Michigan Law Review

Volume 117 | Issue 8

2019

Secret Searches: The SCA's Standing Conundrum

Aviv S. Halpern
University of Michigan Law School

Follow this and additional works at: https://repository.law.umich.edu/mlr

 Part of the Fourth Amendment Commons, Law Enforcement and Corrections Commons, Legislation Commons, and the Privacy Law Commons

Recommended Citation
Aviv S. Halpern, *Secret Searches: The SCA's Standing Conundrum*, 117 MICH. L. REV. 1697 (2019).
Available at: https://repository.law.umich.edu/mlr/vol117/iss8/5

https://doi.org/10.36644/mlr.117.8.secret

This Note is brought to you for free and open access by the Michigan Law Review at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Michigan Law Review by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

NOTE

SECRET SEARCHES: THE SCA'S STANDING CONUNDRUM

*Aviv S. Halpern**

The Stored Communications Act ("SCA") arms federal law enforcement agencies with the ability to use a special type of warrant to access users' electronically stored communications. In some circumstances, SCA warrants can require service providers to bundle and produce a user's electronically stored communications without ever disclosing the existence of the warrant to the individual user until charges are brought. Users that are charged will ultimately receive notice of the search after the fact through their legal proceedings. Users that are never charged, however, may never know that their communications were obtained and searched. This practice effectively makes the provisions of the SCA that allow for nondisclosure unreviewable by the judiciary. Users that were searched but not charged have standing to challenge the scope of these warrants, but receive no notice that the search occurred. Service providers receive notice, but have no standing on behalf of their users under the Fourth Amendment. This Note argues that the nondisclosure orders therefore create a procedural due process violation in addition to a Fourth Amendment violation. Users may have their privacy and property interests infringed without a meaningful opportunity to be heard. Under a due process theory, as opposed to a Fourth Amendment theory, this practice can finally be judicially reviewed.

TABLE OF CONTENTS

* J.D. Candidate, May 2019, University of Michigan Law School. Thank you to every *Michigan Law Review* editor who worked on this piece. Particular thanks to Michael Abrams, Ryan Marosy, Sarah Mezera, Jun Ha Park, and Carolina Velarde for being extraordinary editors, thoughtful contributors, and great friends. Finally, thank you to my fiancée, Noreen Raja, for the support and for convincing me to put aside my tinfoil hat long enough to research and write this piece.

INTRODUCTION

Access to the internet has become such an integral part of society that the United Nations has declared it a fundamental human right.[1] Even the Supreme Court has acknowledged that we are officially in the "Cyber Age."[2] But because internet access and online storage require third-party service providers, there may be significant constitutional issues with respect to electronically stored information ("ESI"). Under the third-party doctrine, the Fourth Amendment generally does not protect information disclosed to third parties.[3] And because electronic communications often require the involvement of third-party service providers, it is unclear whether the Fourth Amendment provides any meaningful protection to information stored by third parties,[4] let alone electronically stored communications ("ESC").[5] The risk of providing the government with unfettered access to potentially sensitive ESI motivated Congress to pass the Stored Communications Act

1. Tim Sandle, *UN Thinks Internet Access Is a Human Right*, BUS. INSIDER (July 22, 2016, 11:57 PM), http://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7 [https://perma.cc/PW44-L8W5].

2. Carpenter v. United States, 138 S. Ct. 2206, 2224 (2018) (Kennedy, J., dissenting) ("It is true that the Cyber Age has vast potential both to expand and restrict individual freedoms in dimensions not contemplated in earlier times.").

3. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443–44 (1976). *But see Carpenter*, 138 S. Ct. at 2217 (declining to extend *Smith* and *Miller* to cover historical cell-site location information).

4. How the third-party doctrine will extend beyond *Carpenter* is still an open question. As of now, several theories could arguably cover electronically stored communications, but none are widely, or even consistently, applied. *See, e.g.*, Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (mosaic theory); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1025–29 (2010) (content/non-content).

5. Because the Stored Communications Act primarily applies to ESC—a narrow subset of ESI—most of the following analysis will be limited to electronic communications. Explicit language will be used to delineate when a portion of the analysis applies strictly to ESC or more broadly to ESI. *See* 18 U.S.C. § 2703 (2012).

("SCA"),[6] ensuring that at least *some* protection extends to electronic information.[7]

Congress passed the SCA in 1986, before the infrastructure and capabilities of the internet were truly understood.[8] The SCA provides a statutory framework for determining when the government can access certain types of ESC from third-party service providers.[9] More specifically, the Act enumerates special tools for government agents to access ESC—including subpoenas, court orders, and warrants ("SCA warrants")—and permits searches without notice.[10]

Sometimes, with the use of nondisclosure orders, the Act even *prohibits* service providers from informing targeted users of a search. Until recently, many of the nondisclosure orders existed in perpetuity—preventing any notice to the user.[11] Because of an October 2017 guidance document issued by the Department of Justice, federal prosecutors may prevent disclosure for up to one year.[12] In some circumstances, "federal prosecutors can seek gag or-

---

6. 18 U.S.C. §§ 2701–2713. The Stored Communications Act has confusingly been referred to by many names: the "Electronic Communications Privacy Act" or "ECPA" because it was part of a larger bill amending the Wiretap Act; "Chapter 121" because it was codified in Chapter 121 of Title 18 of the United States Code; the "Stored Wire and Electronic Communications and Transactional Records Access" statute because of its formal title in Chapter 121; and "Title II" because it was originally enacted as the second title to the ECPA. 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 n.1 (2004) [hereinafter Kerr, *A User's Guide*]; *see also* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 382 (2014). For the sake of simplicity, I will refer to it simply as the "Stored Communication Act," or "SCA."

7. *See* 18 U.S.C. §§ 2701, 2703, 2707 (creating criminal penalties, setting forth procedures limiting government access, and creating a private right of action to remedy conduct that fails to comply).

8. The Stored Communications Act was largely built around the two predominant functions of the internet in 1986: electronic communications services and remote computing services. *See* Kerr, *A User's Guide*, *supra* note 6, at 1213–14. These distinctions are outmoded and do not truly reflect how computer networks work in the modern age. They have resulted in "freezing into law the understandings of computer network use as of 1986." *Id.* at 1214. But this conception is significantly different from the modern understanding of the internet. The World Wide Web, cloud computing services, and online social networks would not exist for another decade. Ryan A. Ward, Note, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 HARV. J.L. & TECH. 563, 566 (2011).

9. *See* 18 U.S.C. § 2703.

10. *Id.*

11. Jennifer Daskal, *Notice and Standing in the Fourth Amendment: Searches of Personal Data*, 26 WM. & MARY BILL RTS. J. 437, 439–40 (2017) (citing 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 [https://perma.cc/P45J-DAR7]).

12. Rod J. Rosenstein, *Memorandum to Heads of Department Law Enforcement Components*, U.S. DEP'T JUST. 2 (Oct. 19, 2017), https://www.justice.gov/criminal-ccips/page/file/1005791/download [https://perma.cc/5XKP-M3Y6], cited in Daskal, *supra* note 11, at 440.

ders that last longer than a year. . . . The guidance does not bind state prosecutors."[13]

Although this guidance changes federal policy, it has not yet been adopted into law. In the meantime, the government is still afforded the ability to conduct searches without, or with significantly delayed, notice. This practice means that, during the period of secrecy, there is no one with both standing and notice to challenge the search or seizure, "thus eliminating one of the most powerful checks on government overreach."[14]

Challenges to SCA warrants on Fourth Amendment grounds have failed. Fourth Amendment standing doctrine limits challenges to claimants whose own reasonable expectations of privacy were violated.[15] Courts have yet to address, however, whether a procedural due process challenge would permit third-party standing. Because the statute does not require authorities to notify a user of a search, the following circumstance arises: the user, who has standing under the Fourth Amendment but no notice of the search, cannot challenge the search or seizure; whereas the service provider, who has notice but no Fourth Amendment standing, cannot assert the user's rights. This Note argues that due process claims—as opposed to Fourth Amendment claims—can overcome this standing conundrum. The due process theory allows for a novel standing argument that should circumvent the Fourth Amendment's barriers to third-party standing and finally provide an opportunity to check government overreach. The search and seizure deprives the user of property and privacy interests in their communications without a meaningful opportunity to be heard.[16] And because the statute lacks a data-deletion requirement, the deprivation could potentially be indefinite.

