra* note 10 ("Many [companies] are depending on the cloud to launch new business models, help streamline their supply chains, and provide applications and platforms to better manage and analyze data.").

forth in the ECPA are no longer sufficient to protect cloud users' communications and personal information.[15] The company is challenging sections 2703 and 2705(b) of the Stored Communications Act (SCA),[16] which governs the privacy of electronic communications[17] that have been in storage for various periods of time.[18] Microsoft alleges that the government's use of "no-notice warrants" under section 2703[19] in conjunction with "secrecy orders" under section 2705[20]

---

15. *See* Am. Compl., *supra* note 14, at para. 7; *see also* Mulligan, *supra* note 12, at 1558 (noting that increased Internet usage "raise[s] questions about the adequacy of the privacy standards developed in 1986").

16. *See* 18 U.S.C. §§ 2701–2712 (2012). The Stored Communications Act (SCA) is part of the Electronic Communications Privacy Act of 1986 (ECPA). *See id.*

17. The ECPA defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12) (2012).

18. *See* Am. Compl., *supra* note 14, at para. 1.

19. Section 2703(b) provides, in relevant part,

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any . . . electronic communication . . . (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction . . . .

18 U.S.C. § 2703(b).

Essentially, section 2703 of the SCA provides five procedures through which a "government entity" can require an electronic communications provider to disclose certain information about its subscribers: (1) subpoena, (2) subpoena with prior notice to the subscriber or customer, (3) court order, (4) court order with prior notice to the subscriber or customers, or (5) search warrant. *Id.* § 2703(b)(1). When using a search warrant, the government is not required to provide notice to the subscriber or customer, and because of the "probable cause" threshold required by a warrant, the government may access the entire contents of the subscriber or customer's account. In contrast, when using a subpoena, the government can only obtain more basic subscriber information without first notifying the subscriber or customer. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. DEP'T OF JUSTICE (July 2002), https://cyber.harvard.edu/practicallawyering/Week9DOJECPAExcerpt.pdf.

20. Section 2705(b) provides, in its entirety,

> 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

violate the company's First Amendment rights and its cloud customers' Fourth Amendment rights.[21] In its Fourth Amendment claim, Microsoft asserts that secrecy orders illegally eliminate notice to the targets of the searches and seizures[22] and unfairly prevent the company from being transparent with its customers.[23]

Microsoft's Fourth Amendment claim raises a unique standing issue—namely, whether Microsoft can bring the claim on behalf of its customers. Generally speaking, a business may bring such a lawsuit,[24] but doing so based on a Fourth Amendment claim is distinctive because the standing inquiry requires a more substantive analysis of the issues.[25] Specifically, for a business to bring a constitutional challenge on behalf of its customers, at least one customer must have standing to bring the claim himself; thus, if Microsoft's customers do not have standing to sue, neither does Microsoft.[26] However, establishing individual standing for the improper sharing of personal information or data has become more difficult after the United States

---

> 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.

18 U.S.C. § 2705(b).

Section 2705 allows a "government entity" to seek a court order preventing an electronic communications provider from notifying its subscriber or customer of the existence of a search warrant, subpoena, or court order where the government entity would not otherwise be required to disclose the search. *Id.* This section provides for a lesser "reason to believe" threshold. *Id.*

21. *See* Am. Compl., *supra* note 14, at para. 7. The government's use of secrecy orders is relevant to both Microsoft's First Amendment claim and its Fourth Amendment claim. In its First Amendment claim, Microsoft argues that law enforcement's excessive use of secrecy orders unconstitutionally prevents it from communicating with its customers about the government's demands for their data. Microsoft's First Amendment claim, however, is beyond the scope of this Comment.

22. *See infra* Section I.B.

23. Jim Kerstetter, *Microsoft Goes on Offensive Against Justice Department*, N.Y. TIMES (Apr. 15, 2016), http://www.nytimes.com/2016/04/16/technology/microsoft-goes-on-offensive-against-justice-department.html.

24. *Infra* Section II.A.2.

25. Nadia B. Soree, *The Demise of Fourth Amendment Standing: From Standing Room to Center Orchestra*, 8 NEV. L.J. 570, 571 (2008).

26. *See infra* Section III.B.1.

Supreme Court's recent decision in *Spokeo, Inc. v. Robins*.[27] This Comment builds on the numerous scholarly critiques of the Supreme Court's Fourth Amendment standing doctrine by specifically highlighting the unique problems that arise from the Court's narrow application of third-party Fourth Amendment standing.[28]

This Comment argues that (1) under the current doctrine, Microsoft likely does not have standing to bring a Fourth Amendment challenge to sections 2703 and 2705 of the SCA on behalf of its customers, and (2) Microsoft and its customers *should* have standing to raise this claim by proposing a new test for the Court to follow under the circumstances.

Part I provides background on the relevant sections of the SCA, Microsoft's lawsuit, traditional standing jurisprudence, and Fourth Amendment standing jurisprudence. Part II discusses the Court's hesitance to extend its third-party standing jurisprudence to Fourth Amendment challenges. Part III notes that Microsoft likely does not have standing under the Court's current jurisprudence but advocates adopting a relaxed hybrid Fourth Amendment standing doctrine where an individual is hindered from raising a claim himself. Part III also advocates limiting the impact of *Spokeo* on the Fourth Amendment to preserve individual privacy protections. A new standing doctrine is the best way to ensure that businesses providing third-party cloud-based technologies have a forum in which to raise Fourth Amendment challenges against privacy laws.

I. BACKGROUND

"It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . . ."
—Justice Bradley[29]

---

27. 136 S. Ct. 1540 (2016) (holding that a data breach resulting in the sharing of personal information was not concrete to satisfy Article III standing requirements); *see infra* notes 79–83 and accompanying text.

28. *See, e.g.*, Albert W. Alschuler, *Interpersonal Privacy and the Fourth Amendment*, 4 N. ILL. U. L. REV. 1, 4 (1983) ("[T]he doctrine [of Fourth Amendment standing] is troublesome, for it is impossible to articulate any purpose of the [F]ourth [A]mendment exclusionary rule that is not undercut to some extent by a requirement of standing."); Soree, *supra* note 25, at 571 ("[T]he Court has developed an unduly narrow vision of [Fourth Amendment] standing.").

29. Boyd v. United States, 116 U.S. 616, 630 (1886).

A. The Electronic Communications Privacy Act

Congress passed the ECPA in 1986 with the intention of protecting wire, oral, and electronic communications while they are being made, transmitted, and stored.[30] The ECPA provides a complex privacy framework that has become increasingly difficult to navigate as technology rapidly advances. Within the ECPA are various subcomponents, including the SCA,[31] which is a provision governing the privacy of electronic communications that have been in storage for various amounts of time.[32] The SCA contains dense, complex language that very few courts have explained or interpreted,[33] and it has gone relatively unchanged since its enactment in 1986.[34]

In response to the growing disparity between the language of the SCA and the state of technology, Microsoft has challenged sections 2703 and 2705 of the SCA.[35] Section 2703 contains the bulk of the privacy protections afforded by the SCA, providing certain mechanisms that the government must use when it seeks the disclosure of electronic communications.[36] Specifically, section 2703(b)(1)(A) "no-notice warrants" allow the government—with a warrant and without notice to the subscriber—to require an electronic communications or cloud storage service provider to

---

30. *See* Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510–22 (2012), U.S. DEP'T JUST. OFF. JUST. PROGRAMS, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last updated July 30, 2013) (providing a brief explanation of the ECPA).

31. *See* 18 U.S.C. §§ 2701–2712 (2012).

32. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004).

33. *Id.* at 1208 ("Despite [the SCA's] obvious importance, the statute remains poorly understood.").

34. Congress has made several minor amendments to the SCA in 1988, 1994, 1996, 1998, 2001, 2002, 2006, and 2009, but none substantially changed the law. *See* 18 U.S.C. §§ 2701–2712. However, Congress is currently contemplating a major substantive change to the SCA for the first time—a change that seeks to address the problems highlighted in this Comment. *See* Email Privacy Act, H.R. 699, 114th Cong. (2d Sess. 2016); *see also* Press Release, Representative Kevin Yoder (R-KS), Bipartisan Group Introduces Bill to Protect Online Privacy (Feb. 4, 2015), http://yoder.house.gov/media-center/press-releases/bipartisan-group-introduces-bill-to-protect-online-privacy ("The federal government is using an arcane 1986 law to conduct warrantless searches of the personal email accounts and other digital communication of the American people . . . . The last time Congress updated our email privacy laws, we were two years removed from the release of the first Macintosh computer.").

35. *See* Am. Compl., *supra* note 14, at para. 4.

36. Kerr, *supra* note 32, at 1218.

disclose the contents of any electronic communication.[37] Section 2705(b) "secrecy orders" allow the government to request that a court delay providers from notifying subscribers that their accounts are subject to government investigation; if the court has a "reason to believe" that there may be an adverse consequence to providing notice, such as "seriously jeopardizing an investigation or unduly delaying a trial," it must grant the request.[38] Because there is no time limit specified in section 2705(b)—only "for such period as the court deems appropriate"—the "delay" could last indefinitely.[39] Conversely, when communication sent through the post is the subject of a search or seizure, government access requires a warrant, and there is an implicit right to notice at all times, regardless of how long the mail has been unopened or stored in a mailbox.[40]

B. Microsoft Corp. v. United States Department of Justice

Microsoft is becoming somewhat notorious for challenging government practices under the SCA and bringing individual data privacy issues into the spotlight.[41] Microsoft's latest focus is on the

37. 18 U.S.C. § 2703(b)(1)(A); *see also* Burnside, *supra* note 6, at 516 (anticipating the need for continual review of the ECPA's language to keep up with the progression of technology).

38. 18 U.S.C. § 2705(b).

39. *Id.*

40. *Ex parte* Jackson, 96 U.S. 727, 733 (1878) ("Letters and sealed packages . . . in the mail are as fully guarded [under the Fourth Amendment] from examination and inspection . . . as if they were retained by the parties forwarding them in their own domiciles. . . . Whilst in the mail, they can only be opened and examined under . . . warrant . . . ."); *see* Amy Webb, *Send Letters, Not Emails*, SLATE (June 12, 2013, 5:08 PM), http://www.slate.com/articles/technology/data_mine_1/2013/06/nsa_surveillance_why_the_post_office_doesn_t_spy_on_your_mail_the_way_nsa.html (noting that in 2006, President Bush's administration argued that the Patriot Act permitted the government to intercept snail mail during exigent circumstances, which was widely criticized because such a policy plainly contravened existing mail protection laws); *see also* Thor Benson, *It's Not Just the NSA—The IRS Is Reading Your Emails Too*, TRUTHDIG (July 10, 2015), http://www.truthdig.com/report/item/its_not_just_the_nsa_the_irs_is_reading_your_emails_too_20150710 ("Americans overwhelmingly believe email should be protected by a warrant, just like a phone call or snail-mail letter." (quoting Gabe Rottman of the American Civil Liberties Union)).

