William & Mary Bill of Rights Journal

Volume 26 | Issue 2 Article 9

Notice and Standing in the Fourth Amendment: Searches of Personal Data

Jennifer Daskal

NOTICE AND STANDING IN THE FOURTH AMENDMENT: SEARCHES OF PERSONAL DATA

Jennifer Daskal*

ABSTRACT

In at least two recent cases, courts have rejected service providers' capacity to raise Fourth Amendment claims on behalf of their customers. These holdings rely on longstanding Supreme Court doctrine establishing a general rule against third parties asserting the Fourth Amendment rights of others. However, there is a key difference between these two recent cases and those cases on which the doctrine rests. The relevant Supreme Court doctrine stems from situations in which *someone* could take action to raise the Fourth Amendment claim, even if the particular third-party litigant could not. In the situations presented by the recent cases, by contrast, the service provider was the *only* source of possible challenge—at least for some meaningful period of time.

In both cases, the searches were done pursuant to a warrant issued in accordance with the Stored Communications Act (SCA). Because the government proceeded by warrant, the government was not required to give notice to the target of the search. The warrants were also accompanied by no-notice orders, meaning that the provider was barred from telling anyone, including the target of the search, that his or her data was being sought by the government—in some cases indefinitely.

The use of such no-notice warrants served on third-party providers is an increasingly common investigatory tool, wrought by the changes in the way personal information is stored and managed in the digital age. Its use presents a significant shift in how investigations are carried out. It relies on a third-party intermediary between the police and the citizenry to gather information about persons of interest. It makes the searches that are occurring much more indirect and less visible. And it means that individuals are a lot less likely to know—and thus have an opportunity to object—if and when their personal information is being sought and collected by law enforcement officials. This Article examines what has changed; why it matters; and

* Associate Professor, American University Washington College of Law. Special thanks to Jeff Bellin, Rebecca Green, Richard Re, Paul Ohm, the faculty at William & Mary Law School, and the participants at the March 2017 *William & Mary Bill of Rights Journal* Symposium, *Big Data, National Security, and the Fourth Amendment*, for their thoughtful comments and feedback.

the implications for the Fourth Amendment. Ultimately, this Article makes the case for notice and revisions to standing doctrine as an essential to protecting Fourth Amendment interests and as good policy.

INTRODUCTION

It used to be the case that if law enforcement sought a target's personal communications or record of business meetings, it would have to go directly to the target.[1] To illustrate, consider a hypothetical target named John. Law enforcement would, for example, either seek the data directly from John, or it would get a warrant to search John's home or other property for the relevant information.[2] If John was present when the search was carried out, he would know about it.[3] In fact, there would be direct interaction between John and the officers searching his home.[4] And if he was not present, Rule 41 of the Federal Rules of Criminal Procedure requires that the officers executing the search "leave a copy of the warrant and receipt at the place where the officer took the property."[5] As a result, John would be on notice of the search.[6] If he thought the search was unlawful, John could raise concerns with the relevant authorities, publicize what happened to him, or bring a formal civil action, even if he were never actually charged with a crime.[7] Additionally, if John were in fact charged, he could bring a motion to suppress.[8]

Perhaps, instead of searching John's property, the investigating officers would go and talk to John's friend or employer and compel that individual to turn over relevant documents about John.[9] In that case, law enforcement officials would not be obliged

---

[1] Prior to the advent of electronic communications, wiretapping, and cell phones, all searches were in physical space. *See* Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

[2] *See id.*

[3] Even in the present day, such physical searches require that "a copy of the warrant and a receipt for property taken" be provided. FED. R. CRIM. P. 41(f)(1)(C).

[4] *See id.*

[5] *Id.*

[6] *See* FED. R. CRIM. P. 41(f)(1)(C) advisory committee's note to 2016 amendment ("The [2016] amendment is intended to ensure that reasonable efforts are made to provide notice of the search, seizure, or copying, as well as a receipt for any information that was seized or copied, to the person whose property was searched or who possessed the information that was seized or copied.").

[7] The civil action would be a Section 1983 claim. *See generally* David E. Nash, Note, *Damage Actions Under Section 1983 for Illegal Searches and Seizures: Reconsidering the Applicability of Collateral Estoppel*, 1980 DUKE L.J. 1029.

[8] The court may exclude evidence obtained through illegal searches. *See generally* William Geller, *Enforcing the Fourth Amendment: The Exclusionary Rule and Its Alternatives*, 1975 WASH. U. L.Q. 621.

[9] For example, third-party consent searches allow such information to be turned over to

to tell John about the search, but the friend or employer would be free to do so.[10] And if the search of the friend's home or employer's workplace was unduly invasive, the friend or employer could challenge the legality of the search—even if under current doctrine John could not himself bring a Fourth Amendment challenge.[11]

Thus, there is someone who could, at least theoretically, provide a check on government overreach—even in those cases where John was not ultimately charged with a crime.[12] John—or his friend or employer—could bring a civil challenge against allegedly abusive police practices, albeit as an ex post challenge.[13] Any such individuals could seek administrative redress via civilian complaint mechanisms. They could also publicize the events, therefore providing a potential deterrent mechanism in the form of undesirable public attention.[14]

These days, however, most personal information related to John is not—or is at least not exclusively—in his home, written down in an address book or diary, or in the possession of close friends or employers. Rather, it is digitized and increasingly in the custody and control of third-party providers—including Internet service providers, purveyors of social media, distributors of electronic gadgets, and other corporate entities that manage, transmit, and store his data and do not have a personal relationship with John.[15]

Instead of searching John's home or seeking information from his close friend or employer, law enforcement officials go to these third-party providers to access the data, generally pursuant to the provisions of the SCA.[16] Depending on what and how the data is being requested, the government will not be obliged to tell John that it is searching his data.[17] The government also can bar the service provider from telling John that he has been the subject of the search through what has colloquially been called a "gag order."[18]

---

police. *See* 4 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 8.3 (5th ed. 2017).

[10] *See id.*

[11] Anyone with a reasonable expectation of privacy in the object of the search has standing to challenge the search. *See generally* Rakas v. Illinois, 439 U.S. 128 (1978).

[12] *See supra* notes 7–11 and accompanying text.

[13] *See supra* notes 7–11 and accompanying text.

[14] *See, e.g.*, George Leef, *Will There Be Justice for Family Whose Home Was Raided Because Cops Couldn't Tell Tea from Pot?*, FORBES (Aug. 1, 2017, 7:30 PM), https://www.forbes.com/sites/georgeleef/2017/08/01/will-there-be-justice-for-family-whose-home-was-raided-because-cops-couldnt-tell-tea-from-pot/#3a0a8c0770e6 [http://perma.cc/96D8-R2ZQ] (profiling *Harte v. Board of Commissioners*, 864 F.3d 1154 (10th Cir. 2017), where a tea grower's home was raided after being suspected of growing drugs).

[15] *See* Alessandro Acquisti, *The Economics of Personal Data and Privacy* 3 (WPISP-WPIE Roundtable Background Paper No. 3, 2010).

[16] *See infra* notes 32–37 and accompanying text.

[17] *See infra* note 37 and accompanying text.

[18] *See infra* notes 45–52 and accompanying text.

Until recently, many of these gag orders were of indefinite duration.[19] As of an October 2017 policy change, federal prosecutors may seek gag orders for a maximum of one year.[20] If, however, there is a finding of exceptional circumstances, approved by a designated supervisor, federal prosecutors can seek gag orders that last longer than a year.[21] The orders also can be renewed.[22] The guidance does not bind state prosecutors.[23]

The government argues that these no-notice provisions are necessary to protect the integrity of their investigations.[24] The statute itself lists a series of compelling reasons that must be invoked to both delay governmental notice and to justify the issuance of a gag order.[25] Specifically, in order to issue either a delayed notice order or gag order, a court must find a reason to believe that notice will result in one of the following consequences:

> (A) endangering the life or physical safety of an individual;
> (B) flight from prosecution;
> (C) destruction of or tampering with evidence;
> (D) intimidation of potential witnesses; or
> (E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.[26]

On their face, each of these seem to be a legitimate reason for delaying or precluding notice. In such situations, our hypothetical target John will not learn about the fact that his data has been subject to a governmental search and seizure—perhaps for good reason and perhaps for some potentially lengthy period of time.