This Note analyzes these due process concerns. It proposes legislative action and suggests alternative theories to assert users' rights until legislative action is taken. Part I provides background information on the history and role of the SCA. Part II explains the Fourth Amendment standing problem and how the nondisclosure orders make SCA warrants unreviewable because no one with standing will have notice. Part III argues that use of SCA warrants presents unique procedural due process concerns because of the lack of

13. Daskal, *supra* note 11, at 440; *see also* Rosenstein, *supra* note 12, at 2.

14. Daskal, *supra* note 11, at 441.

15. Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 137 (2008); *see, e.g.*, Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 915 (W.D. Wash. 2017) ("Based on the foregoing analysis, the court concludes that Microsoft may not bring a claim to vindicate its customers' Fourth Amendment rights. Although the Supreme Court and the Ninth Circuit routinely employ the third-party standing doctrine to cases involving constitutional rights, that doctrine is in tension with Fourth Amendment jurisprudence."); *In re* 381 Search Warrants Directed to Facebook, Inc., 14 N.Y.S.3d 23 (App. Div. 2015) (rejecting Facebook's pre-enforcement challenge regarding the scope of nearly 400 "bulk" warrants served with indefinite nondisclosure orders).

16. In a broader article, Judge Stephen Wm. Smith briefly identifies the standing issue that arises in these circumstances. *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 330 (2012).

notice and an opportunity to be heard. Then, Part VI lays out the third-party standing argument under a due process theory.

I. THE INTERSECTION OF FOURTH AMENDMENT JURISPRUDENCE AND THE INTERNET

Traditional Fourth Amendment jurisprudence does not neatly apply to modern technological advancements.[17] Intended to protect individuals from government overreach, the reasonableness requirement of the Fourth Amendment restricts the government's ability to search and to seize, whereas warrants provide a legal tool that authorizes it to do so.[18] Warrantless searches, on the other hand, are "*per se* unreasonable under the Fourth Amendment," subject only to a few exceptions.[19] Administrative searches are one such exception. In these cases, a "special need" makes the warrant and probable-cause requirements impracticable when seeking information from third-party records.[20]

But Fourth Amendment doctrine was developed for physical spaces, not cyberspace.[21] The doctrine's foray into the cyberworld has been fraught with difficulty and unease; electronic communications are no exception. So, to provide guidance on procedures when seeking access to ESI, Congress passed the Stored Communications Act.[22] This Part will broadly discuss the application of the Fourth Amendment to ESI, specifically focusing on the

---

17. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

18. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 333 (2015). The Fourth Amendment states:

> The 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 Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

19. Katz v. United States, 389 U.S. 347, 357 (1967); *see also* Massachusetts v. Sheppard, 468 U.S. 981, 988 n.5 (1984) ("[A] search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional.").

20. City of Los Angeles v. Patel, 135 S. Ct. 2443, 2452 (2015). There are several other exceptions to the warrant requirement, but none of them seem to apply as explicitly as the administrative search exception. *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149, 152–53 (2004) (border search exception); California v. Acevedo, 500 U.S. 565, 573 (1991) (automobile exception); Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (consent exception); Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (plain view exception); Chimel v. California, 395 U.S. 752, 762–63 (1969) (search incident to arrest exception); Terry v. Ohio, 392 U.S. 1, 20 (1968) (*Terry* stop exception).

21. *See* United States v. Jones, 565 U.S. 400, 405 (2012) ("The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to 'the right of the people to be secure against unreasonable searches and seizures'; the phrase 'in their persons, houses, papers, and effects' would have been superfluous." (quoting U.S. CONST. amend. IV)).

22. 18 U.S.C. §§ 2701–13 (2012).

SCA. Section I.A explains the role of the SCA. Section I.B lays out the statutory framework governing access to electronic communications. Section I.C explores the differences between traditional warrants and SCA warrants and explains how the differences can result in the denial of an individual's procedural due process right.

A. *The SCA's Role as a Legislative Protection for ESC*

After "the advent of computerized recordkeeping systems,"[23] Congress became increasingly concerned about the potential "erosion of [the] precious right" to privacy.[24] And at the time, the third-party doctrine seemed to operate as a bright-line rule, discarding any expectation of privacy in information shared with a third party[25]—like a company operating a recordkeeping system. This led to concerns that network and internet activities would be outside Fourth Amendment protection.[26] The Fourth Amendment only reaches spaces considered to be constitutionally protected, such as a person's home,[27] as well as other areas where someone has a reasonable expectation of privacy, such as a phone booth.[28]

When accessing computer networks, such as the internet, there is no physical "home" to consider.[29] In other words, one's physical location when accessing the internet does not change Fourth Amendment analysis. Whether a "conversation" over a computer network occurred while the participants were physically inside their homes does not provide any additional protection. Yet, if the conversation occurred in person between two individuals inside their home, it would likely be protected. The internet complicates matters because, unlike a physical conversation, accessing computer networks and recordkeeping systems often requires the cooperation of third-party service providers, potentially diminishing any expectation of privacy in the information.[30]

The SCA exists to address these concerns and provide statutory protections for ESC,[31] extending some of the traditional Fourth Amendment pro-

---

23. S. REP. NO. 99-541, at 3 (1986).

24. H.R. REP. NO. 99-647, at 19 (1986).

25. *See supra* note 3 and accompanying text.

26. S. REP. NO. 99-541, at 3 (1986).

27. *See* Payton v. New York, 445 U.S. 573, 586–87 (1980); *see also* United States v. Jones, 565 U.S. 400, 405 (2012) (revitalizing the property approach to the Fourth Amendment).

28. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

29. Kerr, *A User's Guide*, *supra* note 6, at 1209.

30. S. REP. NO. 99-541, at 3 (1986) ("Nevertheless, because it is subject to control by a third-party computer operator, the information may be subject to no constitutional privacy protection.").

31. The architecture of computer networks has had "profound consequences for how the Fourth Amendment protects Internet communications—or perhaps more accurately, how the Fourth Amendment may not protect such communications much at all." Kerr, *A User's Guide*, *supra* note 6, at 1210.

tections to an area of law fraught with uncertainty.[32] Further indicative of its intent, Congress baked the traditional warrant requirement of Federal Rule of Criminal Procedure 41 ("Rule 41") into the statute.[33] But at the time the SCA was passed, Congress did not yet understand how old legal doctrines—let alone the Fourth Amendment—would apply to the internet.[34] Since 1986, however, the internet has changed. Internet access still requires a third-party service provider, but service providers can no longer be classified neatly into the regulated categories the SCA created.

B. *Statutory Framework for Governmental Access to ESC*

To access ESC from a third-party service provider, government agencies must navigate the SCA framework.[35] First, a government agency must classify the holder of the information as either an electronic communications service[36] or as a remote computing service.[37] This distinction is based on Congress's understanding of how the internet operated in 1986. An electronic communications service uses computer networks to allow users to communicate with one another.[38] When sending and receiving electronic communications on the 1980s internet, it was common for service providers to temporarily store data pending delivery.[39] Sometimes this data was backed up in temporary "electronic storage" for several months.[40] Alternatively, a remote computing service is a third-party service that provides sophisticated data processing or storage.[41] In an era before spreadsheet software, users transmitted their data to a third-party computing service for processing or

32. *See* S. REP. NO. 99-541, at 3; H.R. REP. NO. 99-647, at 17–19 (1986).

33. *See* 18 U.S.C. § 2703(a), (b)(1)(A) (2012); *see also* FED. R. CRIM. P. 41.