41. *See* Jennifer Daskal, *A New Lawsuit from Microsoft: No More Gag Orders!*, JUST SEC. (Apr. 14, 2016, 12:56 PM), https://www.justsecurity.org/30583/challenge-microsoft-gag-orders (drawing attention to Microsoft's two-year dispute with the United States government over customer emails stored on servers in another country); *see also* Jay Greene & Devlin Barrett, *Microsoft Sues Justice Department Over Secret Customer Data Searches*, WALL ST. J. (Apr. 14, 2016, 8:03 PM), http://www.wsj.com/articles/microsoft-sues-justice-department-over-secret-customer-data-searches-1460649720; *supra* notes 17–23 and accompanying text (discussing

federal government's use of secrecy orders and no-notice warrants, which together prevent the company's customers from receiving notice when their data is searched or seized by the government.[42]

On April 14, 2016, Microsoft filed suit in the United States District Court for the Western District of Washington, seeking a declaratory judgment that no-notice warrants issued under section 2703(b)(1)(a) of the SCA used in combination with secrecy orders issued under 2705(b) violate, on their face,[43] the company's First Amendment rights and its cloud customers' Fourth Amendment rights.[44] Microsoft argues that "its customers have a right to know when the government obtains a warrant to read their emails,"[45] and therefore the government's use of sections 2703 and 2705 in tandem is unconstitutional.

Microsoft alleges that from September 2014 through May 2016, the government made over 6000 demands for customer information stored on the cloud; more than half of those demands were accompanied by a secrecy order, and about a third of those demands with a secrecy order also contained an indefinite bar on disclosure.[46] Microsoft notes that "the increase in government demands for online data and the simultaneous increase in secrecy [orders]" have the

---

Microsoft's current complaints about the government's privacy breaches under the SCA).

On July 14, 2016, the U.S. Court of Appeals for the Second Circuit ruled in Microsoft's favor, holding that "[section] 2703 of the Stored Communications Act does not authorize courts to issue and enforce against U.S.–based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign server[s]." Microsoft Corp. v. United States, No. 14-cv-2985, slip op. at 2 (2d Cir. July 14, 2016).

42. Daskal, *supra* note 41; *see supra* notes 19–20 (providing the statutory language).

43. Compl. Decl. J. at para. 2, Microsoft Corp. v. U.S. Dep't of Justice, No. 2:16-cv-00538 (W.D. Wash. filed Apr. 14, 2016) [hereinafter Compl.]. When challenging the constitutionality of a statute, a claim may either be brought as applied or on its face. Facial challenges under the Fourth Amendment are generally permitted. City of Los Angeles v. Patel, 135 S. Ct. 2443, 2449 (2015).

44. *See* Compl., *supra* note 43, at para. 2. As of this writing, over seventy parties have filed amicus briefs in *Microsoft Corp.*, including Google, LinkedIn, Twitter, Amazon.com, Dropbox, Snapchat, and other electronic communications providers. *See* No. 2:16-cv-00538 (N.D. Wash. 2016).

45. *See* Am. Compl., *supra* note 14, at para. 1.

46. *See id.* at para. 16. Microsoft initially pled a lesser number of requests for customer data. Compl., *supra* note 43, at para. 16; *see also* Gregg Keizer, *Microsoft: Government's Data Gag Order Practices Worse than First Thought*, COMPUTERWORLD (June 23, 2016, 12:09 PM), http://www.computerworld.com/article/3088103/data-privacy/microsoft-governments-data-gag-order-practices-worse-than-first-thought.html (pointing out that Microsoft upped the number of data demands it claimed to have received from the government in the months preceding the original complaint).

potential "to undermine confidence in the privacy of the cloud," thereby reducing the likelihood that businesses will rely on third-party cloud storage solutions.[47]

More specifically, Microsoft suggests that sections 2703 and 2705 subject its cloud storage customers to a lesser standard of privacy for choosing to store their data on the cloud as compared to other storage options.[48] They argue that under the laws governing paper files and data stored on local servers or hard drives, customers have implicit notice of the execution of a warrant, allowing them to assert their rights or challenges accordingly.[49] Conversely, when customer information is stored on the cloud by a company like Microsoft, the government can request the information it seeks directly from the company without involving the customer—the actual target of the search.[50] Microsoft claims that there is little, if any, explanation to justify this lesser privacy standard.[51]

As reliance on third-party cloud storage has grown, Microsoft argues that "the transition [to third-party storage] 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."[52] Microsoft recognizes that exceptional circumstances may arise where the government's interest in conducting an investigation would justify a temporary secrecy order, but the company objects to the government's habitual use of indefinite secrecy orders.[53]

The government has filed a motion to dismiss for lack of standing or, in the alternative, failure to state a claim.[54] The government

---

47. Am. Compl., *supra* note 14, at para. 5.

48. *Id.* at para. 7.

49. *Id.* at para. 14; *see also* Wilson v. Arkansas, 514 U.S. 927, 934 (1995) (holding that in a "reasonable" search under the Fourth Amendment, individuals have the right to know when the government has searched or seized their property).

50. Kerstetter, *supra* note 23.

51. Am. Compl., *supra* note 14, at para. 1 ("People do not give up their rights when they move their private information from physical storage to the cloud.").

52. *Id.* at para. 3.

53. *Id.* at para. 6.; *cf.* Tracey Maclin, *The Bush Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons from Justice Powell and the* Keith *Case*, 41 U.C. DAVIS L. REV. 1259, 1280–92, 1303–19 (2008) (analyzing President Bush's claim that the government has the authority to order warrantless searches and seizures of electronic communications between American citizens and persons abroad in the name of national security).

54. Motion to Dismiss Pursuant to Fed. R. Civ. P. 12(b)(1) and 12(b)(6), Microsoft Corp. v. U.S. Dep't of Justice, No. 16-cv-00538-JLR (W.D. Wash. filed July 22, 2016), ECF No. 38 [hereinafter Mot. to Dismiss]. This Comment does not

claims "Microsoft's challenge effectively asks [the court] to adjudicate the lawfulness of thousands of such court orders from across the United States."[55] Regarding standing, the government's Motion to Dismiss specifically alleges that Microsoft has failed to state a sufficient injury in fact[56] and that Microsoft's claims may not be redressed through declaratory relief.[57]

Microsoft relies on the test the Supreme Court established in *Powers v. Ohio*[58] to assert its standing to "vindicate its customers' Fourth Amendment rights" because the company's customers do not know their rights have been violated, and they therefore lack the knowledge to challenge the SCA provisions.[59] Whether Microsoft was correct in relying on *Powers* to argue standing, however, is questionable at best.

In its Motion to Dismiss, the government rejected Microsoft's contention that the company satisfies the standing requirement.[60] However, the government does not contest that *Powers* provides the applicable standing framework.[61] The government primarily argues that Microsoft has not demonstrated that it has suffered a sufficient injury in fact to establish its standing as a third party.[62] Microsoft did not submit any of the relevant secrecy orders for the court to analyze and determine the extent of injury.[63] The government also emphasized that the constitutionality of the secrecy orders would require a fact-specific, individualized review by the court.[64]

---

address the merits of the government's 12(b)(6) motion to dismiss, only the 12(b)(1) claim for lack of standing. *Infra* Section II.B.

55. Mot. to Dismiss, *supra* note 54, at 2.

56. *Id.* at 2.

57. *Id.* at 8.

58. 499 U.S. 400 (1991).

59. *Id.* at 410–11; Am. Compl., *supra* note 14, at para. 38.

60. Mot. to Dismiss, *supra* note 54, at 6–8.

61. *Id.* at 11.

62. *Id.* at 6. The government also asserts that Microsoft lacks standing "because a favorable judgment would not redress its alleged injury." *Id.* at 8–9. However, that argument is not central to this Comment's analysis.

63. *Id.* at 6.

64. *Id.* at 7–8 ("Section 2705(b) orders are sought in a wide range of investigations and under many different circumstances, and in each instance a court has determined that the requirements of the statute are met and an order of 'appropriate' duration is justified.").

C. Non-Fourth Amendment Standing and Justiciability

To invoke the court's power to resolve a claim, a party is required to show that it has proper standing to sue.[65] Absent standing, a court does not have the authority to reach or decide the merits of the underlying issues.[66] Standing is founded in Article III of the United States Constitution, which limits the role of the federal courts to resolving "cases" and "controversies."[67] This jurisdictional restriction requires that issues presented to the court be "definite and concrete, not hypothetical or abstract."[68] When reaching the merits of a claim would require a court to pass judgment on the constitutionality of the actions taken by another branch of the federal government, the standing requirement must be strictly applied.[69] It is the plaintiff's burden to demonstrate that the requirements of standing have been met for his or her lawsuit to proceed.[70]

The purpose of the standing requirement is to enable truly adverse and personally affected parties to effectively frame the legal issues, litigate the case, and make the court aware of the practical consequences of the outcome.[71] Further, the standing requirement

---

65. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (explaining standing to be "an essential and unchanging part of the case-or-controversy requirement of Article III" of the Constitution); *see also* Soree, *supra* note 25, at 581 (defining standing as "the ability of a given litigant to invoke the powers of the court for relief").

66. *See* Warth v. Seldin, 422 U.S. 490, 498 (1975).

67. U.S. CONST. art. III, § 2, cl. 1; *see* Whitmore v. Arkansas, 495 U.S. 149, 155 (1990) (noting that Article III "serves to identify those disputes which are appropriately resolved through the judicial process").

68. Ry. Mail Ass'n v. Corsi, 326 U.S. 88, 93 (1945); *see* Gov't & Civic Emps. Org. Comm. v. Windsor, 353 U.S. 364, 366 (1957) (per curiam) ("Federal courts will not pass upon constitutional contentions presented in an abstract rather than in a concrete form.").

69. *See* Raines v. Byrd, 521 U.S. 811, 819–20 (1997) ("[T]he law of [Article III] standing is built on a single basic idea—the idea of separation of powers." (quoting Allen v. Wright, 468 U.S. 737, 752 (1984), *abrogated by* Lexmark Int'l, Inc. v. Static Control Components, Inc., 134 S. Ct. 1377 (2014))); *see also* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) ("[T]he power of the Federal Judiciary may not be permitted to intrude upon the powers given to the other branches."). *But see Allen*, 468 U.S. at 790 (Stevens, J., dissenting) ("[T]he Court could be saying that it will require a more direct causal connection when it is troubled by the separation of powers implications of the case before it. That approach confuses the standing doctrine with the justiciability of the issues that respondents seek to raise.").

70. *Lujan*, 504 U.S. at 561.