John can't challenge the search or seizure because he doesn't know about it.[27] And the service provider, which does know about the search or seizure, can't raise

---

[19] Ellen Nakashima, *Justice Department Moves to End Routine Gag Orders on Tech Firms*, WASH. POST (Oct. 24, 2017), https://www.washingtonpost.com/world/national-security/justice-department-moves-to-end-routine-gag-orders-on-tech-firms/2017/10/23/df8300bc-b848-11e7-9e58-e6288544af98_story.html?utm_term=.341e4db4a441 [https://perma.cc/P45J-DAR7].

[20] Memorandum from Rod. J. Rosenstein, Deputy Attorney Gen., U.S. Dep't of Justice, to Heads of Dep't Law Enf't Components et al., Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. § 2705(b) (Oct. 19, 2017), https://www.justice.gov/criminal-ccips/page/file/1005791/download [https://perma.cc/5XKP-M3Y6] [hereinafter Rosenstein Memorandum].

[21] *Id.*

[22] *See id.*

[23] *See id.*

[24] *See id.*

[25] *See* 18 U.S.C. § 2705 (2012).

[26] *Id.* § 2705(a)(1)(B)(2).

[27] *See infra* notes 45–53 and accompanying text.

Fourth Amendment claims on behalf of John—at least according to the government's and several judges' interpretation of current doctrine.[28] That means that there is *no one* who is both in the position and legally entitled to challenge the search or seizure on Fourth Amendment grounds during the period of secrecy—thus eliminating one of the most powerful checks on government overreach.

This Article challenges this law and practice on both constitutional and policy grounds. It proceeds in three parts. It starts by describing the relevant statutory framework and two recent cases where the issues have been brought to the forefront.[29] It then examines and critiques what the Supreme Court and relevant lower courts have said about both notice and standing.[30] It concludes with a policy argument for a statutory change to require governmental notice in the issuance of SCA warrants, preclude indefinite gag orders (thus codifying what the federal government already has done as a matter of policy), and enable providers to bring Fourth Amendment claims on behalf of their customers.[31]

I. NOTICE AND STANDING: THE RELEVANT STATUTORY PROVISIONS AND TWO RECENT COURT CASES

A. Relevant Statutory Provisions

The SCA sets up a complicated statutory scheme governing, among other things, when and how law enforcement can compel a provider of wire or electronic communications services (what I label the "service provider") to produce stored data.[32] Certain kinds of information can be obtained by subpoena.[33] Other kinds of information can be obtained by court order based on "reasonable grounds to believe" that the sought after data "are relevant and material to an ongoing criminal investigation."[34] And, pursuant to the widespread application and interpretation of the Sixth Circuit's ruling in *United States v. Warshak*,[35] communications content can only be obtained by warrant.[36]

---

[28] *See infra* Part I.

[29] *See infra* Part I.

[30] *See infra* Part II.

[31] *See infra* Part III.

[32] *See* 18 U.S.C. § 2703(a) (2012). The SCA is codified at 18 U.S.C. §§ 2701–2727 (2012).

[33] 18 U.S.C. § 2703(b)(1)(B)(i) (permitting a government entity to compel a provider to disclose the contents of electronic communications through an administrative subpoena).

[34] *Id.* § 2703(d).

[35] 631 F.3d 266, 286 (6th Cir. 2010) ("[I]f government agents compel an ISP to surrender the contents of a subscriber's emails, [this action] necessitates compliance with the warrant requirement . . . .").

[36] *See generally* 18 U.S.C. § 2703 (laying out the statutory framework). The statute itself specifies that if the government is seeking to compel communications content from a so-called "remote computing service" or communications in storage for more than 180 days, then the government can proceed by court order or subpoena, rather than by warrant. *Id.* § 2703(b)(1)(B)(i)–(ii). However, in such cases, it must give notice to the target. *Id.*

When the government uses a warrant to compel production of sought-after data, it need not provide notice to the target.[37]

The embrace of an indefinite no-notice warrant contrasts to other analogous statutory provisions authorizing law enforcement collection of communications content, which permit a *time-limited* delay in government-required notifications.[38] Sneak-and-peak warrants, for example, permit the government to engage in covert searches—but only for a limited period of time.[39] At the end of 30 days, the government is required to give notice, absent another time-limited extension.[40] The Wiretap Act[41] similarly specifies that the target of an intercept order must be provided with relevant information about the wiretap within 90 days of the application for such an order—although it too allows for such notice to be postponed based on a "showing of good cause."[42] Other provisions permit no notice production of *non-content* information from third-party providers. But they are all arguably justified on the grounds that, under current doctrine, there is no Fourth Amendment interest in the kinds of *non-content* information that is being accessed.[43] By contrast, the statutory

§ 2703(b)(1)(B). Currently, however, both the Department of Justice and all major service providers are treating *Warshak* as if it has nationwide application and demanding a warrant as grounds for compelling communications content, regardless of how long it has been in storage. Hanni Fakhoury, *Will Telcos Follow ISPs and Extend Warrant Protection for All?*, ELECTRONIC FRONTIER FOUND. (June 17, 2014), https://eff.org/deeplinks/2014/06/will-telcos-follow-isps-and-require-warrant-cell [https://perma.cc/TUA4-GQKB] ("Although *Warshak* only controlled in the Sixth Circuit, many of the largest online service providers including Facebook, Google, Apple, Microsoft and Yahoo made *Warshak* the rule across the board, and began demanding all law enforcement across the country use a warrant to obtain the contents of electronic communications. As that became the internal policy for the companies, eventually even the Department of Justice followed, ordering federal prosecutors and law enforcement agents nationwide to use a warrant to obtain emails.").

[37] *See* 18 U.S.C. § 2703(b)(1)(A).

[38] *Compare id.*, *with* 18 U.S.C. § 2705 (2012).

[39] *See* 18 U.S.C. § 3103a(b) (2012).

[40] *See* 18 U.S.C. § 3103a(c) (specifying that "each additional delay should be limited to periods of 90 days or less, unless the facts of the case justify a longer period of delay"—nothing in this provision allows for *indefinite* delay); *see also, e.g.*, United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986) ("[T]he warrant was constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. Such time should not exceed seven days except upon a strong showing of necessity.").

[41] 18 U.S.C. §§ 2510–2525 (2012). This Chapter is fully entitled "Wire and Electronic Communications Interception and Interception of Oral Communications."

[42] 18 U.S.C. § 2518(8)(d).