34. Before Congress passed the SCA in 1986, courts were confused about the applicability of certain laws to the internet. *E.g.*, Briggs v. Am. Air Filter Co., 630 F.2d 414, 415 (5th Cir. 1980) (calling the Wiretap Act an "amorphous Congressional enactment" requiring the court to traverse the "fog of inclusions and exclusions" to apply them to the case at bar). The subsequent amendments to the Wiretap Act and the adoption of the modern SCA framework did little to clear up such confusion. *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("Courts have struggled to analyze problems involving modern technology within the confines of [the SCA] framework, often with unsatisfying results."); United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) ("When the Fifth Circuit observed that the Wiretap Act 'is famous (if not infamous) for its lack of clarity,' . . . it might have put the matter too lightly."). For a more in-depth explanation of some of the difficulties the SCA was intended to address, see Kerr, *A User's Guide*, *supra* note 6, at 1209–13.

35. *See* 18 U.S.C. §§ 2701–11.

36. *See id.* § 2703(a), (c).

37. *See id.* § 2703(b)–(c).

38. *Id.* §§ 2711(1), 2510(15). Electronic communications services include email services, Facebook Messenger, and most other direct messaging systems.

39. S. REP. NO. 99-541, at 2–3, 16 (1986).

40. Kerr, *A User's Guide*, *supra* note 6, at 1213.

41. S. REP. NO. 99-541, at 10–11.

storage[42]—tasks that today can be accomplished using a simple program without need for outsourcing.[43]

Although this classification scheme is outmoded and has largely become an exercise of confusing line drawing, the existing SCA framework requires courts to draw these distinctions so they can determine which rules apply. At times, courts have even concluded that the same service provider is an "electronic communication service" for some content and a "remote computing service" for other content.[44] But it is also possible for a service provider not to fit in either category. To illustrate, imagine Jack sends an email to Jill.[45] Before Jill opens the email, Jill's ISP service acts as an electronic communication service: the email is in temporary electronic storage until Jill retrieves the email.[46] Once the message is retrieved, Jill can either delete the email, download it as a file, or leave it on the ISP's server for safekeeping. If the email remains on the ISP's server, the ISP's role has changed to a remote computing service.[47] If the message is downloaded, the ISP is no longer either an electronic communications service or a remote computing service.[48] If it is neither an electronic communications service nor a remote computing service, the traditional Fourth Amendment protections apply rather than the SCA.[49] Classifying service providers becomes even more confusing when the SCA is applied to near-instantaneous communications through services such as Facebook Messenger.[50] Facebook would be an electronic communications service for any unopened messages but a remote computing service for opened messages that were not deleted. Ultimately, the electronic communications service and remote computing service dichotomy can be quite significant because the scope of the SCA's privacy protection depends on the classification.[51]

---

42. *Id.*

43. Kerr, *A User's Guide*, *supra* note 6, at 1214. Modern services that fall within this definition likely include cloud storage services and online compression software.

44. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 982, 987–88, 990 (C.D. Cal. 2010). For a proposal to simplify the SCA and eliminate the ECS and RCS distinctions, see Kerr, *A User's Guide*, *supra* note 6, at 1235–38.

45. For another example, see Kerr, *A User's Guide*, *supra* note 6, at 1216–17.

46. *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461–62 (5th Cir. 1994).

47. H.R. REP. NO. 99-647, at 64–65 (1986) (delineating between unopened and opened emails stored on servers and noting that opened emails stored on a server are protected by the provisions for remote computing services).

48. Kerr, *A User's Guide*, *supra* note 6, at 1216–17.

49. *Id.* at 1216.

50. Facebook Messenger is an instant messaging service on the Facebook platform that allows users to send text, video, or picture messages to one another. *Can I Unsend a Message on Facebook Once It Has Been Sent?*, FACEBOOK: HELP CENTER, https://www.facebook.com/help/messenger-app/android/1419818118281034 [https://perma.cc/U8AQ-9YUD].

51. *Compare* 18 U.S.C. § 2703(a) (2012), *with id.* § 2703(b).

After classifying the service provider, the agency may choose from three information-gathering tools: a court order, a subpoena, or a warrant.[52] This choice is largely driven by the type of ESI sought, as each tool has its own advantages, disadvantages, and scope.[53] For ESC held by an electronic communications service for 180 days or fewer, the SCA requires a search warrant, though the statute is silent on whether notice will be provided to the user.[54] There is even less statutory protection for ESC held for over 180 days or ESC held by remote computing services.[55] With an SCA warrant, a law enforcement entity can compel disclosure of ESI from a remote computing service "*without* required notice to the [user]."[56] Moreover, the government may seek a § 2705(b) order—a nondisclosure order that prohibits the service provider from informing the targeted user of the search.[57]

Notably, these tools permit access beyond just ESC.[58] Under this statutory scheme, the government can access a significant amount of private information,[59] but unlike with traditional warrants, if any notice is given at all, it will likely be after a long period of time. This key difference diminishes or eliminates a fundamental check on government overreach.

II. THE NOTICE–STANDING TWO-STEP

When used in conjunction with nondisclosure orders, SCA warrants can sometimes become unreviewable. If a user is not given notice of a search, the

52. *Id.* § 2703.

53. The rules compelling disclosure are structured as an upside-down pyramid. Kerr, *A User's Guide*, *supra* note 6, at 1222–24. At the base are subpoenas. 18 U.S.C. § 2703(c)(2). If a subpoena is combined with prior notice, a government entity can compel three types of information: basic subscriber information, *id.*; any opened emails or other permanently held files (through the remote computing service rules), *id.* § 2703(b); and any contents in temporary "electronic storage" (such as unretrieved emails) that have been in storage for more than 180 days, *id.* § 2703(a). Next are court orders. *Id.* § 2703(b)(B)(ii), (c)(1)(B). With these orders, described by § 2703(d), and prior notice, an entity can compel all non-content records, *id.* § 2703(c)(2); any opened emails or other permanently held files (also covered by the remote computing service rules), *id.* § 2703(b); and any contents in temporary "electronic storage" that have been in storage for more than 180 days, § 2703(a). Lastly are SCA warrants, which can compel everything, including ESC that has been in storage for less than 180 days. *See id.* § 2703(a), (c).

54. *Id.* § 2703(a).

55. *See id.* § 2703(a)–(b).

56. *Id.* § 2703(b)(1)(A), (c) (emphasis added). If the entity utilizes a court order or subpoena, notice can be delayed under *id.* § 2705.

57. *Id.* § 2705(b).

58. *See id.* § 2703(c) ("A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) . . . ."). This information can include, but is not limited to, the user's name, address, telephone and communication records, and means and source of payments. *Id.* § 2703(c)(2).

59. I discuss the difficulty with the particularity requirement in Section II.A *infra*.

targeted user has standing, but no notice; the service provider has notice, but no standing. This Part explains this conundrum. Section II.A explains the key differences between SCA warrants and traditional warrants. Section II.B then describes the Fourth Amendment standing issue that results.

A. *SCA Warrants and Traditional Warrants*

Traditional warrants are distinct from SCA warrants in a few key respects. First, traditional warrants are limited and have a more stringent particularity requirement. Second, traditional warrants provide for notice to the party whose information was searched. Finally, traditional warrants include procedures for the return or destruction of information obtained.

The first difference between SCA warrants and traditional warrants is the requisite level of particularity. The Fourth Amendment requires that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized."[60] Accordingly, traditional warrants are limited in scope.[61] In contrast, the immense amount of ESI that exists creates unique problems for SCA warrants. It is not clear what level of particularity is sufficient,[62] considering neither Rule 41 nor the SCA explicitly exempt SCA warrants from the particularity requirement. [63] For example, if the government wishes to obtain any emails pertaining to the alleged fraud Jack committed, must it delineate the specific dates of the emails, or can it request emails from a certain time period? Alternatively, can it request all emails ever sent from that account, even if such a request would disclose substantially more information than is sought by the warrant? Courts disagree. At least three different federal courts have required a high degree of particularity when describing electronic communications.[64] Other courts have taken a more general view of particularity.[65]

---

60. U.S. CONST. amend. IV.

61. *See* FED. R. CRIM. P. 41(e)(2)(A)–(B); *see also id.* advisory committee's note to 1990 amendment; United States v. Karo, 468 U.S. 705, 718 (1984) (noting that even though agents may not know exactly where an object will come to rest, the object to be searched can still be described with sufficient particularity).