71. William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 222 (1988); *see* Baker v. Carr, 369 U.S. 186, 204 (1962) (characterizing the "gist" of the standing requirement as whether "the [litigant] alleged . . . a personal stake in the outcome of the controversy").

promotes judicial efficiency by requiring a litigant, after he or she has met the Article III "case or controversy" requirement, to meet additional judicially-created standing requirements.[72]

The Supreme Court set out this strict set of requirements to establish standing in *Lujan v. Defenders of Wildlife*.[73] It articulated a three-part test to determine whether a litigant has proper standing to raise a claim:

> First, the plaintiff must have suffered an "injury in fact"—an invasion of a legally protected interest which is (a) concrete and particularized, and (b) "actual or imminent, not 'conjectural' or 'hypothetical.' Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be "fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court." Third, it must be "likely," as opposed to merely "speculative," that the injury will be "redressed by a favorable decision."[74]

This Comment focuses specifically on the injury in fact requirement for standing.[75]

In *Lujan*, petitioners challenged an amendment limiting the scope of the Endangered Species Act's protection.[76] The Endangered Species Act originally required federal agencies to consult with the Secretary of the Interior regarding agency actions in the United States and abroad to ensure that those actions would not jeopardize endangered species or destroy natural habitats, but the amendment modified the language of the statute so that it only applied "to actions [occurring] within the United States or on the high seas."[77] The Court acknowledged that the "desire to . . . observe an animal species, even for purely esthetic purposes" is a sufficient legal interest for the purpose of establishing standing.[78] However, the petitioners failed to demonstrate that their interest had been or would be harmed by government-funded activities abroad occurring as a result of the

---

72. Soree, *supra* note 25, at 582 n.77.

73. 504 U.S. 555 (1992).

74. *Id.* at 560–61 (citations omitted).

75. The Court has identified several key purposes behind the injury in fact requirement, including, but not limited to (1) restricting access to the judicial process to litigants who will be zealous advocates, (2) giving the right to sue to those personally impacted by a government policy to ensure adequate representation of their interests, and (3) protecting the separation of powers. FALLON ET AL., HART AND WECHSLER'S THE FEDERAL COURTS AND THE FEDERAL SYSTEM 117 (7th ed. 2015) (citations omitted).

76. *Lujan*, 504 U.S. at 557–58.

77. *Id.* at 558. *See generally* 16 U.S.C. §§ 1531–1544 (2012).

78. *Lujan*, 504 U.S. at 562–63.

amendment because "'some day' intentions—without any description of concrete plans . . . do not support a finding of the 'actual or imminent' injury" as required by Article III.[79]

On May 16, 2016, the Supreme Court issued a decision in *Spokeo*, extending the injury in fact requirement to challenges alleging violations of individuals' procedural rights.[80] In that case, an individual claimed that Spokeo, Inc., a company whose website aggregates personal data from the Internet, violated the Fair Credit Reporting Act (FCRA) by publishing false information about his wealth on its website.[81] The Court decided that even though the individual could show a particularized injury from the violation of his statutory rights under the FCRA, a procedural violation on its own is not enough to establish a concrete injury.[82] The Court held that "Article III standing requires a concrete injury even in the context of a statutory violation," and that an allegation of a violation of a procedural right on its own does not "automatically satisf[y] the injury-in-fact requirement."[83] Therefore, at the pleadings stage, a plaintiff must clearly allege an injury in fact that is both concrete *and* particularized.[84] Accordingly, where an individual's procedural or statutory rights have been violated, it has become particularly difficult to plead a sufficient harm to confer standing.

---

79. *Id.* at 564 ("[T]he [petitioners]' profession of an 'inten[t]' to return to the places they had visited before—where they will presumably, this time, be deprived of the opportunity to observe animals of the endangered species—is simply not enough.").

80. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016); *see also* Andrew Hessick, *Establishing Standing After* Spokeo v. Robins, CASETEXT (May 19, 2016), https://casetext.com/posts/establishing-standing-after-spokeo-v-robins (emphasizing that the decision in *Spokeo* changed the law of standing).

81. *Spokeo*, 136 S. Ct. at 1544–46.

82. *Id.* at 1549.

83. *Id.*; *see also* Hessick, *supra* note 80.

84. *Spokeo*, 136 S. Ct. at 1548. "Particularization" requires that an injury "affect the plaintiff in a personal and individual way." *Id.* (citing *Lujan*, 504 U.S. at 560). "Concreteness" requires that an injury "actually exist." *Id.* (citing BLACK'S LAW DICTIONARY 479 (9th ed. 2009)).

D. Fourth Amendment Standing Jurisprudence[85]

*1. Fourth Amendment standing pre-*Rakas v. Illinois

The Supreme Court first dealt directly with the question of Fourth Amendment standing in 1951 in *United States v. Jeffers*.[86] In *Jeffers*, the Court held that an individual had standing to challenge a seizure of contraband narcotics in connection with a search of a hotel room registered to the individual's relatives.[87] In so holding, the Court reasoned that the defendant had a possessory property interest in the drugs.[88] It explained that the defendant was not entitled to have the drugs returned to him because they were contraband, but he did not forfeit his property rights to the drugs for the purposes of the Fourth Amendment.[89]

In 1960, the Court continued to expand its Fourth Amendment standing doctrine. In *Jones v. United States*,[90] it identified other ways someone can bring a Fourth Amendment claim absent a possessory or property interest in the place searched or items seized: (1) the "automatic standing" rule, (2) the "target theory," and (3) the "legitimately on premises" test.[91] The "automatic standing rule" was articulated first by the circuit courts and was adopted by the Supreme Court in *Jones*.[92] In that case, the Court determined that to make an effective showing of standing, a "movant [must] claim either to have owned or possessed the seized property or to have had a substantial possessory interest in the premises searched."[93] The "target theory" was based on the concept that to suppress evidence, someone "must have been a victim of a search or seizure, one against whom the search was directed, as distinguished from one who claims prejudice

---

85. This Comment is only concerned with the Supreme Court's Fourth Amendment standing jurisprudence. Richard Kuhns, an expert on evidence and criminal procedure, has fully discussed Fourth Amendment standing jurisprudence in the lower federal courts. *See generally* Richard B. Kuhns, *The Concept of Personal Aggrievement in Fourth Amendment Standing Cases*, 65 IOWA L. REV. 493, 493 (1980) (noting that after the Supreme Court's decision in *Weeks v. United States*, 232 U.S. 383 (1914), which established the exclusionary rule of evidence, lower federal courts developed various standing requirements to limit the application of the rule).

86. 342 U.S. 48 (1951). Prior to 1951, the Supreme Court had only dealt with Fourth Amendment standing by analogy. *See* Soree, *supra* note 25, at 590–91.

87. *Jeffers*, 342 U.S. at 50, 52–54.

88. *Id.* at 52–54.

89. *Id.* at 54.

90. 362 U.S. 257 (1960), *overruled by* United States v. Salvucci, 448 U.S. 83 (1980).

91. Soree, *supra* note 25, at 592–93.

92. *Jones*, 362 U.S. at 261, 263.

93. *Id.* at 261.

only through the use of evidence gathered as a consequence of a search or seizure directed at someone else."[94] The "legitimately on premises" test was more broad, permitting those who are legally present on the premises where a search or seizure occurs to challenge the legality of the invasion.[95]

2. Impact of Rakas *on Fourth Amendment standing*

In 1978, the Supreme Court held for the first time that an individual litigant cannot assert a claim for a Fourth Amendment violation unless he or she has a legitimate expectation of privacy in the place searched.[96] In *Rakas v. Illinois*,[97] a criminal defendant argued that because police found the evidence serving as the basis for his conviction in his friend's car, it could not be admitted at trial because the search of that car violated the Fourth Amendment.[98] The Court held that passengers have no legitimate expectation of privacy in another individual's automobile and, thus, do not have standing to challenge the search of the automobile.[99] In doing so, the Court completely dismissed the "target" theory from *Jones*, emphasizing that the Fourth Amendment is an individual right that serves to protect the public against unlawful searches or seizures in places where an individual has an expectation of privacy.[100] The *Rakas* decision effectively eliminated standing as an independent inquiry in the Fourth Amendment context and required a substantive inquiry into whether the claim implicates the Fourth Amendment before making a determination on standing.[101]

The Court continued its overhaul of the "automatic standing" rule in *United States v. Salvucci*[102] and *Rawlings v. Kentucky*.[103] In *Salvucci*, two individuals were charged with unlawful possession of stolen mail

94. *Id.*

95. *Id.* at 266–67.

96. *See* Rakas v. Illinois, 439 U.S. 128, 142, 148 (1978); *see also* United States v. Salvucci, 448 U.S. 83, 85 (1980); Rawlings v. Kentucky, 448 U.S. 98, 104 (1980). The question remains, however, whether the fruits of the challenged search or seizure should be excluded from evidence during trial. *See* Soree, *supra* note 25, at 570–71.

97. 439 U.S. 128 (1978).

98. *Id.* at 130.

99. *Id.* at 148.

100. *Id.* at 134–35 ("A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed."); *see also* U.S. CONST. amend. IV, § 1.

101. Soree, *supra* note 25, at 571.

102. 448 U.S. 83 (1980).

103. 448 U.S. 98, 103 (1980).

after the police seized the mail during a search of a family member's apartment.[104] Relying on its decision in *Rakas*, the Court concluded that the individuals did not have a "legitimate expectation of privacy in the invaded place."[105] Moreover, in *Rawlings*, an individual was charged with and convicted for drug trafficking offenses after police found the drugs through an illegal search of another individual's bag.[106] The Court again relied on *Rakas* to conclude that the individual did not have a "legitimate expectation of privacy" in another's bag and therefore was unable to challenge his conviction.[107] This line of cases demonstrates that until very recently, Fourth Amendment standing essentially turned on whether a Fourth Amendment "search" or "seizure" took place and whether the individual's claim met the reasonable expectation of privacy test ("REP test") the Court developed later in *Katz v. United States*.[108]

3. Katz *and Fourth Amendment protection of electronic communications*

The historical Trespass Doctrine articulated a "physical intrusion" requirement for a search or seizure to fall under the purview of the Fourth Amendment—a requirement that cannot be met by intrusions on email and other electronic records.[109] For example, in *Olmstead v. United States*,[110] the Supreme Court rejected the petitioners' claims that wiretapping phone calls violated their Fourth Amendment rights because the government did not physically intrude into the petitioners' homes or offices.[111] Furthermore, and perhaps even more concerning than *Olmstead*, in *Goldman v. United States*,[112] the Supreme Court held that entering the petitioner's office to install a listening device did not constitute a Fourth Amendment violation on the grounds that the trespass did not materially aid in the use of the listening device, despite the fact that the trespass was necessary to install the listening device.[113]

---

104. *Salvucci*, 448 U.S. at 85.
105. *Id.* at 91–92 (quoting *Rakas*, 439 U.S. at 143).
106. 448 U.S. at 100–01.
107. *Id.* at 104.
108. 389 U.S. 347 (1967).
109. *See, e.g.*, Goldman v. United States, 316 U.S. 129, 134–35 (1942) (holding that information heard with a listening device was not illegal due to "trespass or unlawful entry"); Olmstead v. United States, 277 U.S. 438, 457, 464 (1928) ("The insertions were made without trespass upon any property of the defendants.").
110. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347, 352 (1967).
111. *Id.* at 464.
112. 316 U.S. 129, 129 (1942), *overruled by Katz*, 389 U.S. at 352.
113. *Id.* at 134–35.