[43] *See, e.g.*, 18 U.S.C. § 3121 (2012) (section entitled "[g]eneral prohibition on pen register and trap and trace device use; exception"); 18 U.S.C. § 2709 (2012) (section entitled "[c]ounterintelligence access to telephone toll and transactional records"). Under current doctrine, the absence of any notice requirement can arguably be justified on the grounds that there is no reasonable expectation of privacy in the kind of non-content data obtained via these provisions, and thus the collection does not trigger the Fourth Amendment. *See generally* Smith v. Maryland, 442 U.S. 735 (1979). By comparison the kind of data collected by a SCA

framework governing wiretaps is premised on the idea that while notice of a governmental search of *content* can be delayed, it cannot be indefinitely postponed without running afoul of the Fourth Amendment.[44]

A separate provision under the SCA also authorizes a court, upon motion of the government, to preclude the service provider from disclosing the existence of a compelled production order—the so-called "gag order" provision.[45] As described above, the court must determine that there is a "reason to believe" that notification will endanger an individual; lead to a "flight from prosecution," destruction of evidence, or intimidation of a witness; or otherwise jeopardize an investigation in order to issue a gag order.[46] The statute does not include a time limit as to how long such orders can last—instead specifying that they should be issues "for such period as the court deems appropriate."[47] Although the reference to a "period of time" suggests that these orders ought to have *some* limit, the government has been seeking—and courts issuing—gag orders of *indefinite* duration.[48] An October 2017 Department of Justice policy change arguably puts an end to this practice on the federal level—directing prosecutors to, as a default, seek gag orders of no more than a year.[49] But this policy change does not bind state prosecutors.[50]

The issuance of indefinite gag orders is hard to justify (hence the Department of Justice policy change).[51] Whereas there are often sound reasons why secrecy is needed in order to preserve the integrity of an investigation,[52] at some point the investigation is completed. Yet, indefinite gag orders mean that providers may be subject to these secrecy provisions even after the underlying justification for the orders no longer exist.[53]

---

warrant is, pursuant to *Warshak*, generally understood as falling within the protections of the Fourth Amendment. *See* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

[44] *See, e.g.*, *Freitas*, 800 F.2d at 1456 (holding that the "warrant was constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry").

[45] 18 U.S.C. § 2705(b) (2012). The so-called "gag order" provision is actually entitled "Preclusion of Notice to Subject of Governmental Access." *Id.*

[46] *See id.* Microsoft separately contends that "reason to believe" is too lax a standard, although does not specify what standard of proof should be required. Microsoft's Opposition to Government's Motion to Dismiss at 14–16, Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887 (W.D. Wash. 2017) (No. 2:16-cv-00538-JLR) [hereinafter Microsoft's Opposition]; First Amended Complaint for Declaratory Judgment at para. 29, *Microsoft*, 233 F. Supp. 3d 887 (No. 2:16-cv-00538-JLR) [hereinafter First Amended Complaint]. It argues that courts have been issuing gag order rulings based on boiler plate language without sufficient consideration of the *particular* facts that would justify one of the relevant findings. Microsoft's Opposition, *supra*, at 14–15.

[47] 18 U.S.C. § 2705(b).

[48] *See* First Amended Complaint, *supra* note 46, at paras. 5, 16.

[49] *See* Rosenstein Memorandum, *supra* note 20.

[50] *See id.*

[51] *See id.*

[52] *See, e.g.*, 18 U.S.C. § 2705(b).

[53] *See* First Amended Complaint, *supra* note 46, at paras. 5, 16.

Of particular concern, the combination of these secrecy provisions and restrictive third party standing doctrine means that there is no one in the position to raise a Fourth Amendment challenge to the legality of the search or seizure.[54] To be sure, the SCA authorizes a service provider to bring a motion to quash "if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider."[55] But at least one court has concluded that this grant of authority is limited to the issuance of court orders that are not warrants.[56] Pursuant to this interpretation, there is no means for the provider to challenge a warrant.[57] There is also disagreement as to what "undue burden" refers to: whether it refers exclusively to the time and cost of executing a search, or whether it also permits broader challenges based on a provider's business interests in maintaining its customers' trust.[58]

In addition, the SCA's statutory authorization to challenge a search stands in contrast to the more open-ended authority granted to providers to challenge directives issued pursuant to the FISA Amendments Act.[59] As a result, some have concluded that providers lack any basis for bringing Fourth Amendment claims on behalf of their customers—even if their customers are kept in the dark about the relevant search or seizure that the provider seeks to challenge.[60]

1. The Microsoft Litigation

In 2016, Microsoft brought both a facial and as applied challenge to the "gag order" provision of SCA.[61] Microsoft asserted that it had been issued more than 3,200 secrecy orders in the 20-month period ending in May 2016, and that nearly two-thirds were for an indefinite length of time.[62] Some 650 of those were issued in conjunction

[54] *See supra* notes 45–53 and accompanying text; *infra* notes 55–58 and accompanying text.

[55] 18 U.S.C. § 2703(d) (2012).

[56] *In re* 381 Search Warrants Directed to Facebook, Inc., 14 N.Y.S.3d 23, 29 (N.Y. App. Div. 2015).

[57] *See id.* at 31.

[58] *See, e.g.*, *In re* 381 Search Warrants Directed to Facebook, Inc., 78 N.E.3d 141, 153 (N.Y. 2017) (Rivera, J., concurring) (expressing the view that the statute's reference to "undue burden" covers demands for information that would adversely impact a provider's business, reputational, and property interests).

[59] *See* 50 U.S.C. § 1881a(h)(4)(A) (2012) (authorizing providers to "petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court"); 50 U.S.C. § 1861(f) (section entitled "[j]udicial review of FISA orders"); *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009 (FISA Ct. Rev. 2008) (finding that language included in the Protect America Act—which specified that providers could challenge "the legality of [a] directive"—gave providers third-party standing to raise the Fourth Amendment claims on behalf of their customers). The authorization under the SCA, by comparison, focuses particularly on the volume and burden of the request. *See* 18 U.S.C. § 2703(d).

[60] *See In re 381 Search Warrants Directed to Facebook*, 14 N.Y.S.3d at 29.

[61] First Amended Complaint, *supra* note 46, at paras. 27, 32.

[62] *Id.* at para. 16.

with a search warrant; therefore the government had no obligation to disclose the fact of the search to the target *and* Microsoft was indefinitely barred from doing so.[63]

Amicus filings in the case indicate that Microsoft was hardly an outlier. During the first seven months of 2016, Yahoo "received over 700 federal search warrants for user data, and well over half—about 60%—were accompanied by gag orders of indefinite duration."[64] Google reported a similar percentage.[65] Apple asserted it received approximately 590 unlimited or indefinite duration gag orders in the beginning of 2016.[66] LinkedIn asserts that it received hundreds of gag orders over the course of the year ending in September 2016, with nearly two-thirds of them being of indefinite duration.[67] And, between April and June 2016, "nearly three-quarters (58 of 79) of all gag orders received by Snapchat under § 2705(b) had no definite end."[68]

Microsoft argued that these gag orders violate Microsoft's speech rights.[69] Microsoft further claimed that the combination of no-notice search warrants and gag orders violate its customers' Fourth Amendment right to notice of a search.[70] It sought declaratory relief in response.[71]

In response to the government's motion to dismiss, the district court allowed the First Amendment claim to proceed, but dismissed the Fourth Amendment claims on standing grounds.[72] While acknowledging the "difficult situation" that the ruling created, the district court judge, Judge Robart, deemed himself bound by Supreme Court and Ninth Circuit precedent that precludes third parties from raising Fourth Amendment claims.[73] Judge Robart also rejected Microsoft's argument that this case presented "special circumstances" because the target might never learn of the search.[74]

---

[63] *Id.*

[64] Brief of Amici Curiae Amazon.com et al. in Support of Microsoft Corporation at 8, Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887 (W.D. Wash. 2017) (No. 2:16-cv-00538-JLR) [hereinafter Amazon Brief].

[65] *Id.*

[66] Brief of Amici Curiae Apple et al. in Support of Microsoft Corporation's Opposition to Defendants' Motion to Dismiss at 1, *Microsoft*, 233 F. Supp. 3d 887 (No. 2:16-cv-00538-JLR) [hereinafter Apple Brief].

[67] Amazon Brief, *supra* note 64, at 7.

[68] *Id.* at 8.

[69] First Amended Complaint, *supra* note 46, at para. 1.

[70] *Id.*

[71] *Id.* at para. 41.

[72] Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 910–16 (W.D. Wash. 2017).

[73] *Id.* at 915–16.