62. *See* United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (describing the difficulties caused because of the "modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers").

63. *See* 18 U.S.C. § 2703; *see also* FED. R. CRIM. P. 41.

64. *See, e.g.*, *In re* Search of Info. Associated with [Redacted]@mac.com that Is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 145, 152 (D.D.C.) ("Here, the warrant describes only certain emails that are to be seized—and the government has only established probable cause for those emails. Yet it seeks to seize all emails by having them 'disclosed' by Apple."), *vacated*, 13 F. Supp. 3d 157 (D.D.C. 2014); *In re* Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, No. 13-MJ-8163-JPO, 2013 WL 4647554, at *8 (D. Kan. Aug. 27, 2013) ("The target accounts may contain large numbers of emails and files unrelated to the alleged crimes being investigated or for which the government has no probable cause to search and seize."); *see also In re* U.S.'s Application for a Search Warrant to Seize & Search Elec. Devices from Edward Cunnius, 770 F. Supp. 2d 1138, 1139 (W.D. Wash. 2011) (denying a search warrant of electronic devices based on the government's failure

These types of sweeping descriptions are not atypical of SCA warrants. For example, in 2013, Facebook was served with 381 warrants seeking twenty-four categories of information, including:

> any and all subscriber and account information and user contact information . . . account status history . . . historical login information, minifeed, status update history, shares, notes, wall and timeline postings to the target account . . . friend listing, including deleted and removed friends, networks, group listing, future and past events, all undeleted or saved photos . . . [and] any private messages.[66]

Requests like these provide more information about an individual than most realize.[67] Also, the very fact that such a warrant was signed by a judicial officer demonstrates that at least some judges and magistrates underestimate the true magnitude of data that exists online.[68] The requests in that case, *In re 381 Search Warrants*, were not limited to a specific time period; rather, the government requested a vast amount of ESI, beyond just the ESC, from the inception of the account until the date specified.[69] This may actually be a greater amount of information than would result from seizing an email account in its entirety. Sensitive information that would surely be beyond the scope of the warrant would have been swept up by the request—such as any of the metadata embedded into the uploaded or deleted pictures.[70]

The second significant difference is the notice requirement. Traditional warrants require some form of notice to the searched party that a place has been searched or property has been seized.[71] Rule 41 requires that a copy of the warrant and a receipt for any property seized be either delivered to the owner of the property or left where the property was seized, presumably for

---

to provide for review of the ESI by a "filter team" and forswear reliance on the plain view doctrine).

65. *See, e.g.*, *In re* Warrant for All Content & Other Info. Associated with xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 392 (S.D.N.Y. 2014).

66. Opening Brief of Appellant Facebook, Inc. at 10–11, *In re* 381 Search Warrants Directed to Facebook, Inc., 14 N.Y.S.3d 23 (App. Div. 2015) (No. 30178-14).

67. *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014). While the ESI obtained from Facebook may be less than that on a personal cell phone, such information can truly paint a picture of a person's life.

68. *See In re 381 Search Warrants*, 14 N.Y.S.3d 23. To be effective, judges of competent jurisdiction must review and sign a warrant, signifying that they reviewed the evidence and it met the probable-cause determination.

69. *See* Opening Brief of Appellant Facebook, Inc., *supra* note 66.

70. Pictures often have geo-tags embedded into the metadata that include the device it was taken from, where it was taken, and when it was taken. Chris Hoffman, *How to See Exactly Where a Photo Was Taken (and Keep Your Location Private)*, HOW-TO GEEK (May 17, 2017), https://www.howtogeek.com/211427/how-to-see-exactly-where-a-photo-was-taken-and-keep-your-location-private/ [https://perma.cc/ME85-ZW5R].

71. FED. R. CRIM. P. 41(f)(1)(C).

the owner to find.[72] Even so, traditional warrants allow for the element of surprise to minimize the chance of the destruction or tampering of evidence. Under the traditional doctrine, notice is always provided—even though it may be given after the fact.[73]

But SCA warrants do not abide by the same notice requirements. The SCA framework does not contain a notice requirement for information obtained in certain circumstances. For example, disclosure of ESC from a remote computing service is done "*without* required notice to the [user]."[74] Similarly, ESI disclosure requirements explicitly note that a "governmental entity receiving records or information . . . is not required to provide notice to [users]."[75] Without notice, the user will never know of the search or seizure unless a prosecutor ultimately files charges.[76] Coupled with the fact that the SCA also does not contain data retention requirements,[77] individuals may be subject to indefinite deprivations of data.[78]

The underlying concerns shaping the notice requirements for traditional warrants do not apply to ESI. As noted above, traditional warrants are structured to minimize the opportunity for the destruction of evidence.[79] Once a paper document is destroyed, it ceases to exist. But the same is not true for ESI.[80] When ESI is deleted, it is transferred to the unallocated slack space on a server.[81] And until that information is overwritten, it can still be accessed.[82] Additionally, there is a provision requiring both electronic communications

---

72. *Id.* Notwithstanding the SCA's explicit authorization of notice-less searches, one possible argument for notice is that ESI should be treated as a form of the user's property and that service providers are only bailees of that property. *See infra* text accompanying note 111. Accordingly, receipt to the service provider would not be sufficient because the service provider is not the owner of that property.

73. FED. R. CRIM. P. 41(f)(3); 18 U.S.C. § 3103a(b) (2012). Notice can sometimes be delayed if a court finds "reasonable cause," but only if the "warrant prohibits the seizure of any tangible property, [or] any wire or electronic communication." *Id.* This default rule requires that notice be provided within thirty days of the execution of the warrant. *Id.* § 3013a(b)(3).

74. 18 U.S.C. § 2703(b)(1)(A) (emphasis added).

75. *Id.* § 2703(c)(3).

76. *See* Nakashima, *supra* note 11.

77. *See* 18 U.S.C. §§ 2703–11.

78. Although the Department of Justice's new 2017 guidance implements a one-year limit, the guidance is not binding on the states. *See* Rosenstein, *supra* note 12. Further, because the rule was implemented through a guidance document—not baked into the statute itself—the policy could change from administration to administration. Many searches and seizures carried out under SCA warrants may never provide notice and can never be challenged as unconstitutional.

79. *See* FED. R. CIV. P. 41.

80. *See, e.g.*, Genger v. TR Inv'rs, LLC, 26 A.3d 180, 190 n.39 (Del. 2011) (explaining that even when ESI is deleted it can still exist as unallocated slack space).

81. *Id.*

82. *See id.*

services and remote computing services to retain ESI upon request from a governmental entity.[83]

The actor executing the warrant is the third significant difference. Traditional warrants authorize law enforcement agents to conduct the search themselves,[84] whereas SCA warrants require private third-party service providers to devote both time and resources to conducting the search on behalf of law enforcement.[85] This is significant because SCA warrants impose an increased burden on the responding third-party service provider.[86] This implicit burden also raises questions about how much effort the third-party service provider must put into the search.[87]

And finally, traditional warrants have different due process protections and methods of redress. With clear notice, the person being searched has an opportunity to be heard—through a motion to suppress evidence when charges are brought, or through a § 1983 claim against the officers conducting the search.[88] This incentivizes law enforcement officers to request warrants based on probable cause that describe the area being searched and the items being seized with particularity. The SCA affords no such opportunities for redress because to obtain redress, an individual requires notice of a potential violation. These differences underscore certain procedural due process concerns.

B. *The Standing Conundrum*

The absence of notice to the user highlights the restrictive nature of the Fourth Amendment's standing doctrine.[89] Standing for purposes of a Fourth Amendment challenge is much more limited than in other constitutional doctrines. In *Alderman v. United States*, the Supreme Court explained that Fourth Amendment rights are personal rights; they cannot be "vicariously

---

83. 18 U.S.C. § 2703(f) (2012).