These decisions are troubling because they demonstrate the Court's unwillingness to extend the Fourth Amendment's protection to electronic means of communication. The Supreme Court did not extend Fourth Amendment protection to electronic communications until *Katz* when the Court established the reasonable expectation of privacy test and determined the threshold question in a Fourth Amendment analysis to be whether law enforcement had conducted a search.[114]

In *Katz v. United States*, the Court moved away from the Trespass Doctrine and instead emphasized the REP test.[115] The Supreme Court in *Katz* held that taping a microphone to a public phone booth for the purpose of listening to calls constituted a search that violated the Fourth Amendment.[116] The Court was less concerned with whether there was a physical intrusion into the phone booth and more concerned with the privacy that a person who used a phone booth would expect.[117] The REP test articulated in *Katz* has two elements: (1) a person must have a subjective expectation of privacy, and (2) society must also be ready and willing to accept that expectation of privacy as reasonable.[118]

Later, the Supreme Court revived the notion of a "physical intrusion" in *United States v. Jones*.[119] To track the movement of a suspected

---

114. *See* Orin Kerr, *Answering Justice Alito's Question: What Makes an Expectation of Privacy "Reasonable"?*, WASH. POST (May 28, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/28/answering-justice-alitos-question-what-makes-an-expectation-of-privacy-reasonable ("On one hand, a search might refer to merely looking for an item . . . . On the other hand, a search might mean the act of observing an item closely . . . . Finally, a search might refer to the physical act of looking through a space in ways that expose its contents to plain view.").

The Supreme Court began to formulate what constitutes a reasonable expectation of privacy as early as 1886, when it indicated that the Fourth Amendment should "apply to all invasions on the part of the government and its employ[ee]s of the sanctity of a man's home and the privacies of life." Boyd v. United States, 116 U.S. 616, 630 (1886).

115. *Id.* at 353.

116. *Id.* at 351, 353.

117. *Id.* at 351–53 ("[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his home or office, is not . . . subject [to] Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (citations omitted)) (overruling, in part, *Olmstead* and *Goldman*'s physical intrusion requirement).

118. *Id.* at 361 (Harlan, J., concurring); *see also* Kerr, *supra* note 114.

In her concurrence in *United States v. Jones*, 132 S. Ct. 945 (2012), Justice Sotomayor advocated for a full adoption of Justice Harlan's test, placing significant value on protecting individuals from violations of a subjectively reasonable expectation of privacy. *See id.* at 954–55 (Sotomayor, J., concurring).

119. 132 S. Ct. 945, 949 (2012).

narcotics trafficker, federal agents placed a GPS tracker on a vehicle registered to the suspect's wife.[120] The federal agents then used the GPS to track the vehicle for twenty-eight days and used the information as the basis for an indictment against the suspect.[121] The Court held that the warrantless[122] installation of a GPS tracker on the vehicle constituted a search that violated the Fourth Amendment.[123] The Court noted that *Katz* did not repudiate the Trespass Doctrine, it merely provided another means to establish a Fourth Amendment violation by recognizing an expectation of privacy in more than just the home.[124]

In defining what constitutes a "reasonable expectation of privacy," the Supreme Court has not been clear.[125] Several members of the Court, in fact, have even gone so far as to expressly recognize the ambiguity of the REP test:

> It involves a degree of circularity . . . and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks . . . . In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant change in popular attitudes.[126]

---

120. *Id.* at 948.

121. *Id.*

122. The government did initially obtain a warrant authorizing the installation of the GPS tracker on the target vehicle within ten days; however, the agents did not install the device until the eleventh day, after the warrant had expired. *Id.*

123. *Id.* at 949.

124. *Id.* at 950–51.

125. Jeremy Fogel, *From the Bench: A Reasonable Expectation of Privacy*, 40 LITIG., Spring 2014, at 1, 1, http://www.americanbar.org/publications/litigation_journal/2013-14/spring/a_reasonable_expectation_privacy.html ("Lay understanding, legal authority, and technological reality often bear little resemblance to each other and are frequently in extreme tension."); Kerr, *supra* note 114; *see* O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (plurality opinion) ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable."); Oliver v. United States, 466 U.S. 170, 177 (1984) ("No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion not authorized by a warrant."); Daniel B. Yeager, *Search, Seizure and the Positive Law: Expectations of Privacy Outside the Fourth Amendment*, 84 J. CRIM. L. & CRIMINOLOGY 249, 280 (1993) (noting that the Court has never clearly defined privacy or provided a set of workable guidelines).

126. *Jones*, 132 S. Ct. at 962 (Alito, J., concurring) (writing for himself and Justices Ginsburg, Breyer, and Kagan).

The *Katz* decision essentially requires that the Supreme Court define (1) privacy and (2) when privacy can reasonably be expected;[127] however, the Court's precedent has not sufficiently defined either.[128] The Supreme Court has instead resorted to drawing lines between invasive practices and less invasive practices, concluding that the former satisfies the REP test and that the latter does not.[129] Part of this inquiry turns on determining "what *should* be a search."[130]

Courts have historically found that, absent special circumstances, the "home" receives the utmost Fourth Amendment privacy protection, and the government must obtain a warrant issued upon probable cause to conduct a search or seizure.[131] Applying Supreme Court precedent to an individual's use of the Internet poses a significant legal issue because Internet users do not have a true "home" in or on the Internet.[132]

*4. Post-*Spokeo *Fourth Amendment standing*

As a result of the Court's decision in *Spokeo*, it is more difficult for plaintiffs alleging procedural rights violations to establish standing.[133] That decision requires that an individual satisfy the concrete harm requirement for standing to assert violations of a procedural right,

---

127. CONSTITUTIONAL CRIMINAL PROCEDURE 105–06 (Andrew E. Taslitz et al. eds., 5th ed. 2014).

128. Generally, the Court has concluded that privacy falls into two categories, but it has failed to provide additional guidance. One commentator described these categories of privacy as follows:

> The privacy at stake covers both *being in private*—doing what one chooses to do, and with whom one chooses, without intrusion—and *having in private*—preserving what one treasures, or merely possesses, unexposed to the world. Both kinds of privacy enable the individual to constitute himself as the unique person he is. Both are aspects of the fully realized life. And both importantly provide conditions for the realization of the common good as well.

Lloyd L. Weinred, *The Fourth Amendment Today*, *in* THE BILL OF RIGHTS: ORIGINAL MEANING AND CURRENT UNDERSTANDING 184, 185–86 (Eugene W. Hickok, Jr. ed., 1991) (emphasis added).

129. *See* Kerr, *supra* note 114.

130. *Id.*

131. Kerr, *supra* note 32, at 1209.

132. *See id.* at 1209–10 ("[It] is really just a block of ones and zeroes stored somewhere on somebody else's computer . . . . Our most private information ends up being sent to private third parties and held far away on remote network servers."); *see also* Webb, *supra* note 40 ("The very nature of email is anti-control and anti-privacy . . . .").

133. *See supra* notes 80–84 and accompanying text.

thereby requiring more than just a particularized, personal harm.[134] As the Court explained, a harm resulting from a procedural rights violation, unlike substantive rights violations, does not necessarily satisfy the injury in fact requirement because procedural violations are more likely to be divorced from a concrete harm.[135] It is unclear what long-term impact the *Spokeo* decision will have on the Fourth Amendment standing doctrine because the decision was only rendered in May of 2016.[136]

Given that the Fourth Amendment largely safeguards procedural rights,[137] *Spokeo* may have a significant impact on Fourth Amendment standing doctrine. The Fourth Amendment's procedural safeguards include "probable cause, judicial oversight of police intrusions," and the warrant particularity requirement.[138] However, the Supreme

---

134. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (noting that particularization is necessary but not sufficient to establish injury in fact); *supra* note 82 and accompanying text (highlighting the distinction between a "concrete" harm and a "particularized" harm).

135. *See Spokeo*, 136 S. Ct. at 1549; *see also* Richard L. Heppner Jr., *Understanding Standing After "*Spokeo v. Robins,*"* LEGAL INTELLIGENCER (June 22, 2016), http://www.thelegalintelligencer.com/id=1202760588959/Understanding-Standing-After-Spokeo-v-Robins (arguing that a "purely procedural failing is not enough" to establish a real injury following *Spokeo*); Hessick, *supra* note 80 (discussing ways in which certain procedural harms can result in concrete injuries).

136. One lower court applying *Spokeo* concluded that there was insufficient evidence to suggest that information obtained through a data breach would be used to the detriment of the victims of the breach. Attias v. CareFirst, Inc., No. 15-cv-00882 (CRC), 2016 WL 4250232 (D.D.C. Aug. 10, 2016). On the other hand, the Sixth Circuit concluded that it would be "unreasonable to expect Plaintiffs to wait for actual misuse" of their data "before taking steps to ensure their own personal . . . security." Galaria v. Nationwide Mut. Ins. Co., Nos. 15-3386/3387, 2016 WL 4728027 (6th Cir. Sept. 12, 2016).

One legal commentator has suggested that the "actual harm" requirement is a "significant development" that could "bring some measure of relief to companies tasked with storing vast quantities of consumer data." John Devine et al., *Plaintiffs Cannot Bring Data Breach Lawsuits Without Evidence that Information Will Be Used to Harm*, JD SUPRA BUS. ADVISOR (Aug. 17, 2016), http://www.jdsupra.com/legalnews/plaintiffs-cannot-bring-data-breach-15526.

Justices Blackmun and O'Connor predicted this interpretation issue following the Court's decision in *Lujan*. They feared that "the Court [sought] to impose fresh limitations on the constitutional authority of Congress to allow citizen suits in the federal courts for injuries deemed 'procedural' in nature," Lujan v. Defs. of Wildlife, 504 U.S. 555, 589–90 (Blackmun, J., dissenting) (1992), and noted that "[o]nly later cases [would] tell what the Court [meant] by its intimation that 'procedural' injuries are not constitutionally cognizable injuries," *id.* at 602.

137. *See* Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 199 (1993).

138. *Id.*

Court has often found that the Fourth Amendment serves to protect a greater—and substantive—right to privacy.[139]

The American people have long regarded the sharing of personal data to be harmful in itself, even moreso than a mere procedural violation of the Fourth Amendment.[140] Congress has repeatedly passed bills and enacted statutes to protect individuals from the uncalled-for disclosure of their personal information.[141] It follows that sharing information pursuant to an unreasonable search or seizure of personal information or communications to a federal agency could cause an additional, substantive harm.

The *Spokeo* Court issued its decision in the context of a violation of the FCRA, a statute enacted in part to ensure the privacy of personal information shared with credit reporting agencies.[142] Similarly, in *Attias v. CareFirst, Inc.*,[143] insurance policyholders sued after a data breach resulted in the release of their "names, birth dates, email addresses, and subscriber identification numbers."[144] The U.S. District Court for the District of Columbia held that, despite the company's alleged failure to safeguard its policyholders' personal information as required by statute,[145] there was not a sufficient injury in fact to justify standing because the policyholders' information was not actually misused by the perpetrators of the data hack.[146]

---

139. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (finding that the "penumbras" of the First, Fourth, Fifth, and Ninth Amendments together "create zones of privacy"); Mapp v. Ohio, 367 U.S. 643, 656 (1961) (stating that the Fourth Amendment right to privacy is "no less important than any other right carefully and particularly reserved to the people").

140. *See Public Opinion on Privacy*, ELEC. INFO. PRIVACY CTR., https://epic.org/privacy/survey (last updated Jan. 26, 2017) (noting that individuals wish to have control over their personal information and that privacy laws were strengthened to "protect their personal information from the government and commercial entities"). *But see* Cheryl Conner, *Sharing Too Much? It'll Cost You*, FORBES (Oct. 19, 2012, 9:11 AM), http://www.forbes.com/sites/cherylsnappconner/2012/10/19/sharing-too-much-itll-cost-you (exemplifying how much data individuals share online through social media platforms).