[74] *Id.* at 914–16. Judge Robart also earlier denied the American Civil Liberties Union (ACLU) the right to intervene in the case. Microsoft Corp. v. U.S. Dep't of Justice, No. C16-0538JLR, 2016 WL 4506808, at *7–8 (W.D. Wash. Aug. 29, 2016). At that time, Judge Robart emphasized that, among other things, Microsoft was litigating the Fourth Amendment claim on behalf of its customers. *Id.* The judge thus concluded that the ACLU's interests were not "sufficiently different" from Microsoft's. *Id.* at *7; *see also id.* at *8 (emphasizing that the ACLU "has not demonstrated that Microsoft is incapable or unwilling to make all available

Instead, he concluded that the result was analogous to the situation faced by the victim of an unreasonable search in a stranger's home.[75]

Since then, the Department of Justice announced a new policy rule with respect to gag orders—directing federal prosecutors to seek gag orders of no more than a year and requiring federal prosecutors to conduct an "individualized and meaningful assessment" as to whether there are sufficient grounds to request such gag orders and to seek such orders only "when circumstances require."[76] Microsoft, in turn, decided not to proceed with the case; according to Microsoft, the Department's policy has significantly improved, making continued litigation unnecessary.[77] The case was dismissed on October 25, 2017.[78] Yet, even if federal prosecutors are now barred from seeking indefinite gag orders, it is a practice that can be continued by the states.[79] Thus, Judge Robart's ruling—and reasoning—remains relevant.[80] It relies on a restrictive interpretation of third party standing—a result that I argue undercuts key Fourth Amendment protections.[81]

Importantly, there is a key difference between the situation addressed by the Microsoft litigation and the situation identified by Judge Robart in which someone is the target of an unreasonable search in a stranger's home.[82] In the latter case, a stranger whose home was unlawfully searched can bring a Fourth Amendment challenge.[83] Of course, the stranger might not have any incentive to do so, but there is at least a *possible* source for such a challenge.[84] More importantly, the fact of the search

---

arguments in support of the objectives it holds in common with the ACLU"). But once Judge Robart determined Microsoft lacked standing to raise the issue, this was no longer the case. *See Microsoft*, 233 F. Supp. 3d at 910–11. As a potential target of such secret searches, the ACLU might have been able to raise the claims that Microsoft was unable to pursue. To be sure, the ACLU would face its own standing issues, given its likely inability to prove that it was a target of both a search and a gag order. *See* Am. Civil Liberties Union v. Clapper, 804 F.3d 617, 626 (2d Cir. 2015) (declining to reach the First and Fourth Amendment constitutional issues in the case because the harm to Appellants was in flux during the transitional period of the Freedom Act). But once Microsoft's claim was dismissed, the issues were sufficiently different. If the ACLU could get around the separate standing issue, it would have been able to raise the Fourth Amendment claim.

[75] *Microsoft*, 233 F. Supp. 3d at 916.

[76] *See* Rosenstein Memorandum, *supra* note 20.

[77] *See* Brad Smith, *DOJ Acts to Curb the Overuse of Secrecy Orders. Now It's Congress' Turn.*, MICROSOFT ON THE ISSUES (Oct. 23, 2017), http://blogs.microsoft.com/on-the-issues/2017/10/23/doj-acts-curb-overuse-secrecy-orders-now-congress-turn/ [https://perma.cc/B3JM-2L6R].

[78] Order Granting Microsoft Corporation's Unopposed Motion for Voluntary Dismissal, Microsoft Corp. v. U.S. Dep't of Justice, No. 2:16-cv-00538-JLR (W.D. Wash. Oct. 24, 2017).

[79] *See* Rosenstein Memorandum, *supra* note 20.

[80] *Microsoft*, 223 F. Supp. 3d at 910–16.

[81] *See id.*

[82] *Id.* at 916.

[83] *See* Rakas v. Illinois, 439 U.S. 128, 143 (1978).

[84] *See generally* U.S. CONST. amend. IV.

would not be a secret. The stranger whose house was searched would learn of it and could talk about it. Even if he or she did not know or convey the information to the target, he could discuss it with friends, public interest groups, or the media. There would thus be a mechanism for holding the government accountable, even if an actual lawsuit was never filed.[85]

In the cases identified by Microsoft, by contrast, no one other than the service provider may ever learn about the search.[86] Unlike the stranger, the provider is barred from telling *anyone* about the search.[87] The result is, as Judge Stephen Smith warned, a "regime of secrecy surrounding [SCA] court orders,"[88] coupled with extremely limited opportunities for push back via court challenges.

2. The Facebook Litigation

In another case, Facebook sought to challenge the issuance of nearly 400 warrants that Facebook argued were overbroad.[89] Issued in conjunction with a disabilities fraud case, the warrants sought virtually all communications, including all "undeleted or saved photos," "private messages," and "chat history" of a cross-section of 381 individuals (including high school students) with virtually no date-range limitations.[90] The warrants also were accompanied by no-notice orders.[91]

Facebook moved to quash, arguing that the breadth of the compulsion orders violated its customers' Fourth Amendment rights.[92] It also challenged the non-disclosure orders.[93] The New York Supreme Court (New York's equivalent of a district court) denied both challenges.[94] As in the Microsoft case, the Supreme Court judge concluded that Facebook lacked standing to bring the Fourth Amendment claim, since it was Facebook's customers—not Facebook—that had an expectation of privacy in the sought-after data.[95] The court also determined that disclosure would risk jeopardizing the ongoing criminal investigation; as a result, the gag orders were valid.[96]

---

[85] *See supra* notes 7–14 and accompanying text.

[86] *Microsoft*, 233 F. Supp. 3d at 915–16.

[87] *Id.*

[88] Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 314 (2012) (examining secrecy resulting from a combination of sealing and absence of notice associated with surveillance conducted pursuant to the Electronic Communications Privacy Act, of which the SCA is a part).

[89] *In re* 381 Search Warrants Directed to Facebook, Inc., 78 N.E.3d 141, 143 (N.Y. 2017).

[90] Brief of Appellant at 12–15, *In re 381 Search Warrants Directed to Facebook*, 78 N.E.3d 141 (No. APL-2015-00318) [hereinafter Brief of Appellant].

[91] *In re* 381 Search Warrants Directed to Facebook, Inc., 14 N.Y.S.3d 23, 25 (N.Y. App. Div. 2015).

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

Facebook appealed.[97] While the appeal was pending, the government charged 62 of the 381 individuals whose data was targeted by the warrants, and Facebook was ultimately permitted to notify the remaining 319.[98] But Facebook continued to pursue the claim—emphasizing that most of the targets lacked a "meaningful remedy" and that, as the entity uniquely situated to challenge the orders, it should be permitted to do so.[99]

Both the intermediate appellate court and New York's highest court ruled against Facebook.[100] The intermediary appellate court concluded that "there is no constitutional or statutory right to challenge an alleged defective warrant before it is executed," whether the challenge was brought by the direct target or third-party provider.[101] It thus sidestepped the third-party standing issue, deciding instead that, in contrast to subpoenas, there was no right of pre-enforcement review, whether sought by the target of the search or the provider served with the warrant.[102] It described ex ante protections, in the form of approval of a warrant by a neutral judicial officer, and ex post protections, in the form of a suppression remedy, as more than sufficient to "successfully ensure that the government does not exceed its authority when requesting or executing a search warrant."[103]

New York's highest court upheld the ruling.[104] It concluded that even if Facebook could bring an initial motion to quash, there was no right to appeal the denial.[105] In doing so, it rejected Facebook's argument that the SCA warrant in this case operated

---

[97] *Id.*

[98] *See* Brief of Appellant, *supra* note 90, at 15–16.

[99] *See id.* at 30 ("It is inconceivable that the hundreds of targeted but non-indicted Facebook users could all be expected to retain lawyers and file lawsuits against the Government challenging the bulk warrants. . . . As the recipient of the warrant, and the entity that actually conducts the search, Facebook is uniquely positioned to help preserve privacy rights from unjustified governmental intrusions.").