84. *See In re* Application of the U.S. for an Order Authorizing the Installation of a Pen Register, 610 F.2d 1148, 1154 (3d Cir. 1979).

85. *See In re* 381 Search Warrants Directed to Facebook, Inc., 14 N.Y.S.3d 23, 28–29 (App. Div. 2015).

86. *In re* Application for Cell Tower Records Under 18 U.S.C. § 2703(d), 90 F. Supp. 3d 673, 677 (S.D. Tex. 2015) ("[The SCA's] reference to 'unusually voluminous' requests implies that a merely 'voluminous' request, perhaps encompassing multiple accounts, is within the contemplation of the law." (quoting 18 U.S.C. § 2703(d))).

87. For example, when running a search for specific emails, does a simple keyword search suffice or is a more exacting search required? *See* MICHAEL R. ARKFELD, THE LAW STUDENT'S GUIDE TO ELECTRONIC DISCOVERY AND EVIDENCE 5-30 to 5-49 (2016–2017 ed.).

88. *In re 381 Search Warrants*, 14 N.Y.S.3d at 27 ("The motion to suppress is the most important ex post protection available to citizens."); *see also* 42 U.S.C. § 1983 (2012). Whether a § 1983 claim is truly a "meaningful" opportunity to be heard remains to be seen. *See* William Baude, *Is Qualified Immunity Unlawful?*, 106 CALIF. L. REV. 45 (2018).

89. *E.g.*, Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 916 (W.D. Wash. 2017).

asserted."[90] Similarly, in *Rakas v. Illinois*, the Court made clear that only individuals who themselves suffered an unreasonable search could seek to exclude evidence under the Fourth Amendment.[91] In other words, the government must have unreasonably searched or seized the person asserting the Fourth Amendment claim, excluding those situations where the government obtains damaging evidence through an unreasonable search or seizure of a third party.[92] Even a possessory interest in the evidence being searched or seized might not be enough to confer standing.[93]

But in those cases, the third party was not the only other party that could reasonably assert the rights of the party that was unreasonably searched.[94] Some scholars question whether the lack of available avenues to challenge SCA warrants might be enough to confer Fourth Amendment standing.[95] But thus far, no service provider has been granted standing to object on behalf of its users.[96]

III. THE PROCEDURAL DUE PROCESS ARGUMENT

Because service providers cannot notify a targeted user about the existence of SCA warrants with nondisclosure orders, service providers have turned to the courts. These challenges have come in several forms and have

90. 394 U.S. 165, 174 (1969).

91. 439 U.S. 128, 143–49 (1978).

92. *See* United States v. Payner, 447 U.S. 727, 735 (1980) (rejecting the target theory of standing and "conclud[ing] that the supervisory power does not authorize a federal court to suppress otherwise admissible evidence on the ground that it was seized unlawfully from a third party not before the court").

93. *See* Rawlings v. Kentucky, 448 U.S. 98, 105–06 (1980) (finding that an individual's ownership of the drugs located in the searched purse of a third party was not sufficient to confer standing).

94. *Payner*, 447 U.S. at 730 (the individual whose briefcase was searched had standing); *Rawlings*, 448 U.S. at 104–06 (the owner of the purse may have had standing).

95. Daskal, *supra* note 11, at 456–59 (arguing for relaxed standing requirements by utilizing the third-party standing test outlined in *Powers v. Ohio*, 499 U.S. 400, 410–11 (1991)); Sarah E. Pugh, Comment, *Cloudy with a Chance of Abused Privacy Rights: Modifying Third-Party Fourth Amendment Standing Doctrine Post-*Spokeo, 66 AM. U. L. REV. 971 (2017).

96. *E.g.*, Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887, 912–15 (W.D. Wash. 2017) (denying a Fourth Amendment challenge on standing grounds); City & County of San Francisco v. HomeAway.com, Inc., 230 Cal. Rptr. 3d 901, 912–13 (Ct. App. 2018) (finding that a service provider has no standing to challenge an SCA subpoena on behalf of its users). There had been some success in challenging the territorial reach of SCA warrants, but recent legislation has made those arguments unavailable. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 222 (2d Cir. 2016) (dismissing the service provider's First Amendment claims but sustaining a challenge to the SCA's extraterritorial reach), *cert. granted sub nom.*, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (vacating and remanding with instructions to dismiss the case as moot because of the amended CLOUD Act, which gave the SCA extraterritorial reach).

been largely unsuccessful.[97] Instead of Fourth Amendment challenges, service providers should bring due process challenges on behalf of their users.[98] Then, perhaps a court will recognize third-party standing.

The Due Process Clause of the Fifth Amendment guarantees that "[n]o person shall . . . be deprived of life, liberty or property, without due process of law."[99] Under this doctrine, "[p]arties whose rights are to be affected are entitled to be heard; and in order that they may enjoy that right they must first be notified."[100] And as the Supreme Court has previously explained, "the Fourth Amendment [is not] the sole constitutional provision in question when the Government seizes property subject to forfeiture."[101] So although the Fourth Amendment limits the government's ability to search or seize property, it is not the only source of protection afforded to property owners.[102]

This Part argues that the use of SCA warrants violates the procedural due process rights of individual users. Essential to this argument is the tripartite balancing test set forth in *Mathews v. Eldridge*, which considers: (1) whether government action implicates a private interest, (2) whether there is a risk of erroneous deprivation of that interest and the probable value of additional or substitute procedural safeguards, and (3) whether there is a justifying government interest.[103] Absent notice to targeted users, service providers will have the best opportunity to challenge SCA warrants themselves and potentially even on behalf of their users.[104] Section III.A argues that the warrants implicate users' constitutional interests. Section III.B explores the risks of erroneous deprivation. Section III.C argues that there is no justifying government interest.

---

97. Some have been dismissed on standing grounds. *See supra* Section II.B. Others have unsuccessfully argued that 18 U.S.C. § 2703(d) authorizes service providers to quash SCA warrants that are "unusually voluminous in nature" or create an "undue burden." *See In re* 381 Search Warrants Directed to Facebook, Inc., 14 N.Y.S.3d 23, 29 n.4 (App. Div. 2015). But at least one court has limited this authority to objections to court orders, rather than warrants. *Id.* at 29.

98. Professor Orin Kerr previously wrote an article arguing that service providers may have a pre-enforcement procedural due process objection to SCA warrants based on the compliance costs rather than a Fourth Amendment objection asserting their users' rights. Orin Kerr, *New York Court of Appeals to Hear Argument in 'In re 381 Search Warrants' Case*, WASH. POST: VOLOKH CONSPIRACY (Feb. 6, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/06/new-york-court-of-appeals-to-hear-argument-in-in-re-381-search-warrants-case/ [https://perma.cc/JD4J-XCCP].

99. U.S. CONST. amend. V.

100. Fuentes v. Shevin, 407 U.S. 67, 80 (1972) (quoting Baldwin v. Hale, 68 U.S. (1 Wall.) 223, 233 (1863).

101. United States v. James Daniel Good Real Prop., 510 U.S. 43, 49 (1993).

102. *Id.* at 52.

103. *See* Mathews v. Eldridge, 424 U.S. 319, 334–35 (1976).

104. *See infra* Part IV.

A. *Constitutional Interests*

Users that are the subject of criminal charges after authorities execute an SCA warrant receive due process: these users eventually obtain notice of the deprivation and have a meaningful opportunity to be heard. Users with notice can move to suppress the evidence gleaned from a warrant that violates the Fourth Amendment or bring a § 1983 claim.[105] The notice problem becomes an issue when charges are never brought against a targeted user. If charges are never brought, the user may never know that a search was conducted that may have violated whatever property interest the user has in their ESI.[106]

This implicates a quasi-property interest.[107] Although a full-fledged property interest in one's own data has not been formally recognized, this Note argues that a quasi-property interest exists in ESI. There has been some scholarly discussion about the merits and drawbacks of treating data as personal property,[108] but there also is a strong argument that individuals have at least a quasi-property interest in their ESI. Property is a general term for a bundle of rights typically associated with physical things, like homes, cars, phones, or even more ephemeral things like intellectual property.[109] This

---

105. Section 1983 claims are notoriously difficult to win. *See* Baude, *supra* note 88, at 48.

106. *See In re* Application of Jason Leopold to Unseal Certain Elec. Surveillance Applications & Orders, 300 F. Supp. 3d 61, 86 (D.D.C. 2018) ("Although the SCA contains no similar default sealing or nondisclosure provisions, the SCA authorizes the government to seek such nondisclosure and, in practice, the government has 'always been able to restrict access' to SCA warrants and § 2703(d) orders 'by requesting a sealing order, regardless of the statutory default,' and to delay or preclude a notification to a subscriber or customer of an SCA warrant or § 2703(d) order's existence." (quoting *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 291 n.9 (4th Cir. 2013) (citations omitted))).