141. *See supra* note 5 (providing examples of the bills and statutes enacted to protect personal information).

142. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1540 (2016).

143. No. 15-cv-00882 (CRC), 2016 WL 4250232 (D.D.C. Aug. 10, 2016).

144. *Id.* at *1 (noting that social security numbers were not the subject of the data breach). If social security numbers had been shared, then perhaps the injury would have at least been closer to sufficient. The court did not explicitly discuss that scenario, however.

145. *Id.*

146. *Id.* at *2 ("'[A]llegations of *possible* future injury' do not satisfy constitutional standing requirements." (quoting Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138,

If courts do not regard the mere sharing of personal data as a sufficient injury in fact to establish standing, a Fourth Amendment claim post-*Spokeo* will likely require a more significant harm than a warrantless search or seizure alone. A court would likely find that an individual has not suffered an injury in fact until the fruits of an improper search or seizure are used against him or her, resulting in criminal proceedings, civil sanctions, denial of immigration benefits, or another similarly substantial harm.[147]

5. Case study: Clapper v. Amnesty International USA

Clapper v. Amnesty International USA[148] serves as a fairly recent example of the Supreme Court's Fourth Amendment standing jurisprudence. Amnesty International USA ("AI"), a human rights organization, facially challenged the constitutionality of a provision of the Foreign Intelligence Surveillance Act (FISA)[149]—another provision of the ECPA—allowing electronic surveillance that serves foreign intelligence and national security purposes without notice to the subject of surveillance.[150] AI suggested that there was an "objectively reasonable likelihood" that its communications with foreign actors would be intercepted in the future pursuant to this provision of FISA.[151] The Supreme Court found that this hypothetical future harm was insufficient to establish standing to raise a Fourth Amendment claim even though AI would be unable to later prove that they were the subjects of wiretapping due to the secret nature of the FISA surveillance program.[152] The Court noted that "[t]he

---

1147 (2013))); *see also Spokeo*, 136 S. Ct. at 1548 (noting that a violation of a right in itself "concern[s] particularization, not concreteness").

147. *See* United States v. Salvucci, 448 U.S. 83 (1980); Rawlings v. Kentucky, 448 U.S. 98 (1980); Rakas v. Illinois, 439 U.S. 128 (1978); *see also* Soree, *supra* note 25, at 582 ("[A]ny defendant seeking to suppress unlawfully obtained evidence arguably has [met her Article III burden] . . . .").

148. 133 S. Ct. 1138 (2013).

149. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a (2012).

150. *Clapper*, 133 S. Ct. at 1142.

151. *Id.* at 1147.

152. *Id.* at 1148–49 (remarking that respondents did not have standing based on a "highly attenuated chain of possibilities"). The Court found it "speculative" that (1) the government would target the parties that AI was in communication with, (2) the government would rely on the challenged section of FISA to monitor the communications, (3) the Foreign Intelligence Surveillance Court would authorize the surveillance, (4) the surveillance would correctly intercept the intended communications, and (5) that AI's communications would be part of the intercepted communications. *Id.* at 1148–50. For further discussion on standing to litigate

assumption that if respondents have no standing to sue, no one would have standing, is not a reason to find standing."[153] This language is significant because this reasoning does not provide an opportunity to bring a Fourth Amendment challenge unless an individual can prove a concrete, personal injury.

Similarly, in *United States v. Richardson*,[154] an individual lacked standing to challenge the CIA's actions under Article I, Section 9, Clause 7 of the Constitution requiring "a regular Statement and Account of the Receipts and Expenditures of all public Money"[155] because it constituted a "generalized grievance."[156] The Court said,

> It can be argued that if respondent is not permitted to litigate this issue, no one can do so. In a very real sense, the absence of any particular individual or class to litigate these claims gives support to the argument that the subject matter is committed to the surveillance of Congress, and ultimately to the political process.[157]

Even though Richardson was not decided in the Fourth Amendment context, the case serves to highlight the underlying separation of powers concerns associated with the Court's standing inquiry.

II. MICROSOFT'S OPTIONS FOR ASSERTING THIRD-PARTY STANDING

"More than 120 years after Justice Bradley's call to vigilance against 'stealthy encroachments,' the federal government has more than taken its first steps towards crossing the constitutional boundaries of the people's right to privacy; it has walked for miles."
—Nadia B. Soree[158]

A. Third-Party Standing

In general, a plaintiff may not rely upon the legal rights of others when asserting a claim for relief.[159] An organization or another similar third party, however, has the capacity to bring a legal claim on

---

under FISA, see Ben Cook, *The New FISA Court Amicus Should Be Able to Ignore Its Congressionally Imposed Duty*, 66 AM. U. L. REV. 539, 549–50 (2016).

153. *Clapper*, 133 S. Ct. at 1154 (alteration in original) (quoting Valley Forge Christian Coll. v. Ams. United for Separation of Church and State, Inc., 454 U.S. 464, 489 (1982)).

154. 418 U.S. 166 (1974).

155. U.S. CONST. art. I, § 9, cl. 7.

156. *Richardson*, 418 U.S. at 176.

157. *Id.* at 179.

158. Soree, *supra* note 25, at 570.

159. Warth v. Seldin, 422 U.S. 490, 499 (1975); *see* Soree, *supra* note 25, at 582–83. This concept dates back to the early 1900s and the Supreme Court's decision in *Tyler v. Judges of the Court of Registration*, 179 U.S. 405 (1900), in which the Court noted that a plaintiff is "bound to show an interest in the suit personal to himself." *Id.* at 406.

behalf of others under certain circumstances.[160] Various courts have recognized that both state and private actors, in addition to traditional voluntary membership organizations, can assert the rights of others in the court.[161] Yet the courts apply a more exacting standard for establishing standing when a third-party, rather than an individual, seeks to assert individual rights.[162]

1. Powers v. Ohio *test for individual third-party standing*

The Supreme Court in *Powers v. Ohio* explained when a third-party individual may raise a vicarious claim on behalf of an injured party. In that case, a criminal defendant was able to challenge his own conviction by raising an Equal Protection claim on behalf of a juror who had been excluded from the trial on the basis of his race in a peremptory challenge by the prosecutor.[163] The Court emphasized that the "discriminatory use of peremptory challenges" results in a direct harm to a criminal defendant, and the defendant has a legitimate interest in challenging the practice.[164] It reasoned that the criminal defendant and juror are sufficiently closely related such that the criminal defendant would be a worthy advocate on behalf of the juror.[165] Moreover, the Court recognized that even though jurors

160. *See, e.g.*, Abigail All. for Better Access to Developmental Drugs v. Eschenbach, 469 F.3d 129, 132 (D.C. Cir. 2006) (permitting a non-profit organization to file suit on behalf of its terminally ill members, challenging a provision of the Food, Drug, and Cosmetic Act that made it difficult for terminally ill patients to access experimental drugs).

161. *See, e.g.*, Virginia v. Am. Booksellers Ass'n, 484 U.S. 383, 392–93 (1988) (permitting a bookstore to preemptively raise a First Amendment claim on behalf of booksellers); Hunt v. Wash. State Apple Advert. Comm'n, 432 U.S. 333, 345 (1977) (holding that a state agency had standing to raise a claim on behalf of Washington apple growers and dealers); Craig v. Boren, 429 U.S. 190, 194–95 (1976) (authorizing a beer vendor to assert an Equal Protection claim for males not allowed to purchase beer prior to turning twenty-one); *In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 258 (D.D.C. 2003) (clarifying that Verizon was "an adequate advocate to assert the First Amendment rights of its subscribers"), *rev'd on other grounds sub nom.* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1239 (D.C. Cir. 2003).

162. *See* cases cited *supra* note 161 (applying more specific standards for establishing third-party standing, such as an "actual and well-founded fear" that a law will be enforced against a plaintiff, a "financial nexus" between the interests of the third party and its constituents, third-party standing, and First Amendment chilling effect).

163. 499 U.S. 400, 403, 411 (1991) (noting that standing has been permitted in the criminal context where defendants challenge their convictions by asserting the rights of third parties or where raising a third party's rights would prevent future prosecution).

164. *Id.* at 411.

165. *Id.* at 413.

excluded on the basis of race do have the ability to bring a lawsuit on their own behalf,[166] such challenges are unlikely.[167]

The *Powers* Court went on to articulate the following third-party standing test:

> The litigant must have suffered an "injury in fact," thus giving him or her a "sufficiently concrete interest" in the outcome of the issue in dispute; the litigant must have a close relation to the third party; and there must exist some hindrance to the third party's ability to protect his or her own interests.[168]

Almost all applications of the *Powers* test have been in the context of criminal justice or immigration law[169] and have not involved a company or organization bringing a constitutional challenge on behalf of its clients or members.

2. Hunt v. Washington State Apple Advertising Commission *test for organizational third-party standing*

To assert standing as a third-party organization, the party must show a significant personal stake in the outcome of a claim to justify finding jurisdiction in a federal court.[170] For example, in *Hunt v. Washington State Apple Advertising Commission*,[171] Washington State apple growers challenged the constitutionality of a North Carolina Board of Agriculture regulation requiring all apples shipped into North Carolina to display the USDA grade or nothing.[172] Because the Washington State apple growers' standards were higher than the USDA standards, the Washington State apple growers were at a disadvantage in North Carolina.[173] The Supreme Court held that the Washington State Apple Advertising Commission had standing to challenge the regulation because (1) the growers could not use their pre-printed packages displaying the apple type and Washington grade

166. *Id.* at 414 (citing Carter v. Jury Comm'n of Greene Cty., 396 U.S. 320, 329–30 (1970)).

167. *Id.*

168. *Id.* at 411 (citations omitted).

169. *See, e.g.*, Miller v. Albright, 523 U.S. 420, 433 (1998) (holding that an illegitimate daughter had standing to bring an Equal Protection challenge to a statute governing the citizenship of illegitimate children on behalf of her citizen father); Harris v. Evans, 20 F.3d 1118, 1120, 1125 (11th Cir. 1994) (ruling that a prison inmate was unable to assert a guards' First Amendment rights to speak with the parole board).

170. Nat'l Taxpayers Union, Inc. v. United States, 68 F.3d 1428, 1433 (D.C. Cir. 1995) (citing Havens Realty Corp. v. Coleman, 455 U.S. 363, 378–79 (1982)).

171. 432 U.S. 333 (1977).

172. *Id.* at 336–37.