[100] *In re 381 Search Warrants Directed to Facebook*, 14 N.Y.S.3d at 25; *In re* 381 Search Warrants Directed to Facebook, Inc., 78 N.E.3d 141, 143–44 (N.Y. 2017).

[101] *In re 381 Search Warrants Directed to Facebook*, 14 N.Y.S.3d at 25. The court separately suggested, albeit without deciding, that, thanks to the third-party doctrine, the relevant information might not even by protected by the Fourth Amendment at all. *See id.* at 30.

[102] *Id.* at 29. Facebook argued that 18 U.S.C. § 2703(d)—which authorizes a "court issuing an order pursuant to this section, on a motion made promptly by the service provider, [to] quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider"—gave them a statutory right to object. *In re 381 Search Warrant Directed to Facebook*, 14 N.Y.S.3d at 29. But the court read the provision as providing a statutory right to object to subpoenas and court orders that fell short of a warrant. *Id.*

[103] *In re 381 Search Warrants Directed to Facebook*, 14 N.Y.S.3d at 26–27.

[104] *In re 381 Search Warrants Directed to Facebook*, 78 N.E.3d at 152–53.

[105] *Id.* at 152.

more like a subpoena than a warrant in the way it compelled a third party to produce data.[106] Under New York law, subpoenas are appealable; warrants are not.[107]

Only the dissenting judge reached the standing issue.[108] The dissent examined the factors laid out in the leading Supreme Court case on third-party standing, *Powers v. Ohio*,[109] and concluded that all were met.[110] Facebook suffered an injury in terms of the burden of complying with the warrant; Facebook had a sufficiently close relation to its customers to bring the claim; and the direct targets of the search were hindered in their ability to raise the claim themselves.[111] As the dissenting judge put it:

> Even stipulating that each user would, despite the initial indefinite gag order, be told at some point of the seizure, the mere formal possibility of a civil suit does not foreclose Facebook from asserting third-party standing as the litigant best placed to vindicate its users' rights in practice, before a violation of any rights has occurred, by way of the adversarial system on which our rule of law rests.[112]

The dissenting judge thus went a step further than what Microsoft sought in the gag order case.[113] In the gag order case, Microsoft emphasized the "special circumstances" that exist when the targets are indefinitely, and perhaps permanently, denied the relevant information that would allow them to bring a Fourth Amendment claim.[114] The dissent in the Facebook case concluded that even if targets are ultimately notified about the search, they are not likely to be able to vindicate their claims;[115] thus, the relevant third-party provider on whom the warrant has been served should be permitted to do so.[116]

---

[106] *Id.* at 146.

[107] *Id.* at 145–46. This is an interesting contrast with the position taken by the government in the Microsoft Ireland case. In that case, the government argued that the warrants *should* be treated like subpoenas for purposes of assessing territoriality. *See, e.g.*, *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by the Microsoft Corp., 15 F. Supp. 3d 466, 472 (S.D.N.Y. 2014).

[108] *In re 381 Search Warrants Directed to Facebook*, 78 N.E.3d at 170–73 (Wilson, J., dissenting).

[109] 499 U.S. 400, 410–11 (1991).

[110] *In re 381 Search Warrants Directed to Facebook*, 78 N.E.3d at 172 (Wilson, J., dissenting).

[111] *See id.*

[112] *Id.* at 173.

[113] *See id.*; Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 912–16 (W.D. Wash. 2017).

[114] *Microsoft*, 233 F. Supp. 3d at 912–13.

[115] *In re 381 Search Warrants Directed to Facebook*, 78 N.E.3d at 172–73 (Wilson, J., dissenting).

[116] *Id.* at 171–72.

II. THE CONSTITUTIONAL LAW BACKDROP

A. Notice as a Fourth Amendment Requirement

In several contexts, the Supreme Court has stressed the importance of ex ante notice as a means of protecting property, reducing the likelihood of violence, and preserving dignity.[117] The requirement that police officers knock and announce their presence before entering one's home is designed to give individuals an opportunity to "prepare themselves" for the entry of the police, thus preserving their dignity, while at the same time minimizing the risk of property destruction and likelihood of violent escalation.[118]

Even if the search does not involve direct police to citizen interaction, ex post notification—perhaps delayed—is still required pursuant to both the Constitution and Rule 41 of the Federal Rules of Criminal Procedure.[119] In *Berger v. New York*,[120] for example, the Supreme Court struck down a surveillance scheme that, among other problems, did not require notice to the government's targets.[121] A decade later, the Court in *United States v. Donovan*[122] described notice as essential to the constitutionality of the Wiretap Act.[123] And in *Dalia v. United States*,[124] the Supreme Court again emphasized the importance of notice.[125] In concluding that the delayed notification provisions of the Wiretap Act provided a constitutionally adequate substitute for advance notice, the Court made clear that while notice could be delayed, it could not be abandoned altogether.[126] While not a constitutional provision, Rule 41 stems from an understanding of what the Constitution and good policy requires, mandating

---

[117] *See, e.g.*, Hudson v. Michigan, 547 U.S. 586, 594 (2006) (discussing how an announced entry—as opposed to an unannounced entry—better protects the owner's property and privacy).

[118] *Id.* (citation omitted).

[119] U.S. CONST. amend. IV; FED. R. CRIM. P. 41(f)(1).

[120] 388 U.S. 41 (1967).

[121] *Id.* at 60 (emphasizing that the statute "has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts"); *see also* Katz v. United States, 389 U.S. 347, 355 n.16 (1967) (emphasizing that a critical component of a conventional warrant is that it "ordinarily serves to notify the suspect of an intended search"); United States v. Freitas (*Freitas I*), 800 F.2d 1451, 1456 (9th Cir. 1986) (concluding that "the absence of any notice requirement in the warrant casts strong doubt on its constitutional adequacy"); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 803 (1994) (describing notice as essential element of what makes warrants reasonable).

[122] 429 U.S. 413 (1977).

[123] *Id.* at 429 n.19; *id.* at 430 (citing with approval Senator Hart's determination that "notice of surveillance is a constitutional requirement of any surveillance statute" (citation omitted)).

[124] 441 U.S. 238 (1979).

[125] *Id.* at 247–48 (discussing notice requirements in previous cases).

[126] *See id.* The array of knock-and-announce cases also emphasize the importance of notice, but, for slightly different reasons, focuses more on concerns about unnecessary police violence and destruction of property.

that law enforcement officials leave an inventory of property seized, thereby ensuring that the target knows what was taken and has an opportunity to reclaim it.[127]

Berger,[128] *Donovan*,[129] and *Dalia*[130] make clear that while protection of property and risk of escalating violence provide relevant justifications for a notice requirement, they are not the only justifications. In this trio of cases, there is no deprivation of property.[131] The phones or other devices used to communicate are not taken away or otherwise interfered with.[132] The participants can continue to engage in their ongoing communications, albeit with an extra set of ears.[133] And there is no direct police to citizen encounter that risks violent escalation.[134] Yet, these cases make clear that such forms of surveillance still require some form of notice, albeit ex post.[135] There are at least four reasons why this would be the case—and that this is the right result.

First, the risk of abuse. Notice is necessary to ensure citizens have the relevant information to respond to and protect themselves from abuse or overreach.[136] Without notice individuals will have no basis to object or push back against excessive surveillance.[137]

Second, the importance of trust. The Supreme Court has recognized this in connection with the issuance of ordinary warrants—describing the issuance of such warrants as assuring the citizen of the "lawful authority of the executing officer, his need to search, and the limits of his power to search."[138] Notice provisions do the same—assuring the citizen that the government is acting according to lawful authority and subject to required limits.[139]

Third, the protection of expressive freedom. When people fear they are being watched, their freedom is put at risk.[140] If the fear of secret surveillance is sufficiently strong or widespread, individuals will be less willing to experiment or express unpopular or unconventional ideas.[141] Notice requirements help minimize

---

[127] *See* U.S. CONST. amend. IV; FED. R. CRIM. P. 41(f)(1)(B)–(C).