107. There may also be an argument that a liberty interest is implicated: the interest in being free from unreasonable searches and seizures. Although several courts have recognized this specific liberty interest in the Fourth Amendment context, *see, e.g.*, Washington v. Lambert, 98 F.3d 1181, 1187 (9th Cir. 1996), some courts have carried the interest over into the procedural due process context, *see, e.g.*, Tenenbaum v. Williams, 193 F.3d 581, 605 (2d Cir. 1999); *see also* Schweitzer v. Crofton, 560 F. App'x 6, 10–11 (2d Cir. 2014) (recognizing a due process interest to be free from unreasonable searches and seizures but concluding that the interest was not violated). *But see* Bostrom v. N.J. Div. of Youth & Family Servs., 969 F. Supp. 2d 393, 415 (D.N.J. 2013) ("If the court were to find [a deprivation of such a liberty interest in the procedural due process context,] then all unreasonable searches would constitute procedural due process claims.").

108. Although some scholars argue against treating data as property, *see, e.g.*, Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1295–301 (2000), others assert quasi-property rights as a potential step to protect an individual's property rights, Gianclaudio Malgieri, *"Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?*, J. INTERNET L., Nov. 2016, at 3, 8–10.

109. *See* J.E. Penner, *The "Bundle of Rights" Picture of Property*, 43 UCLA L. REV. 711, 712 (1996). Although there are other property theories beyond the "bundle-of-rights," the bundle of rights metaphor is descriptively useful to describe the complex relationship that may arise from data bailment. *See* Jane B. Baron, *Rescuing the Bundle-of-Rights Metaphor in Property Law*, 82 U. CIN. L. REV. 57, 58–59 (2013).

"bundle of rights" is abstract: it is often described as including the right to use property, exclude others from that property, and sell that property.[110] If ESI is a user's property, the user retains an interest in it and is able to control its alienability.[111] This argument has intuitive appeal: just because another party has access or possession over the user's property does not necessarily mean that the user no longer owns that property.[112] As Justice Gorsuch noted in his dissent in *United States v. Carpenter*, data can be thought of as an individual's "papers and effects."[113] If handing a physical private document to a third party would not eliminate your property interest, neither should entrusting your data to a third party.[114]

But the argument for a full-fledged property right is not broadly accepted and could affect how companies commodify user data.[115] Some may argue that ESI should not be treated like property because the user is "giving up" their information by engaging in online conduct, effectively waiving any downstream rights over how the information is subsequently used.[116] And technically the third party is making carbon copies of, not seizing, the ESI. Also, granting users the unfettered ability to exclude or alienate their own information after giving it up may have problematic consequences.[117] Treating ESI under the quasi-property framework instead might better "allow for equitable relief to become readily available for infraction of the entitlement."[118]

The term "quasi-property" refers to the "relational entitlement mechanism to simulate property's exclusionary framework within limited settings," and is commonly associated with the Supreme Court's decision in *International News Service v. Associated Press*.[119] In that case, the Associated Press ("AP") sued the International News Service for copying the substance of the

110. Penner, *supra* note 109, at 717–18; *see also* Int'l News Serv. v. Associated Press, 248 U.S. 215, 250 (1918) (Brandeis, J., dissenting).

111. *Cf.* Penner, *supra* note 109, at 742 ("Thus there are two sides to the coin of property—one inward-looking, the protection of the owner in his use of his own, and one outward-looking, his power to alienate his property to others . . . ."). When another party has control over your personal property, it is called a bailment. It is the "delivery of personal property by one person (the *bailor*) to another (the *bailee*) who holds the property for a certain purpose." *Bailment*, BLACK'S LAW DICTIONARY (10th ed. 2014).

112. *See* Carpenter v. United States, 138 S. Ct. 2206, 2268–69 (2018) (Gorsuch, J., dissenting).

113. *Id.*

114. *Id.*; *see also* 8 C.J.S. *Bailments* § 36 (2017).

115. *See* Litman, *supra* note 108.

116. *Id.* at 1300–01.

117. *Id.* (explaining that allowing bargaining for downstream use and alienability would decrease consumer privacy).

118. Shyamkrishna Balganesh, *Quasi-Property: Like, but Not Quite Property*, 160 U. PA. L. REV. 1889, 1913 (2012).

119. *Id.* at 1891–92.

AP's news stories, rewriting them, and selling them.[120] The Supreme Court found that a quasi-property interest existed.[121] Even though there was no full right to alienability as with traditional property rights, the AP still had a limited right to exclude their competitors from the substance of their articles for a limited amount of time.[122] In essence, quasi-property means that an object is property for some circumstances, but not for others. There may be a limited right to exclude or alienate.[123] Quasi-property interests have been recognized in several other contexts: biomedicine and sepulchre;[124] trade secret;[125] reputation for purpose of trademark dilution claims.[126]

There is a strong argument for a quasi-property interest in ESI. Just as handing a physical document to a third party does not eliminate the property interest therein,[127] neither should handing data to a third party. Even though users do not have comprehensive control over their data, the privacy statutes of several states, along with the General Data Protection Regulation ("GDPR") in the European Union, have begun to grant users rights to ESI that look more and more like controls on alienability and the right to exclude.[128] Some may argue there is never a "deprivation" because ESI is only copied and never removed. But there is a deprivation of the quasi-property right, in that the user is no longer able to exert the same level of control over their personal information. Recognition of these rights would expand the remedies available to users while still avoiding the expressive commodification associated with a full-fledged property right.[129] If users have a quasi-property right in their ESI, then the due process argument will be viable.

---

120. Int'l News Serv. v. Associated Press, 248 U.S. 215, 231 (1918).

121. *Id.* at 236.

122. *Id.* at 245–46.

123. Balganesh, *supra* note 118, at 1893.

124. *E.g.*, Newman v. Sathyavaglswaran, 287 F.3d 786, 796–97 (9th Cir. 2002) (holding that plaintiffs "had property interests in the corneas of their deceased children protected by the Due Process Clause of the Fourteenth Amendment"). *But see* Florida v. Powell, 497 So. 2d 1188, 1193 (Fla. 1986) (holding that there was "no protectable liberty or property interest in the remains of their decedents"); Ga. Lions Eye Bank, Inc. v. Lavant, 335 S.E.2d 127, 128 (Ga. 1985) ("[I]n Georgia, there is no *constitutionally* protected right in a decedent's body.").

125. Lauren Henry Scholz, *Privacy as Quasi-Property*, 101 IOWA L. REV. 1113, 1131 (2016).

126. Balganesh, *supra* note 118, at 1897–98 (citing Kathleen B. McCabe, Note, *Dilution-by-Blurring: A Theory Caught in the Shadow of Trademark Infringement*, 68 FORDHAM L. REV. 1827, 1835 (2000)).

127. *See supra* note 114 and accompanying text.

128. *See* Malgieri, *supra* note 108, at 9–10 (arguing that the GDPR is a form of quasi-property based on relational, relative forbearance); *see also* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.120 (2018) (giving consumers the right to have some downstream control of their data); *id.* § 1798.105 (giving consumers the right to request data deletion from businesses that collect personal information).

129. *See* Balganesh, *supra* note 118, at 1914; *see also* Litman, *supra* note 108.