173. *Id.*

without forgoing the ability to sell Washington apples in North Carolina, (2) it was the Commission's job to "protect[] and enhanc[e] the market for Washington apples," and (3) an interstate commerce claim does not require the participation of the growers themselves.[174]

The three-part standing test that the Supreme Court articulated in *Hunt* is as follows: (1) at least one member of the organization must satisfy the requirements for individual standing; (2) the interests that the organization seeks to protect must be related to the organization's purpose; and (3) the claim cannot require that an individual member of the organization participate in the lawsuit, meaning no single injured party can be the lynchpin of the cause of action.[175] Unlike the *Powers* test, the *Hunt* test does not consider whether the individuals in the organization have the ability to raise a claim and protect their rights themselves, but instead, it prohibits standing where the claim and recovery would require individual participation in the lawsuit.[176]

Although the *Hunt* test has traditionally applied to organizations with a member-like constituency,[177] the purpose of this test is to ensure that the organization can adequately represent and protect the interests of any harmed constituents.[178] One strong indicator of a sufficient relationship to confer standing is whether the outcome of the litigation could negatively affect the interests of the organization.[179]

Even though courts have not always expressly invoked the *Hunt* test to determine a party's standing, they have applied similar principles and justifications to confer standing on corporations.[180] For example,

---

174. *Id.* at 343–44.

175. *Id.* at 342–43 ("So long as . . . the relief sought does not make the individual participation of each injured party indispensable to proper resolution of the cause, the association may be an appropriate representative of its members, entitled to invoke the court's jurisdiction.") (quoting Warth v. Seldin, 422 U.S. 490, 511 (1975)); *see also* United Food & Commercial Workers Union Local 751 v. Brown Grp., Inc., 517 U.S. 544, 557 (1996) (elucidating that the first two prongs are constitutional requirements for standing and the third prong is a judicially-created prudential limitation); Sierra Club v. EPA, 292 F.3d 895, 898 (D.C. Cir. 2002) (reciting the same three-part test).

176. *Hunt*, 432 U.S. at 343.

177. *Id.* at 344–45 (noting that "indicia of membership in an organization," like electing members of the board or commission and financing its activities, are enough to establish a sufficient relationship between parties to confer standing).

178. *See id.* at 345 (concluding that the Commission represented, protected, and expressed the views of the state's apple growers).

179. *See id.* (noting a "financial nexus" between the Commission and its constituents).

180. *See, e.g.*, *supra* Section II.A.2 (discussing the Supreme Court's decision to confer standing on the Washington State Apple Advertising Commission because the

in *In re Verizon Internet Services, Inc.*,[181] the U.S. District Court for the District of Columbia applied a similar rationale in concluding that Verizon had standing to bring a First Amendment challenge to the Digital Millennium Copyright Act on behalf of its Internet subscribers.[182] The court determined that the relationship between Verizon and its customers was such that Verizon would be able to adequately raise "concrete and sharply presented" customer grievances.[183] The court went on to recognize that Verizon had a significant interest in the litigation because a failure to protect its customers' rights could "affect Verizon's ability to maintain and broaden its client base."[184]

B. Raising a Fourth Amendment Claim as a Third Party

The Supreme Court has held that a Fourth Amendment violation cannot be raised vicariously because it is strictly an individual right.[185] Accordingly, only an individual whose Fourth Amendment rights have been allegedly violated can make a claim for relief upon those rights.[186]

III. MICROSOFT INCORRECTLY RELIES ON THE *POWERS* TEST TO ESTABLISH STANDING AND SHOULD HAVE INSTEAD RELIED ON THE *HUNT* TEST

"[T]he defense of privacy follows, and never precedes, the emergence of new technologies for the exposure of secrets . . . . [T]he case for privacy always comes too late."
—Jill Lepore[187]

Commission was responsible for protecting apple growers and its claim did not require their participation).

181. 257 F. Supp. 2d 244 (D.D.C. 2003), *rev'd on other grounds sub nom.* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1239 (D.C. Cir. 2003).

182. *Id.* at 257–58.

183. *Id.* at 258.

184. *Id.*

185. Rakas v. Illinois, 439 U.S. 128, 133–34 (1978) ("Fourth Amendment rights are personal rights which . . . may not be vicariously asserted." (quoting Alderman v. United States, 394 U.S. 165, 174 (1969))); *accord* Steagald v. United States, 451 U.S. 204, 219 (1981) ("[R]ights such as those conferred by the Fourth Amendment are personal in nature . . . ."), *reh'g granted*, 664 F.2d 1241 (1981).

186. Moreland v. Las Vegas Metro. Police Dep't, 159 F.3d 365, 369 (9th Cir. 1998); *see Rakas*, 439 U.S. at 134 ("A person who is aggrieved by an illegal search . . . of a third person[] . . . has not had any of his Fourth Amendment rights infringed.").

187. *The Prism*, NEW YORKER (June 24, 2013), http://www.newyorker.com/magazine/2013/06/24/the-prism.

A. Microsoft Incorrectly Relies on Powers v. Ohio *to Assert Its Standing to Raise a Fourth Amendment Claim on Behalf of Its Customers*

Microsoft improperly relies upon the *Powers* test under third-party current standing doctrine for individuals to assert its standing to bring a Fourth Amendment challenge to the SCA on behalf of its customers and should have instead relied upon the test articulated by the Supreme Court in *Hunt* regarding organizational standing. Neither party addresses the *Hunt* case in their briefs before the court.[188] Despite the lack of discussion about the *Hunt* case and the government's failure to refute Microsoft's reliance on *Powers*, it is unclear whether Microsoft has standing to bring its Fourth Amendment challenge to the SCA because the court may raise standing issues sua sponte.[189]

Microsoft applied the *Powers* test and argued (1) that the government's actions have damaged the company's business interest in protecting its customers' privacy and maintaining customer trust,[190] (2) that the relationship between a service provider and its customers is sufficiently close to justify raising a vicarious claim under *Powers*,[191] and (3) that Microsoft's customers are not able to assert their own interests because they are unaware that a search or seizure of their data has occurred due to the nature of the government's actions under sections 2703 and 2705 of the SCA.[192] Microsoft's argument is compelling, particularly concerning its customers' inability to raise

188. *See generally* Am. Compl., *supra* note 14; Mot. to Dismiss, *supra* note 54; Microsoft's Opposition to Government's Motion to Dismiss, Microsoft Corp. v. U.S. Dep't of Justice, No. 2:16-cv-00538-JLR, 2016 WL 4734703 (W.D. Wash. filed Aug. 26, 2016) [hereinafter Pl.'s Opp'n].

189. Because standing relates to a court's subject matter jurisdiction and the overall justiciability of a case, a court may raise such issues sua sponte without full briefings from the parties. Adam A. Milani & Michael R. Smith, *Playing God: A Critical Look at Sua Sponte Decisions by Appellate Courts*, 69 TENN. L. REV. 245, 248 (2002).

190. Am. Compl., *supra* note 14, at para. 39.

191. *Id.* (citing *In re* Verizon Internet Servs., Inc., 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 sub nom.* Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1239 (D.C. Cir. 2003)).

192. *Id.*; *cf.* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1154 (2013) (denying respondents' argument that the nature of FISA wiretaps would fail to provide notice to the targets of the search because if the government decides to use the information from a search, it must notify the affected person first).

their own Fourth Amendment challenges; however, the company has applied the wrong test.[193]

Microsoft's attempt to assert its customers' Fourth Amendment rights vicariously in its challenge to the SCA is not even remotely analogous to *Powers*. In *Powers*, a criminal defendant challenged his own conviction by raising an Equal Protection claim on behalf of one of the jurors excluded from the trial on the basis of race.[194] Courts have applied the *Powers* test primarily in the criminal law and immigration contexts,[195] not to corporations or other companies bringing a constitutional challenge on behalf of their customers. Furthermore, the harm required of a *Powers* plaintiff is much more significant than that required under *Hunt*—the criminal defendant in *Powers* had a personal stake in his own liberty. While courts have found that corporations do have an interest in customer retention,[196] courts place an exceedingly high value on a criminal defendant's ability to challenge his conviction by raising the rights of others.[197]

Microsoft should instead have relied upon the test articulated in *Hunt* to establish standing of a third-party *organization*.[198] Microsoft's position as a cloud service provider in a business-customer

193. In its response, Microsoft suggests that the government has conceded that *Powers* is the controlling framework to determine standing. *See* Pl.'s Opp'n, *supra* note 188, at 17. However, because standing goes to subject matter jurisdiction, a court may address the issue sua sponte.

194. Powers v. Ohio, 499 U.S. 400, 410–12 (1991).

195. *See, e.g.*, Miller v. Albright, 523 U.S. 420 (1998) (holding that an illegitimate daughter had standing to bring an Equal Protection challenge to a statute governing the citizenship of illegitimate children on behalf of her citizen father); Harris v. Evans, 20 F.3d 1118, 1120, 1125 (11th Cir. 1994) (ruling that a prison inmate was unable to assert a guard's First Amendment rights to speak with the parole board).

196. *See, e.g.*, *In re Verizon*, 257 F. Supp. 2d at 258 (recognizing that "Verizon has a vested interest in vigorously protecting [the rights of its customers] 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 Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003).

197. *See Powers*, 499 U.S. at 414 ("Petitioner has much at stake in proving that his jury was improperly constituted due to an [E]qual [P]rotection violation, for we have recognized that discrimination in the jury selection process may lead to the reversal of a conviction."). In its filings, Microsoft indicated that its "customer trust" has been harmed, but it did not provide any evidence suggesting that it has actually lost customers as a result. *See* Am. Compl., *supra* note 14, at para. 39; Pl.'s Opp'n, *supra* note 188, at 17–18. The Court has repeatedly found that criminal defendants may raise the rights of third parties in challenging their own convictions. *See, e.g.*, Eisenstadt v. Baird, 405 U.S. 438, 443–46 (1972); Griswold v. Connecticut, 381 U.S. 479, 481 (1965); McGowan v. Maryland, 366 U.S. 420, 429–30 (1961).

198. *See* Hunt v. Wash. State Apple Advert. Comm'n, 432 U.S. 333, 342–43 (1977); *supra* note 175 and accompanying text (articulating the *Hunt* three-part test).

relationship is analogous to that of an organization's relationship with its voluntary members because this relationship implies that the business has the ability to adequately represent the interests of the harmed customers sufficient to justify conferring standing.[199] Specifically, Microsoft has an important business interest at stake in the litigation because a decision upholding the constitutionality of sections 2703 and 2705 of the SCA stands to threaten customer confidence in and reliance on Microsoft's cloud-storage solutions,[200] thereby damaging its ability to attract and retain customers. This "privacy" or "security" nexus is similar to the "financial nexus" between the third-party organization and its constituents in *Hunt*.[201] Because Microsoft stands to lose business on account of the government's use of secrecy orders in conjunction with no-notice warrants, Microsoft has the motivation and ability to serve as a zealous advocate of its customers' rights; therefore, the *Hunt* test—as it applies to third-party organizations and other similar entities—is appropriate for *Microsoft Corp.* Under the *Hunt* test, however, Microsoft's standing argument still likely fails.

B. Microsoft Likely Does Not Have Standing Under the Current Hunt *Test*

1. Microsoft likely fails to satisfy the first prong of the Hunt *test*

The *Hunt* test requires that at least one member of the organization must have standing to sue in his or her own right.[202] While there is conclusive evidence in *Microsoft Corp.* that the government's actions constituted a search—thus implicating the Fourth Amendment[203]—there is no evidence in the record before the court that would suggest a Microsoft customer has suffered a sufficient injury in fact as a result of the search to confer standing to

---

199. *See In re Verizon*, 257 F. Supp. 2d at 258 (citing Virginia v. Am. Booksellers Ass'n, 484 U.S. 383, 392–93 (1988)); Dep't of Labor v. Triplett, 494 U.S. 715, 720 (1990); Sec'y of State of Md. v. Joseph H. Munson Co., 467 U.S. 947, 958 (1984); Craig v. Boren, 429 U.S. 190, 194–97 (1976)).