[128] 388 U.S. 41 (1967).

[129] 429 U.S. 413 (1977).

[130] 441 U.S. 238 (1979).

[131] *See Dalia*, 441 U.S. at 241–42; *Donovan*, 429 U.S. at 418; *Berger*, 388 U.S. at 44–45.

[132] *See Dalia*, 441 U.S. at 241–42; *Donovan*, 429 U.S. at 418; *Berger*, 388 U.S. at 44–45.

[133] *See Dalia*, 441 U.S. at 241–42; *Donovan*, 429 U.S. at 418; *Berger*, 388 U.S. at 44–45.

[134] *Cf.* Hudson v. Michigan, 547 U.S. 586, 594 (2006) (discussing the potential danger of physical harm during a search).

[135] *See* FED. R. CRIM. P. 41(f).

[136] *See Donovan*, 429 U.S. at 439 ("[L]egislative history indicates that postintercept notice was designed instead to assure the community that the wiretap technique is reasonably employed.").

[137] *See id.*

[138] United States v. Chadwick, 433 U.S. 1, 9 (1977) (citing Camara v. Municipal Court, 387 U.S. 523, 532 (1967)).

[139] *See id.*

[140] *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (warning that governmental surveillance "chills associational and expressive freedoms").

[141] *See id.*

unfounded fears of surveillance by bringing out what kind of surveillance is being conducted into the open and minimizing the fear of unwatched watching.[142]

Fourth, the protection of democratic processes. Without transparency about what the government is doing in the name of security, there is no way for citizens to weigh in.[143] Without notice, and thus knowledge of governmental action, there is no way to assess whether the actions are something to support or whether to push for change.[144] Transparency—and hence notice requirements—is essential to meaningful democratic accountability.[145]

Yet, despite these potent concerns, no-notice warrants have consistently been issued pursuant to the SCA, often coupled with gag orders.[146] One possible explanation is the blithe application of the third party doctrine, pursuant to which there is no reasonable expectation of privacy in certain information transmitted to a third-party service provider.[147] According to this view, there is no Fourth Amendment concern at all.[148] But in light of *Warshak*,[149] this rationale fails with respect to the no-notice searches of emails;[150] *Warshak*, after all, concluded that emails *are* deemed protected by the Fourth Amendment, even though they are in the hands of a third party.[151]

Alternatively, courts have recognized that individuals retain a Fourth Amendment interest in at least some data (such as emails) held by third-party providers, but have concluded that notice to the third party is sufficient to meet the Fourth Amendment's requirements.[152] This, after all, is what Judge Robart relied on in comparing

---

[142] *See id.*

[143] *See* Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 896–98 (2006) ("[C]ontemporary political theorists place the publicity of government laws and actions at the core of democracy because it enables both the rational choice of the individual citizen and the full flowering of informed public debate by the collective.").

[144] *See id.*

[145] *See id.*

[146] *See, e.g.*, *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014); *In re* 381 Search Warrants Directed to Facebook, Inc., 78 N.E.3d 141 (N.Y. 2017). *But see, e.g.*, *In re* Grand Jury Subpoena for [Redacted]@yahoo.com, 79 F. Supp. 3d 1091 (N.D. Cal. 2015).

[147] *See, e.g.*, United States v. Alabi, 943 F. Supp. 2d 1201, 1245 (D.N.M. 2013) ("[T]here is no reasonable expectation of privacy in otherwise private information disclosed to a third party.").

[148] *See, e.g.*, *In re* United States, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009) ("Much of the reluctance to apply traditional notions of third party disclosure to the e-mail context seems to stem from a fundamental misunderstanding of the lack of privacy we all have in our e-mails. Some people seem to think that they are as private as letters, phone calls, or journal entries. The blunt fact is, they are not.").

[149] 631 F.3d 266 (6th Cir. 2010).

[150] *Id.* at 274.

[151] *See id.*

[152] *See* Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 916 (W.D. Wash. 2017); *In re* Grand Jury Subpoena for [Redacted]@yahoo.com, 79 F. Supp. 3d 1091, 1093–95

the situation presented by Microsoft in the gag order case to a warrant served on a stranger.[153] And other courts have reached analogous conclusions in this and other contexts.[154] If the government serves a warrant on FedEx for a particular package, for example, it need not separately notify the owner of that package.[155]

But there is a difference in kind between third-party search cases employing ordinary Rule 41 warrants and those searches carried out pursuant to the SCA.[156] In the "ordinary" cases, the stranger is permitted to publicize the fact of the search.[157] Similarly, FedEx is permitted to tell its customer—or anyone else.[158]

The SCA provisions are different because of the combination of the no-notice warrant *and* the gag order provisions.[159] There may, of course, be times in which the *practical* result is the same in both situations—if, for example, there is a search of a package sent via FedEx, no subsequent prosecution, and FedEx never informs its customer or otherwise publicizes the search. But, there is also an important difference. Concerned customers could demand notice. They could only contract with mailing services that commit to provide notice of governmental searches. In the SCA context, however, that is not possible. The provider may be *precluded* from giving notice.[160] It thus cannot contract with its customers to do something that U.S. law prohibits it from doing.[161]

(N.D. Cal. 2015). *Carpenter v. United States*, heard by the Supreme Court in November 2017, may further limit reliance on third-party doctrine as a basis for dismissing such Fourth Amendment concerns, at least as it applies to the collection of location information. 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402). For critiques of the third party doctrine, see, e.g., Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015); Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1117–19 (2006) (reviewing DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004)); Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 147–58; Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 40–44 (2011).

[153] *Microsoft*, 233 F. Supp. 3d at 916.

[154] *See, e.g.*, United States v. Bansal, 663 F.3d 634, 662–63 (3d Cir. 2011) (concluding that when property is in the hands of a third party, the Federal Rules of Criminal Procedure require notice to that third party and nothing more); United States v. Scully, 108 F. Supp. 3d 59, 83 (E.D.N.Y. 2015) ("There is no separate requirement that the officer provide the warrant, a receipt, or any other form of notice to the owner of the property." (quoting *In re* United States, 665 F. Supp. 2d 1210, 1221 (D. Or. 2009))); United States v. Henshaw, No. 15-00339-01-CR -W-BP, 2017 WL 1148469, at *6 (W.D. Mo. Feb. 24, 2017).

[155] *See, e.g.*, United States v. Zacher, 465 F.3d 336, 339 (8th Cir. 2006).

[156] *Compare* FED. R. CRIM. P. 41, *with* 18 U.S.C. § 2703 (2012).

[157] *See In re Grand Jury Subpoena*, 79 F. Supp. 3d at 1093.

[158] *See id.*

[159] *See id.* at 1093–95.

[160] *See* 18 U.S.C. § 2705(b) (2012).

[161] *See id.*

There is also a difference in degree. The scope and scale of information now in the hands of third parties is vast.[162] Third-party providers—at the behest of the government—can access that information with relative ease.[163] Police do not themselves have to go to a home, put themselves at risk, or track a target.[164] The quantity of searches is in no way limited by the number of available police officers.[165] As Justice Alito put it, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical."[166] In the digital age, the resource limitations that apply to searches and seizures of people and other tangible things are in many cases lifted, or at least greatly reduced.[167] Thus, the quantity of no-notice searches is exponentially greater than any comparable search or seizure of analogous tangible thing.[168]

Put simply, the simple analogies to the search of the stranger's home or of a package in FedEx's control fail to tell the full story or account for the full range of interests at stake.[169] The scale and scope of searches of digital evidence is likely much greater than comparable searches of their tangible counterparts.[170] There is as a result also a greater likelihood of searches with neither ex ante nor ex post notice by the government to the target.[171] The reasoning of *Berger*,[172] *Donovan*,[173] and *Dalia*[174] all highlight the resulting constitutional concerns.