B. *Risk of Erroneous Deprivation*

The second *Mathews* factor weighs the risk that the administrative procedure will work an erroneous deprivation of the private interest, as well as the probable value of any added procedural safeguards to reduce the risk.[130] This factor focuses on the "fairness and reliability" of the existing procedures governing the deprivation.[131] The risk of an erroneous deprivation stems from the lack of a notice and hearing requirement—eliminating a crucial check on government.

In the civil forfeiture context, the Supreme Court has explained that "[t]he practice of *ex parte* seizure . . . creates an unacceptable risk of error."[132] The same is true in the SCA context. There is a significant risk of erroneous deprivation of users' liberty and quasi-property interests when the government executes an overly broad SCA warrant. If the underlying SCA warrant is invalid or overbroad, it should not have issued, and any seizure of ESI is erroneous.[133] Further, without any meaningful check, the government's tendency toward dragnet surveillance goes unfettered.[134] If users and third parties are unable to challenge a potentially overbroad search, users will not have redress[135] and will not be able to serve as a crucial check on government overreach. Without such deterrence, the government will be emboldened to issue overly broad, general SCA warrants as in *In re 381 Search Warrants*.[136] This lack of deterrence and the inability to check the government's probable cause determination, coupled with the lack of a meaningful or a timely opportunity to be heard, creates a significant risk of erroneous deprivation.

Without a data-deletion requirement,[137] users are potentially subjected to an unlimited deprivation of the quasi-property interests in their data. Further, because service providers are generally precluded from informing their users of the search and do not have standing to assert users' Fourth Amendment rights,[138] any erroneous deprivations that occur will be effec-

130. Mathews v. Eldridge, 424 U.S. 319, 335 (1976).

131. *Id.* at 343–44.

132. United States v. James Daniel Good Real Prop., 510 U.S. 43, 55 (1993).

133. *See* United States v. Galpin, 720 F.3d 436, 439 (2d Cir. 2013) ("[T]he warrant was facially overbroad and thus violated the Fourth Amendment . . . .").

134. *Cf.* Goss v. Lopez, 419 U.S. 565, 580–81, 580 n.9 (1975) (citing Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 170–72 (1951) (Frankfurter, J., concurring) ("[F]airness can rarely be obtained by secret, one-sided determination of facts decisive of rights. . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it.")).

135. *Cf.* Hector v. Watt, 235 F.3d 154, 157 (3d Cir. 2001) ("Victims of unreasonable searches or seizures may recover damages directly related to the invasion of their privacy—including (where appropriate) damages for physical injury, property damage, injury to reputation, etc. . . . ." (quoting Townes v. City of New York, 176 F.3d 138, 148 (2d Cir. 1999))).

136. *See supra* note 66 and accompanying text.

137. *See* 18 U.S.C. §§ 2701–11 (2012).

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

tively immunized from challenge or review. This factor should weigh in favor of either providing notice or some other method to check the scope and validity of a warrant.

C. *Addressing Government Interests*

The government may have several important interests at issue. The government has an interest in the speedy execution of its warrant to prevent data or evidence destruction, and in investigating and solving crimes quickly. So, the argument goes, extremely delayed or nonexistent notice is needed to prevent criminals from rushing to delete their ESI and abscond.[139]

Though these interests are surely legitimate to some extent, they are not impacted by a notice requirement. Underlying the government's concern is the fear that because data is more ephemeral, it can be easily and quickly deleted and the government can lose vital evidence.[140] Under the current SCA framework, the government can issue a preservation order, which requires that service providers copy and retain the targeted user's data in their possession for up to ninety days while a warrant is pending. [141] This preservation obligation adequately addresses the government's concern. If the data is copied and preserved, the government will obtain at least as much ESI as was on the third-party servers at the time a magistrate approved the warrant. This provides no opportunity for the user to delete their ESI before the warrant is executed.

Indeed, the existing preservation requirements provide the government with security it does not have when dealing with physical property.[142] Assume that, once again, Jack will be the target of a search. Once the government wishes to start the clock, it can issue a preservation order to Facebook.[143] Facebook must then "take all necessary steps" to preserve all the evidence in its possession without notifying Jack.[144] This presumably covers any additional ESI that Jack creates during that time. On day eighty-nine, the government can serve Facebook with the SCA warrant.[145] This system essentially allows the target to be under supervision for three months while a court order is pending. Accordingly, preservation orders adequately address the government's fear of deletion. The procedural safeguard this Note advo-

---

139. *E.g.*, *id.*

140. *See In re* Search Warrant for [Redacted].com, 248 F. Supp. 3d 970, 982 (C.D. Cal. 2017) (recognizing that the government has an interest in protecting its investigation).

141. 18 U.S.C. § 2703(f) ("A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.").

142. *See id.*

143. *See id.*

144. *See id.*

145. *See id.* It is important to note that the warrant may only cover a subset of the information preserved. In that circumstance, the scope of the warrant will be complied with.

cates for is guaranteed notice after the fact. Providing such notice would not significantly affect the government interest; it would do nothing more than allow individuals an opportunity to be heard if the search is overbroad or unreasonable.

If there were some ongoing or repeated investigation into a target, meaning that an SCA warrant was issued periodically to gather additional evidence without a charge being brought, perhaps guaranteed notice would then implicate the government interest. There is no denying that after-the-fact notice would signal to the targeted user that they are being searched. That said, an ongoing search of that sort is not permitted with respect to the physical world, even when there are significant government interests at play.[146]

The government interests are outweighed by the individual interests and high risk of erroneous deprivation. Therefore, a guaranteed notice requirement would not significantly affect the government interests. Based on this analysis, SCA warrants with nondisclosure provisions seem to run afoul of the requisite amount of process due under the Constitution.

IV. THIRD-PARTY STANDING UNDER A DUE PROCESS THEORY

The lack of notice for some searches carried out pursuant to SCA warrants violates the procedural due process rights of individual users. In at least some non-negligible set of cases, no one will be able to challenge the validity or scope of an SCA warrant, potentially for some extended period of time.[147] A statutory solution to this conundrum would be best.[148] But because the legislature can often move slowly, and in recent times somewhat unpredictably, this Note argues that by challenging SCA warrants under a procedural due process theory, as opposed to a Fourth Amendment theory, an opening arises for third-party standing.

Addressing the interests of users in this context is difficult because service providers do not have standing to bring a Fourth Amendment challenge to defective SCA warrants on behalf of their users.[149] Fourth Amendment standing is much more difficult to establish than standing to assert other constitutional rights.[150] Accordingly, arguing that there is also a procedural

146. *See supra* notes 18–19 and accompanying text. Outside of the SCA, notice can generally be delayed if a court finds reasonable cause that immediate notice would have an adverse result; and even then it can only be delayed for a reasonable period not to exceed thirty days in most circumstances. FED. R. CRIM. P. 41(f)(3); 18 U.S.C. § 3103a(b). Upon a showing of good cause and an "updated showing of the need for further delay," the court can extend the delayed notice for additional periods of up to ninety days. 18 U.S.C. § 3103a(c).

147. *See supra* note 12 and accompanying text; Daskal, *supra* note 11, at 440.

148. For a statutory proposal that focuses on this issue, see Daskal, *supra* note 11, at 459–60. For a broader proposal, see Kerr, *A User's Guide*, *supra* note 6, at 1233–42.

149. *E.g.*, *In re* 381 Search Warrants Directed to Facebook, Inc., 14 N.Y.S.3d 23, 25 (App. Div. 2015); *see also* Section II.B.

150. *See* Section II.B. For an argument that third-party standing should exist in the SCA context, see Daskal, *supra* note 11.

due process issue based on implication of a quasi-property right creates a stronger standing argument.