200. *See* Am. Compl., *supra* note 14, at para. 5. For a discussion about the negative impact of the government's use of secrecy orders on Microsoft's cloud storage business, see *supra* notes 43–51 and accompanying text.

201. *Hunt*, 432 U.S. at 345.

202. *Id.* at 343.

203. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining that Fourth Amendment violations require a showing of an actual expectation of privacy and that the expectation is one held by society to be reasonable).

raise a Fourth Amendment challenge to sections 2703 and 2705 of the SCA.[204]

a. The government's actions under sections 2703 and 2705 of the SCA constitute a search implicating the Fourth Amendment

Before addressing whether a Microsoft customer has standing to sue in his own right, the Fourth Amendment standing doctrine mandates a reasonable expectation of privacy inquiry to determine whether the legal question implicates the Fourth Amendment.[205] This requires determining (1) whether Microsoft's customers had a subjectively reasonable expectation of privacy in their communications stored on the cloud and (2) whether society as a whole recognizes their subjective expectation of privacy as reasonable.[206]

Microsoft's customers likely did have a subjective expectation of privacy, and society is likely ready to recognize that expectation as reasonable. Most Americans believe email and other stored communications and documents should be protected in the same fashion as phone calls and snail mail letters.[207] On the other hand, email has never been an entirely secure method of communication with emails stored on the sender's computer, on the Internet service provider's cloud service, and on the recipient's computer,[208] thereby diminishing the expectation of privacy for emails. The expectation of privacy has also evolved with technological developments. As Justice Murphy noted more than seventy years ago, "the search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment."[209] Determining what constitutes a privacy invasion is not straightforward, and popular attitudes about privacy inevitably

204. *See generally* Am. Compl., *supra* note 14; Pl.'s Opp'n, *supra* note 188.

205. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

206. *See id.* As an alternative to the reasonable expectation of privacy test, Jim Harper of the Cato Institute would engage in a factual inquiry to determine whether "the individual claiming Fourth Amendment protection *actually* [had] privacy." Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1398 (2008).

207. *See* Benson, *supra* note 40. *But see* Melissa Medina, Note, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 268 (2013) (noting that Google's assertion that its email subscribers did not have a reasonable expectation of privacy in its communications was consistent with well-established law).

208. *Email Privacy Concerns*, FINDLAW, http://files.findlaw.com/pdf/consumer/consumer.findlaw.com_online-scams_email-privacy-concerns.pdf (last visited Feb. 5, 2017).

209. Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting).

shift as the boundaries between home, office, and public space continue to gray.[210] Therefore, it is not unreasonable to conclude that Microsoft's customers expected that their emails were conversations kept between themselves and their recipients;[211] moreover, society would recognize that expectation as reasonable given the major shift in access to similar technologies.

b. Microsoft's customers likely have not suffered a sufficient injury in fact to raise a claim themselves

To establish standing to raise a Fourth Amendment claim post-*Spokeo*, a Microsoft customer must identify a harm that is both concrete *and* particularized. In this case involving government investigations,[212] he or she would likely need to show that the disclosure of cloud-based personal information to the government under sections 2703 and 2705 of the SCA resulted in an indictment, criminal proceedings, denial of immigration benefits, or another significant harm.[213] After *Spokeo*, the sharing of personal data and information does not immediately result in an injury in fact sufficient to confer standing; the sharing of personal data and information only satisfies the *particularized*, personal harm requirement.[214] A plaintiff could not show a *concrete* harm until the disclosed information was used in a negative or harmful way against the individual.[215]

The facts alleged in the record before the court do not suggest that the government's use of no-notice warrants and secrecy orders under sections 2703 and 2705 of the SCA have led to any of Microsoft's customers being subject to legal proceedings related to the information that the government obtained through the search or seizure.[216] It is possible that a Microsoft customer may be in such a

---

210. *See supra* notes 125–32 and accompanying text.

211. Kerr, *supra* note 32, at 1209 (noting that an Internet user may consider online storage space as a "virtual home" that receives Fourth Amendment protections).

212. *See supra* notes 30–34 and accompanying text.

213. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547–50 (2016); *see also* Attias v. CareFirst, Inc., No. 15-cv-00882, slip op. at 1, 11–12 (D.D.C. Aug. 10, 2016); Soree, *supra* note 25, at 570–71; *supra* notes 82–84 and accompanying text; *supra* notes 137–41 and accompanying text (explaining that chances are high that *Spokeo* will be the most significant for cases involving procedural rights).

214. For a discussion on the difference between a concrete harm and a particularized harm, see *supra* note 84.

215. *See id.*

216. *See generally* Am. Compl., *supra* note 14. This is also similar to *California Bankers Association v. Shultz*, 416 U.S. 21 (1974), in which the Court denied standing to bank customers who could not show that information about their personal

position, especially considering that emails are a common form of evidence used in "commercial litigation and white-collar criminal cases."[217] However, given that Microsoft has the burden of demonstrating its standing to sue, this hypothetical situation is not sufficient to meet the requirement that at least one Microsoft customer have standing to sue in his own right.[218]

2. Microsoft fulfills the requirements of the second prong of the Hunt *test*

The *Hunt* test as applied to corporations would also require that the corporation's interest in litigating a claim be related to the subject matter in which the corporation has relevant experience or expertise.[219] In seeking to protect its customers' Fourth Amendment rights, Microsoft claims that it improves trust among its customers as a cloud storage provider.[220] As reliance on digital technology in business has increased, companies that do not prioritize the security of their customers' personal data have lost "customers' goodwill—and their business."[221] Moreover, while merely asserting its customers' Fourth Amendment rights will likely increase customer faith in Microsoft, it does nothing to increase confidence in the cloud as a service. Absent a successful lawsuit, Microsoft argues that the government's continued practices under sections 2703 and 2705 of the SCA have the potential to reduce confidence in the cloud as a whole, thereby potentially reducing its cloud customer base.

It is unclear whether the "germane to its purpose" prong would require that Microsoft have a demonstrated long-standing interest in protecting customer privacy to establish standing. It could be argued that Microsoft has only recently taken an interest in its customers' data privacy and has struggled to establish and maintain customer trust over the years.[222] However, Microsoft has recently taken a

---

financial transactions had been reported under the Treasury Department regulations. *Id.* at 67–68.

217. *See* Jason Knott, *Email and the Business Records Exception*, A.B.A. SEC. LITIG. (Sept. 25, 2013), http://apps.americanbar.org/litigation/committees/trialpractice/articles/summer2013-0913-email-and-business-records-exception.html.

218. *See* Lujan v. Defs. of Wildlife, 504 U.S. 555, 562 (1992).

219. Hunt v. Wash. State Apple Advert. Comm'n, 432 U.S. 333, 342–43 (1977).

220. Am. Compl., *supra* note 14, at para. 39.

221. Morey et al., *supra* note 13.

222. *See, e.g.*, Tom Warren, *EFF Blasts Microsoft over Windows 10 Privacy Concerns*, VERGE (Aug. 22, 2016, 7:18 AM), http://www.theverge.com/2016/8/22/12582622/eff-microsoft-windows-10-privacy-concerns (noting that "Windows 10 sends an unprecedented amount of usage data back to Microsoft" and that there is a clear "trust issue").

hardline approach to improving customer trust and ensuring its customers' privacy, and it established the "Microsoft Trust Center" to emphasize its dedication to security.[223] Even if there is a lack of historical dedication to privacy, Microsoft has transformed itself into a company that is incredibly devoted to protecting customer privacy, likely satisfying the requirement that Microsoft's interest in the litigation be essential to its operation as a cloud service provider.

3. Microsoft fails to satisfy the third prong of the Hunt *test*

The *Hunt* test also provides that a claim must be able to proceed without individual participation in the lawsuit.[224] Because *Rakas* held that a Fourth Amendment claim may not be raised vicariously by anyone aside from the individual whose rights were violated[225] a Microsoft customer whose data has been accessed by the government under sections 2703 and 2705(b) likely must participate in the lawsuit. Moreover, because Microsoft cannot satisfy the first prong of the *Hunt* test absent facts demonstrating that a Microsoft customer has suffered a sufficient injury in fact,[226] Microsoft's lawsuit would require proof that an individual Microsoft customer has faced a negative impact as a result of the government search.

Microsoft relies heavily on *In re Verizon Internet Services* to suggest that the company has standing to raise a Fourth Amendment claim on behalf of its customers.[227] However, while *In re Verizon Internet Services* serves as an example of a corporation having standing on behalf of its customers,[228] the context of the law suit makes a significant difference. In *In re Verizon Internet Services*, the D.C. District Court found that Verizon had standing to bring a *First Amendment* challenge on behalf of its customers.[229] Notably, courts are more likely to strictly adhere to the "prudential limitations on standing" in

223. *See, e.g.*, Microsoft Trust Center, *Responding to Government and Law Enforcement Requests to Access Customer Data*, https://www.microsoft.com/en-us/TrustCenter/Privacy/Responding-to-govt-agency-requests-for-customer-data (last visited Feb. 5, 2017); *Why Businesses Can Trust Office 365 with Their Data*, BIZTECH (Aug. 18, 2016), http://www.biztechmagazine.com/article/2016/08/why-businesses-can-trust-office-365-their-data (noting Microsoft's additional efforts to enhance consumer trust through a prioritization of security and collaboration with third-party software).

224. *Hunt*, 432 U.S. at 342–43.

225. *See* Rakas v. Illinois, 439 U.S. 128, 133–34 (1978).

226. *Supra* Section III.B.1.b.

227. Am. Compl., *supra* note 14, at para. 39.

228. *Supra* notes 181–84 and accompanying text.

229. *In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 258 (D.D.C. 2003).

Fourth Amendment cases than in First Amendment cases;[230] therefore, *In re Verizon Internet Services* is likely not controlling.

C. Justice Requires the Adoption of a New Relaxed Hunt *Test to Determine General Third-Party Standing Under the Fourth Amendment*

Despite the Supreme Court's ruling in *Spokeo*, the Court should firmly establish the unauthorized disclosure of personal data and information as a search implicating the Fourth Amendment and as a harm that is both concrete and particularized.[231] Otherwise, individuals who have been the subject of a government investigation will find themselves unable to raise a Fourth Amendment challenge until after the information has been disclosed, subjecting them to an even greater harm.