B. Standing

The absence of notice to the target in these SCA warrant cases makes the third-party standing issue particularly acute.[175] As previously described, the combination

---

[162] *See generally* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring); United States v. Warshak, 631 F.3d 266, 295 (6th Cir. 2010).

[163] *See Jones*, 565 U.S. at 429 (Alito, J., concurring).

[164] *See id.*

[165] *See id.*

[166] *Id.*; *see* Illinois v. Lidster, 540 U.S. 419, 426 (2004) (emphasizing that "[p]ractical considerations—namely, limited police resources and community hostility to related traffic tieups—seem likely to inhibit any such proliferation" of sobriety checkpoints); *see also* Neil Richards, *Secret Government Searches and Digital Civil Liberties*, NAT'L CONST. CTR., https://constitutioncenter.org/digital-privacy/secret-searches-and-seizures-and-digital-civil-liberties#footnote-ref-22 [https://perma.cc/VQ5J-3FQP] (last visited Dec. 4, 2017).

[167] *See Jones*, 565 U.S. at 429 (Alito, J., concurring).

[168] *See id.*

[169] Notably, I am not alone in raising these concerns. *See, e.g.*, Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH L.J. 117, 185–88 (2012); Smith, *supra* note 88; *see also* Richards, *supra* note 152, at 1125.

[170] *See Jones*, 565 U.S. at 429 (Alito, J., concurring).

[171] *See, e.g.*, Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 916 (W.D. Wash. 2017).

[172] 388 U.S. 41 (1967).

[173] 429 U.S. 413 (1977).

[174] 441 U.S. 238 (1979).

[175] *See Microsoft*, 233 F. Supp. 3d at 897.

of no-notice provisions and restrictive third-party standing rules means that there will be *no one* who can raise a Fourth Amendment claim, in at least some non-negligible set of cases, for some potentially extended period of time.[176] Contrary to Judge Robart's decision in the Microsoft case, this seems like exactly the kind of special circumstance that should justify third-party provider standing in these cases—particularly given that in several situations presented to Judge Robart, no-notice warrants were coupled with gag orders of indefinite duration.[177] In fact, a brief examination of the key Supreme Court cases that Judge Robart relied on suggests that they are not as limiting as Judge Robart assumed (although to be fair, Judge Robart was also hemmed in by a series of Ninth Circuit precedent that are beyond the scope of what I address here).[178]

In *Alderman v. United States*,[179] the Court reaffirmed the idea that Fourth Amendment rights are personal rights that cannot be "vicariously asserted."[180] But the ruling arose in the context of an assertion of the exclusionary rule and seemed to turn in part on the fact that there was someone who could challenge the search, even if the defendant in the criminal case could not.[181] The Court explicitly emphasized that the actual "victim can and very probably will object for himself when and if it becomes important for him to do so."[182] Similarly, in *Rakas v. Illinois*,[183] the Court made clear that only individuals whose reasonable expectation of privacy has been violated can seek to exclude evidence based on a Fourth Amendment violation.[184] But there, too, the *Rakas* Court emphasized that "[t]here is no reason to think that a party whose rights have been infringed will not, if evidence is used against him, have ample motivation . . . to suppress it."[185]

In other contexts in which the Court has stated that entities cannot bring Fourth Amendment claims, the actual target of the relevant government action is on notice and thus has an opportunity to object. In *California Bankers Ass'n v. Schultz*,[186] for example, the Supreme Court cursorily rejected a bank's authority to vicariously assert the Fourth Amendment claims of depositors engaged in the kind of $10,000 domestic currency transactions that triggered the relevant reporting requirements.[187] But depositors who fell in this category presumably could have raised concerns.[188] The

---

176 *See id.* at 916.
177 *Id.* at 912–16.
178 *See id.*
179 394 U.S. 165 (1969).
180 *Id.* at 174 (citations omitted).
181 *See id.* at 171–86.
182 *Id.* at 174.
183 439 U.S. 128 (1978).
184 *Id.* at 143–49.
185 *Id.* at 134 (citing *Alderman*, 394 U.S. at 174).
186 416 U.S. 21 (1974).
187 *Id.* at 67–68.
188 *See id.*

situation presented by the Microsoft litigation[189] was quite different. In that case, the persons whose Fourth Amendment rights were implicated—what the *Alderman* court calls the "victim"[190]—has no ability to raise the claims because they were not, and cannot be, told of the search.[191] Given the issuance of indefinite no-notice orders, they might never be told of the search.[192]

In such situations, Microsoft's contention that there are "special circumstances" seems correct.[193] After all, the Supreme Court, albeit in contexts that do not involve the Fourth Amendment, has recognized the need to relax standing rules in analogous situations. In *NAACP v. Alabama*,[194] for example, the Court permitted the NAACP to bring a due process claim on behalf of its members; the Court emphasized that it was dealing with a situation in which the "constitutional rights of persons who are not immediately before the Court could not be effectively vindicated except through an appropriate representative."[195] Similarly, in *Barrows v. Jackson*,[196] the Supreme Court concluded that standing rules should be relaxed in an equal protection case when there is a risk that state action could yield a denial of constitutional rights and "it would be difficult if not impossible for the persons whose rights are asserted to present their grievance before any court."[197] To be sure, these cases did not involve Fourth Amendment claims, but the principle is analogous whether one is discussing Fourth or First Amendment rights.[198] Those directly implicated by government action may not be in a position to challenge it; in those cases, third-party adjudication may be the only—or best—mechanism for certain grievances to be heard, and thus key constitutional rights adequately protected.[199]

Microsoft thus seems correct in its application of the factors laid out in *Powers v. Ohio*,[200] the leading case on third-party standing. As the *Powers* Court concluded, third-party standing may be appropriate when the following three factors are met: (1) the litigant experienced an "injury in fact," therefore providing him or her with a "sufficiently concrete interest" in the outcome of the dispute;[201] (2) the litigant has

---

[189] Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887 (W.D. Wash. 2017).

[190] *See Alderman*, 394 U.S. at 174; *supra* notes 179–82 and accompanying text.

[191] *See Microsoft*, 233 F. Supp. 3d at 916; *see also* Rakas v. Illinois, 439 U.S. 128, 133 (1978) (reaffirming that Fourth Amendment rights may not be asserted vicariously).

[192] *See Microsoft*, 233 F. Supp. 3d at 916.

[193] *See* Microsoft's Supplemental Brief on Motion to Dismiss in Response to Court's Minute Order at 1, *Microsoft*, 233 F. Supp. 3d 887 (No. 2:16-cv-00538-JLR).

[194] 357 U.S. 449 (1958).

[195] *Id.* at 459.

[196] 346 U.S. 249 (1953).

[197] *Id.* at 257.

[198] *See generally NAACP*, 357 U.S. 449; *Barrows*, 346 U.S. 249.

[199] *See generally NAACP*, 357 U.S. 449; *Barrows*, 346 U.S. 249.

[200] 499 U.S. 400 (1991).

[201] *Id.* at 411 (quoting Singleton v. Wulff, 428 U.S. 106, 112 (1976)).

a "close relation to the third party;"[202] and (3) there is "some hindrance to the third party's ability to protect his or her own interests."[203]

In cases involving no-notice search warrants coupled with gag orders of indefinite duration, the third factor is clearly met. The third party cannot protect his or her own interests if he or she lacks any knowledge of the search and seizure. This is a particular concern in cases involving indefinite gag orders. But even in cases where the target is eventually told, however, the delay period can be prolonged. The Department of Justice, for example, talks about gag orders of "only" a year.[204] But during that year, the government may collect, and perhaps disseminate, a significant amount of information about a target. That information can be used in support of a whole host of additional investigative measures or civil sanctions, even if it does not ever yield criminal sanctions. Moreover, that year-long delay period can be renewed.[205] During that time period, there is a clear hindrance in the target's ability to assert his or her rights—with potential consequences for the affected target.