To argue for third-party standing under a due process theory, service providers can rely on a line of Supreme Court cases that relax the standing rules for claims that could not otherwise be brought. This concept was first signaled in *NAACP v. Alabama*, where the Court created organizational standing.[151] There, although the Court acknowledged that constitutional rights are personal, it still permitted the NAACP to bring a due process claim on behalf of its members because the members' rights could not otherwise be vindicated.[152] A third-party standing theory similarly focused on making process available was advanced in *Barrows v. Jackson*, an equal protection case. The Supreme Court relaxed the standing rules because it would be "difficult if not impossible for the persons whose rights are asserted to present their grievance before any court."[153] White neighbors sued Jackson to try to indirectly enforce a racially restrictive covenant; Jackson had sold a home to black buyers in violation of the constitutionally infirm covenant.[154] The Court ultimately held that Jackson had standing to raise an equal protection claim on behalf of the buyers, who were not parties to the contract and who were not in court.[155] Similarly, in *Eisenstadt v. Baird*, a third-party activist was granted standing on behalf of individuals who were procedurally unable to bring their own claims.[156] A Massachusetts law outlawed distribution of contraceptives, except by physicians or pharmacists, and then only to married individuals.[157] Baird intentionally violated the law and was prosecuted.[158] He was ultimately allowed to raise an objection on behalf of third parties not before the court because "unmarried persons denied access to contraceptives . . . [were] not themselves subject to prosecution and, to that extent, [were] denied a forum in which to assert their own rights."[159] Just like in *Barrows*, the Court permitted third-party standing because the affected individuals had no other opportunity to have their claims heard.

---

151. 357 U.S. 449, 459 (1958) ("[T]his Court has generally insisted that parties rely only on constitutional rights which are personal to themselves . . . . The principle is not disrespected where constitutional rights of persons who are not immediately before the Court could not be effectively vindicated except through an appropriate representative before the Court.").

152. *NAACP*, 357 U.S. at 459.

153. Barrows v. Jackson, 346 U.S. 249, 257 (1953).

154. *Id.* at 251–52.

155. *Id.* at 255–57 ("Ordinarily, one may not claim standing in this Court to vindicate the constitutional rights of some third party. . . . But in the instant case, we are faced with a unique situation in which it is the action of the state *court* which might result in a denial of constitutional rights and in which it would be difficult if not impossible for the persons whose rights are asserted to present their grievance before any court.").

156. 405 U.S. 438, 443–46 (1972).

157. *Eisenstadt*, 405 U.S. at 440–41.

158. *Id.* at 440.

159. *Id.* at 446.

Under this line of cases, when individuals are in the precarious position of being unable to challenge a government practice that implicates their personal rights, third-party standing may arise. It may be the best—or the only—method to safeguard and vindicate the individuals' constitutional rights. In the context of SCA warrant challenges, service providers will need to rely on *Powers v. Ohio*, the seminal third-party standing case.[160] To assert third-party standing, three criteria must be met: (1) "[t]he litigant must have suffered an 'injury in fact,' " so that the litigant has a " 'sufficiently concrete interest' in the outcome of the issue"; (2) "the litigant must have a close relation to [the user]"; and (3) "there must exist some hindrance to the [user's] ability to protect his or her own interests."[161]

In most circumstances with SCA warrants, service providers will have suffered sufficient injury in fact and will have a sufficient interest in the outcome. To comply with SCA warrants, the service provider must search, cull, and produce data responsive to the warrants' requirements.[162] When service providers must expend resources on compliance, they forego the free use of their equipment and the efficient allocation of their employees' time. This may be sufficient to meet the first prong for third-party standing, and the argument has some support at least one circuit. The Third Circuit found that a warrant requiring a telephone company to provide technical assistance sufficiently implicated the company's property interest to justify a limited pre-enforcement hearing.[163] If such a minimal use of time and resources is sufficient to justify a hearing in that circumstance, courts should generally find it sufficient to meet the first prong.

Next, service providers also have a sufficiently close relationship with their users. The close relation prong looks at whether "the relationship between the [service provider] and the [user] may be such that the former is fully, or very nearly, as effective a proponent of the right as the latter."[164] The nature of the relationship between service providers and users is special, and it creates several incentives that align the interests of both parties. Service providers are in control of the user's ESI and have more resources than the individual user, giving them the ability to effectively advocate for the user's rights. Service providers also hold an astronomical amount of private data in their online repositories.[165] Social media sites boast billions of active daily

160. 499 U.S. 400, 410–411 (1991).

161. *Powers*, 499 U.S. at 410–11 (quoting Singleton v. Wulff, 428 U.S. 106, 112–16 (1976)).

162. *See* 18 U.S.C. § 2703(a), (c), (g) (2012).

163. *In re* Application of the U.S. for an Order Authorizing the Installation of a Pen Register, 610 F.2d 1148, 1157 (3d Cir. 1979).

164. *See* Singleton v. Wulff, 428 U.S. 106, 115 (1976).

165. *See* Daskal, *supra* note 18, at 377 ("Nowadays, however, it is no longer feasible to participate in a digital world without exposing an incredible wealth of private information—including one's associations and private thoughts—to a third party.").

users.[166] Online repositories contain conversations between individuals and their families, their partners, their closest confidants, their attorneys, and their coworkers. This puts service providers into a position of power with respect to their users. But service providers have economic incentives to protect the privacy interests of their users in order to avoid lost business, lost profits, and reputational harm.[167] These incentives align the interests of service providers and their users. So, if a service provider is able to challenge an SCA warrant, it will likely do so with the same goals in mind. Service providers are also the most logical party to bring these challenges: they are often well represented and they can challenge multiple warrants at one time. Permitting such challenges would be the most economical approach.

Finally, as argued above, there is a significant hindrance to users asserting their own rights. Without notice, a user cannot protect their own constitutional interests. As Professor Daskal explains, the recent policy change instituted by the Department of Justice only discusses nondisclosure orders of up to one year, but "during that year, the government may collect, and perhaps disseminate, a significant amount of information about a target."[168] Plus, the year-long delay can be renewed and extended.[169] During that time, the user's ability to assert their rights is hindered.

As this exercise demonstrates, service providers have a strong claim for third-party standing under the *Powers* test. Allowing timely challenges has a number of policy benefits. Courts can finally provide a needed check on government overreach in an administrable way. Permitting these challenges would rein in current SCA warrant practices to look more like those of traditional warrants and increase government transparency. Service providers would also benefit. They could chip away at the prevalence of overly broad SCA warrants. This, presumably, would save the money and resources that would otherwise go toward execution of such warrants. For users, the benefits are obvious: their constitutional interests could be vindicated. To reap these benefits, service providers should change the types of challenges they bring from Fourth Amendment challenges to Fifth Amendment challenges.

166. Facebook reports 1.49 billion daily active users on average for September 2018. *Company Info*, FACEBOOK: NEWSROOM, https://newsroom.fb.com/company-info/ [https://perma.cc/FQ5X-BKX5].

167. *See* Pat Conroy et al., *Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry*, DELOITTE INSIGHTS (Nov. 13, 2014), https://dupress.deloitte.com/dup-us-en/topics/risk-management/consumer-data-privacy-strategies.html [https://perma.cc/LXB4-FD3W]; David Hoffman, *Privacy Is a Business Opportunity*, HARV. BUS. REV. (Apr. 18, 2014), https://hbr.org/2014/04/privacy-is-a-business-opportunity [https://perma.cc/2MSR-JBAX].

168. Daskal, *supra* note 11, at 457.

169. *Id.*; *see also* Rosenstein, *supra* note 12.

CONCLUSION

The government's ability to obtain ESI without providing notice to users implicates users' right to procedural due process. It deprives them of a quasi-property interest without the opportunity to be heard at a meaningful time. And because the Stored Communications Act does not include a data-deletion provision, it may result in an indefinite deprivation of those rights.

Absent a statutory fix to this problem, allowing third-party service providers to vindicate the rights of their users makes sense. The concept of privacy rights is changing with the increase in digitized communications. Individuals are increasingly using third-party service providers to store, protect, or communicate their most private information. And in response, law enforcement is increasingly using data collected from third-party service providers, except without meaningful notice to the targeted users. The SCA's secret searches have created an impossible problem for its targets. But framing the issue under procedural due process may allow third parties to assert the rights of their users. It would serve as an essential check on government overreach. Without such a check, there is little incentive for government agencies to tailor the scope of their SCA warrants. Instead, SCA warrants will continue to be excessive and invasive.