Moreover, the Court should depart from its long-held policy that a Fourth Amendment claim cannot be raised vicariously. Otherwise, outdated and inadequate standing doctrines will prevent challenges over whether existing statutes should apply to new forms of private information—including third-party electronic communications—that implicate the Fourth Amendment. To combat these issues, the Court should blend the *Hunt* and *Powers* tests and adopt the following test for third-party Fourth Amendment standing: (1) the individual whose rights are being asserted has suffered an invasion of a reasonable expectation of privacy, thereby establishing an injury in fact; (2) the third party has an interest in the litigation related to its area of expertise; and (3) the individual is unable to assert his or her own rights. The first two prongs of the *Hunt* test ensure that the third party can adequately represent the individual's interests, and the last prong of the *Powers* test prioritizes the inability of the individual to protect his or her own interest by raising his or her own claim.[232]

---

230. Kowalski v. Tesmer, 543 U.S. 125, 130 (2004) (quoting Sec'y of State of Md. v. Joseph H. Munson Co., 467 U. S. 947, 956 (1984)).

231. If the Court does not determine that the disclosure of personal data is a concrete and actual harm, satisfying the *Spokeo* requirement, there will be long-term implications every time there is a search without subsequent litigation. *See supra* notes 73–79 and accompanying text. By committing to the basic Fourth Amendment standing requirement—that there be a search or seizure—the Court provides increased protection for individuals subjected to government investigation.

232. This is not the first time that the Court has been called upon to change its standing requirements as applied to third parties. For example, in *Sierra Club v. Morton*, 405 U.S. 727 (1972), Justice Blackmun called for "an imaginative expansion of our traditional concepts of standing in order to enable an organization such as the Sierra Club, possessed, as it is, of pertinent, bona fide and well-recognized attributes

1. *Microsoft would have standing under the new hybrid test for Fourth Amendment standing*

When there is no notice of a search or seizure to Microsoft's cloud customers, *and* Microsoft, as the cloud service provider, cannot communicate with its customers about the search or seizure, there is a big problem. Exacerbating this problem is the fact that Microsoft customers, and therefore Microsoft, likely lack standing to challenge the government's practice under the SCA. However, if the Court were to limit the impact of *Spokeo* and adopt a hybrid standing test to emphasize the inability of an individual to assert their own rights, Microsoft would likely prevail and vindicate its customers' Fourth Amendment rights.

a. Microsoft would likely satisfy the first prong of the hybrid standing test

If the Court were to reject extending the *Spokeo* decision to Fourth Amendment standing, Microsoft customers would clearly have suffered an injury in fact because a search of the customers' personal information has clearly occurred.[233] In *Clapper*, the Supreme Court controversially noted that standing is not justified for an individual or group just because the constitutionality of a statute may not otherwise be challenged.[234] *Clapper* is distinguishable from *Microsoft Corp.*, however, because the respondents in *Clapper* relied on hypothetical future harm from wiretap surveillance[235] whereas *Microsoft Corp.* raises a Fourth Amendment claim related to a harm that has already occurred: the disclosure of Microsoft's customers' data to the government.[236] Moreover, because the individuals affected by the government's searches or seizures are not aware that their cloud-stored communications have been accessed, Microsoft is the only party that has the knowledge to bring such a lawsuit.

Microsoft has also recognized that there should be exceptions to their argument,[237] but the fact that the government's practices under

---

and purposes in the area of the environment, to litigate environmental issues." *Id.* at 757 (Blackmun, J., dissenting).

233. *See supra* Section III.B.1.a.

234. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1148–49 (2013).

235. *Supra* note 152 and accompanying text.

236. Am. Compl., *supra* note 14, at para. 5.

237. For example, the company allows that a lengthy or indeterminate bar is justified in the name of national security. *Supra* note 53 and accompanying text. This argument provides additional problems for Microsoft's lawsuit because in recognizing that there are exceptions, Microsoft may lose its facial challenge to the SCA. That discussion is beyond the scope of this Comment.

sections 2703 and 2705 of the SCA cannot otherwise be challenged, even when they pertain to searches that do not implicate national security concerns, should make the Court uneasy. Individuals cannot be without a forum to challenge these government practices.

b. Microsoft would likely satisfy the second prong of the hybrid standing test

As discussed, Microsoft's position as a cloud-service provider satisfies the requirement that Microsoft's interest in litigating its customer's privacy interests relate to information stored on Microsoft's cloud platform.[238] Microsoft can adequately represent its customers' privacy interests because increased customer trust will likely strengthen Microsoft's business as a cloud service provider.[239] Conversely, Microsoft argues, if it cannot assert its customers' Fourth Amendment rights, the company stands to lose cloud customers.[240]

c. Microsoft would likely satisfy the third prong of the hybrid standing test

Despite the poor fit between the *Powers* test and its argument to show standing,[241] Microsoft likely relied on the test because of its last prong that protects individuals who are either unable or unlikely to assert their own rights.[242] Microsoft might have hoped to appeal to the Court's desire to permit an individual to have his or her day in court because Microsoft's customers are, in fact, unable to assert their own Fourth Amendment rights. The government's practice of combining no-notice warrants and secrecy orders under sections 2703 and 2705 of the SCA leave these customers unaware that the government has accessed their personal information and communications stored on the cloud.[243] This proposed framework would better protect individual rights because it would permit third-

---

Clapper, in which the Court permitted the NSA to conduct wiretap searches to gain additional intelligence for national security purposes, provides an example of this national security exception in the FISA context. *Supra* notes 153–58 and accompanying text; *see also Standing—Challenges to Government Surveillance*—Clapper v. Amnesty International USA, 127 HARV. L. REV. 298, 298 (2013) (suggesting that the United States Supreme Court's holding in *Clapper* should only apply in limited circumstances—in the case of "foreign affairs or national security").

238. *See supra* Section III.B.2.
239. *See supra* notes 180–84 and accompanying text.
240. *See supra* notes 180–84 and accompanying text.
241. *See supra* notes 190–97.
242. *See* Powers v. Ohio, 499 U.S. 400, 411 (1991).
243. *Supra* notes 48–51and accompanying text.

party standing when an organization or corporation such as Microsoft raises a Fourth Amendment challenge on behalf of its customers who are unable to do so on their own.[244]

2. Enacting the Email Privacy Act amendment to the SCA would not diminish the need for an updated Fourth Amendment standing doctrine

Congress is currently contemplating a significant change to the SCA—the Email Privacy Act—that would eliminate the specific substantive problems raised by the *Microsoft Corp.* lawsuit.[245] The proposed amendment requires that any secrecy order issued under section 2705 of the SCA (1) be limited to a maximum of 180 days and (2) make a showing that notifying the individual of the search would have an "adverse result."[246] In other words, if this bill becomes law, the government would not be able to use indefinite secrecy orders, absent extenuating circumstances. Moreover, this amendment would require the government to obtain a warrant in all circumstances, not just when communications have been stored for fewer than 180 days.[247]

The Email Privacy Act amendment to the SCA was approved unanimously by the House Judiciary Committee[248] and passed the full House on April 27, 2016, with incredible support.[249] Equivalent legislation considered in the Senate also had support,[250] but it did not pass.[251] Congressmen Jared Polis (D-Colo.) and Kevin Yoder (R-Kan.) reintroduced the bill on January 9, 2017, with new urgency: while the

---

244. See *supra* Section II.A.1 for a discussion of the *Powers* test and Section II.A.2 for a discussion of the *Hunt* test.

245. Daskal, *supra* note 41. Members of Congress have introduced a version of this ECPA reform bill every year since 2012. Kevin Collier, *Amid Fears of Trump Cabinet, Congress Revives Email Privacy Bill*, VOCATIV (Jan. 12, 2017, 9:35 AM), http://www.vocativ.com/391324/amid-fears-of-trump-cabinet-congress-revives-email-privacy-bill.

246. Daskal, *supra* note 41.

247. *Summary: H.R. 699: Email Privacy Act*, GOVTRACK, https://www.govtrack.us/congress/bills/114/hr699/summary (last updated Feb. 24, 2016).

248. Dustin Volz, *Long-Stalled Email Privacy Bill Advances in Congress*, REUTERS (Apr. 13, 2016), http://www.reuters.com/article/us-usa-cyber-emails-idUSKCN0XA1VK.

249. *See Summary: H.R. 699: Email Privacy Act*, *supra* note 247. The Email Privacy Act "[a]mends the [ECPA] to prohibit a provider of remote computing service or electronic communication service to the public from knowingly divulging to a governmental entity the contents of any communication that is in electronic storage or otherwise maintained by the provider, subject to exceptions," and would also require notice of a warrant within three to ten days to the subject of the search. *Summary: H.R. 699 – 114th Congress (2015–2016)*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/699 (last visited Feb. 5, 2017).

250. Volz, *supra* note 248.

251. Collier, *supra* note 245.

loophole in ECPA permitting the government to circumvent the warrant requirement has not often been used, President Donald Trump's cabinet, particularly Attorney General Jeff Sessions, is suspected to be more "hostile to civil liberties."[252]

Microsoft Corp. will likely take years to make its way through the court system,[253] so the passing of the Email Privacy Act could make the substantive issues at the heart of the case moot. However, as reliance on third-party technologies increases, it is likely that a similar standing problem will arise again. For example, what if the government tried to access non-communicative, substantive business documents stored on the cloud? This information would not be governed by the ECPA or the SCA, and the Email Privacy Act amendment would not apply. There is still a significant need for more clarity on the Fourth Amendment standing doctrine as it applies to third parties.

For a third-party plaintiff to establish standing for a Fourth Amendment claim, the Court should allow a plaintiff to show a harm sufficient to confer standing by pleading either (1) a search or seizure as defined by the Fourth Amendment or (2) a lack of notice of a search or seizure. The Court should also emphasize the ability (or inability) of an individual to assert their own rights when determining whether third-party standing is appropriate.

CONCLUSION

A court will likely determine that Microsoft lacks standing to bring a Fourth Amendment challenge to sections 2703 and 2705 of the SCA because Microsoft's customers themselves lack standing. Microsoft improperly relied upon the *Powers* test to establish third-party standing to raise a Fourth Amendment claim on behalf of its customers because the *Hunt* test for organizational standing is more appropriate for Microsoft's business/customer relationship. Microsoft has a stake in the outcome of the lawsuit because it stands to lose cloud customers if the SCA is upheld as constitutional; therefore, the company should be able to act as an adequate advocate for its customer's rights.

The government's simultaneous exercise of SCA sections 2703 and 2705—issuing no-notice warrants and indefinite secrecy orders—prevents a cloud customer from receiving notice that a search or seizure of their communications has taken place. Yet, Microsoft likely does not have standing to raise a Fourth Amendment claim because Microsoft cannot satisfy the current third-party standing test under

252. *Id.* (quoting Julian Sanchez of the Cato Institute).
253. Kerstetter, *supra* note 23.

Hunt that requires the participation of a harmed Microsoft customer. Furthermore, unless the Court declines to extend the *Spokeo* holding to the Fourth Amendment, a Microsoft customer may not have suffered the requisite injury in fact because the invasion of privacy is particularized but not necessarily concrete: Microsoft's customers likely satisfy the reasonable expectation of privacy test—indicating a Fourth Amendment search and potential Fourth Amendment violation—but there is no evidence that they have suffered any further negative impact from the search, and they may be left without an avenue to challenge the constitutionality of the search.

Microsoft Corp. helps to illustrate the problems with a narrow Fourth Amendment standing doctrine. A more flexible hybrid test for third-party Fourth Amendment standing, reflecting portions of both the *Hunt* and *Powers* tests, is necessary to ensure that individuals' data and information is protected as technologies continue to develop.