In most circumstances, the first and second factors are also met. A third-party provider presumably suffers some injury—in the form of lost time and resources—in carrying out the search. To the extent that the provider complies in a way that undermines, or is perceived as undermining, its customers' interests, it can have a broader economic cost in terms of lost business. And as the entity entrusted to manage individuals' most personal communications, the provider also arguably has a sufficiently close relationship with its customers to bring a claim on their behalf.

Put another way, it seems that the Supreme Court case law is not nearly as clear-cut as it has been portrayed. After all, no Supreme Court case explicitly precludes courts from permitting third-party assertions of Fourth Amendment rights in those limited situations where the *Powers* factors are met.[206] It seems that if the target is denied any information about the search, providers should be permitted to raise relevant Fourth Amendment concerns in the targets' stead.

C. Ex Ante or Ex Post Challenges

There is, however, a key question as to the timing of a permitted challenge. After all, most of the case law seems to suggest that ex post challenges to warrants should be permitted, but that ex ante notice of searches and seizures—and thus challenges—can be delayed.[207] Moreover, the kind of destruction of property and escalation of violence concerns that support the need for ex ante notice simply do

---

[202] *Id.* (citing *Singleton*, 428 U.S. at 113–14).
[203] *Id.* (citing *Singleton*, 428 U.S. at 115–16).
[204] *See* Rosenstein Memorandum, *supra* note 20.
[205] *See id.*
[206] *See Powers*, 499 U.S. at 411.
[207] *See, e.g.*, *In re* Grand Jury Subpoena for [Redacted]@yahoo.com, 79 F. Supp. 3d 1091, 1093–95 (N.D. Cal. 2015).

not apply when the government is asking a third-party provider to access data on its behalf.[208] Yet, the kind of challenges both Facebook and Microsoft are seeking come in the form of an ex ante check: a motion to quash the warrant.[209]

There is both precedent and good reason for permitting such ex ante challenges. These kinds of search warrants are in key respects analogous to subpoenas.[210] They do not involve a direct police search of a person or place.[211] Rather, they—like a subpoena—compel a company to produce information in its custody or control.[212] To be sure, the government must satisfy the higher substantive standard of a finding of probable cause; but this does not change the fact that the warrant operates, like a subpoena, as a form of compelled disclosure.[213] As a general matter, a company being subpoenaed for records can file a motion to quash.[214] Providers served with a warrant should be permitted to do so as well, particularly in those situations when their customers are not provided notice of the search. And perhaps—as the dissenting judge in the Facebook case persuasively argued[215]—in all contexts. This is the case for at least four reasons.

First, providers are often "best placed" to safeguard the rights at issue.[216] They are likely to be better equipped to understand the relevant issues and better equipped to raise challenges if and when there is a violation of the target's rights.

Second, the risk of proliferation and dissemination of collected data highlights the importance of ex ante review—protecting against the collection before it even takes place.

Third, it makes logical sense to allow for ex ante challenges in this context. It is, after all, not clear at what point ex parte (versus ex ante) review would occur. The obvious choice would be at the point in time of target notice. At that point, the target could specify whether or not he or she wished the provider to pursue a claim on his or her behalf. But the extended period of secrecy—even with a default maximum of one year absent renewal[217]—highlights the need for some sort of effective, advance checking, prior to target notice.

---

[208] *See* Hudson v. Michigan, 547 U.S. 586, 594 (2006) (discussing potential violence and destruction that might accompany a search).

[209] *See In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 468 (S.D.N.Y. 2014); *In re* 381 Search Warrants Directed to Facebook, Inc., 78 N.E.3d 141, 143 (N.Y. 2017).

[210] *See In re Warrant to Search*, 15 F. Supp. 3d at 471.

[211] *See id.*

[212] *Id.* at 469.

[213] *See id.* at 470.

[214] *See generally* FED. R. CIV. P. 45(d)(3).

[215] *See In re* 381 Search Warrants Directed to Facebook, Inc., 78 N.E.3d 141, 159–63 (N.Y. 2017) (Wilson, J., dissenting).

[216] *See id.* at 173.

[217] *See* Rosenstein Memorandum, *supra* note 20.

Fourth, the sensitivity of the information—as indicated by the obligation to get a warrant—heightens, not diminishes, the importance of such pre-enforcement challenges.

III. A STATUTORY FIX

The doctrine can and should evolve to reflect the concerns raised by the combination of no-notice warrants, gag orders, and a restrictive interpretation of third-party standing rules. But doctrinal changes are slow. Rather than wait for the needed evolution of the case law, these issues can—and should—be resolved via amendments to the SCA. Here, I suggest three:

First, require notice in connection with the issuance of warrants for content. Under the current statute, notice is required when the government obtains content via a court order that falls short of the warrant requirement and when it obtains content via a subpoena; it need not provide notice when it obtains data via a warrant.[218] This distinction cannot be supported, given the importance of notice to vindicating the interests that the Fourth Amendment is meant to protect.[219]

Specifically, the statute should be updated to require notice in connection with the issuance of warrants. The delayed notice provisions should also apply, permitting the government to delay notice in cases where such notice would impede the investigation or otherwise cause an "adverse result," as that term has been defined in the statute.[220]

Second, the SCA should be amended to include time limits on gag orders that match the time limits associated with the delayed notice orders. Delayed notice orders issued in conjunction with § 2703(d) orders and subpoenas can be granted for renewable periods of ninety days.[221] The gag order provisions should track those requirements—and any such delayed notice provisions implemented in connection with warrants. There is in fact no legitimate justification for a gag order that persists longer than a delayed notification order.

Third, providers should be given explicit authorization to raise Fourth Amendment claims and other challenges based on the burden imposed by the full range of orders to disclose, including subpoena, court order, and warrant. Providers are often the best, if not the only, party situated to assess the legitimacy of the government's actions and push back on requests that are overly broad or arguably unconstitutional.[222]

---

[218] *See* 18 U.S.C. § 2703(b) (2012). As discussed previously, however, the government has, since the Sixth Circuit ruling in *Warshak*, adopted a practice which always obtains a warrant when it is seeking content for purposes of a criminal investigation. *See supra* notes 32–36 and accompanying text.

[219] *See, e.g.*, Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 916 (W.D. Wash. 2017).

[220] *See* 18 U.S.C. § 2705(a)(1)(B)(2) (2012).

[221] *Id.* § 2705(a)(1)(B)(4).

[222] *See* Brief of Appellant, *supra* note 90, at 30.

Given the increasingly important role these intermediaries play in managing our data and responding to disclosure demands from law enforcement officials, they should be permitted to bring claims on their customers' behalf. This does not mean that they always will—or should—either bring a challenge or win. Whether or not the warrant or any other compulsory order will be enforced ultimately will—and should—be decided by a judge.

The statute also should be written in a way that ensures the government can access critical information as any such challenge proceeds. Specifically, the provider should be obliged to produce the information if it loses its initial motion to quash. If the provider wins on appeal, then the government should be precluded from using the information that has been obtained in any criminal case.

CONCLUSION

The rise of digitized communications is not only changing the ways in which the citizenry interacts with one another, but also changing the interactions between citizens and the police. Increasingly, law enforcement officials are seeking data from third-party providers, without the knowledge of or any notice to the target of the search and seizure. Meanwhile, providers are precluded from bringing Fourth Amendment challenges to these searches and seizures, even in situations in which they are the only ones with knowledge of what the government is doing. This kind of secret searching creates the risk of abuse and overreach, threatens to erode trust in law enforcement, and eliminates the kind of transparency that is essential to the effective functioning of a democracy.