Preservation Requests and the Fourth Amendment

*Armin Tadayon**

CONTENTS

* Adjunct Professor at George Mason University, Volgenau School of Engineering, J.D., George Mason University School of Law, 2013. I would like to thank Chris Madsen for his guidance and invaluable feedback on the earlier drafts of this article. I'd like to thank Devron Brown and Amanda Irwin for their help in developing this article. I am also grateful for the advice and assistance of the editors of the *Seattle University Law Review*.

INTRODUCTION

Every day, Facebook, Twitter, Google, Amazon, ridesharing companies, and numerous other service providers copy users' account information upon receiving a preservation request from the government. These requests are authorized under a relatively obscure subsection of the Stored Communications Act (SCA). The SCA is the federal statute that governs the disclosure of communications stored by third party service providers. Section 2703(f) of this statute authorizes the use of "f" or "preservation" letters, which enable the government to request that a service provider "take all necessary steps to preserve records and other evidence in its possession" while investigators seek valid legal process.[1]

Section 2703(f) is clearly a valuable tool for law enforcement, and one that investigators are loath to give up. According to the government, it permits investigators to prevent the destruction of evidence in a minimally intrusive way while seeking legal process.[2] It is also a useful means to obtain evidence because relying on § 2703(f) does not violate the Fourth Amendment as it does not involve government action. Even if the use of "f" letters does implicate the Fourth Amendment, the preservation

1. 18 U.S.C. § 2703(f)(1).

2. *See* OFFICE OF LEGAL EDUC. EXEC. OFFICE FOR U.S. ATT'YS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 27 (Nathan Judish et al. eds., 3d ed. 2009) [hereinafter DOJ Manual].

of account information is reasonable because users have consented to the preservation of their records through their acceptance of the service provider's Terms of Service.

Despite its legality, § 2703(f) is harmful to user privacy. Privacy advocates argue that the provision is outdated, it is relied upon excessively by investigators, and it circumvents privacy protections by avoiding judicial oversight. The provision is textually inconsistent. Critics of § 2703(f) argue that it violates the Fourth Amendment because it lacks traditional safeguards and because the preservation of account information is an unreasonable seizure.

This Article aims to impartially present and evaluate both the benefits and harms of using "f" letters as a law enforcement tool. Part I provides the background of the SCA and places the statute in historical context. Part II surveys various service providers' Terms of Service and Privacy Policies and provides statistics regarding the use of preservation letters. Part III analyzes both the benefits and harms resulting from the government's use of "f" letters. Finally, Part IV suggests a remedy that enables investigators to continue using "f" letters when appropriate while also limiting the privacy harms that can occur under the existing process.

I. THE STORED COMMUNICATIONS ACT

A. Erections, Warshak*, and the Stored Communications Act*

United States v. Warshak[3] was the first case to pose a constitutional challenge to the Stored Communications Act, and it illustrates the conflicting interests of law enforcement and individual privacy.[4] The statutory privacy law regulates the voluntary and compelled disclosures of stored content and non-content information held by third party service providers.[5] In this case the government was investigating Steven Warshak's company, Berkeley, for fraud. Berkeley's principal product was Enzyte, a pill purported to increase the size of a man's penis.[6]

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

4. Susan Freiwald & Patricia L. Bellia, *The Fourth Amendment Status of Stored E-Mail: The Law Professors' Brief in* Warshak v. United States, 41 U.S.F. L. REV. 559, 560 (2007). As Freiwald and Bellia show in their insightful article, *United States v. Warshak* was a particularly important decision in the development of electronic surveillance law because it involved a balancing of interests between a user's right to privacy in his stored electronic communications and the government's interest in gaining access to such information in order to pursue and prosecute a potential criminal. Through its decision, the Sixth Circuit addressed not only the procedural hurdles that law enforcement agents must overcome in order to obtain access to a user's electronic information under the Stored Communications Act (SCA) but also whether the SCA's requirements satisfy the Fourth Amendment.

5. Codified at 18 U.S.C. §§ 2701–11.

6. *Warshak*, 631 F.3d at 276.

Berkeley advertised aggressively through suggestive commercials featuring "Smilin' Bob" and "a very happy missis at home."[7] The advertisement campaign, which claimed that individuals who took the pill "experienced a 12 to 31% increase in the size of their penises," cited an independent customer study later confirmed to be fake.[8] In addition, the company falsified other statistics, enrolled customers in an auto-ship program without their consent, and artificially inflated the number of its sales transactions to maintain lines of credit from merchant banks.[9] These questionable corporate practices eventually caught the attention of government regulators and investigators.

Because Berkeley personnel relied on e-mail for communication, in October 2004 the government requested Warshak's Internet Service Provider (ISP) to preserve the contents of Warshak's e-mails, as well as all future messages.[10] The service provider began preserving copies of Warshak's incoming and outgoing e-mails, and per the government's instructions, Warshak was not informed that his communications were being preserved.[11] In January 2005, the government obtained a subpoena pursuant to § 2703(b) and compelled Warshak's ISP to disclose all the e-mails it had preserved since receiving the preservation request.[12] The government served Warshak's ISP with an ex parte § 2703(d) order in May 2005 and mandated that the ISP turn over additional e-mails in Warshak's account.[13] In total, the government obtained the contents of approximately 27,000 e-mails from Warshak's account.[14] Warshak eventually received notice of the subpoena and §2703(d) order in May 2006.[15]

Seeking to exclude the e-mails the government obtained from his ISP, Warshak argued that the government had violated § 2703(f) by engaging in the prospective preservation of his e-mails and that the evidence should be suppressed.[16] The Sixth Circuit held that Warshak had a reasonable expectation of privacy in his e-mails and that the government violated his Fourth Amendment rights by compelling his ISP to disclose his e-mails without first obtaining a warrant based on probable cause.[17]

---

7. *Id.* at 277; *see also* Associated Press, *Company Touts Pills for Middle-Age Ailments*, NBC NEWS (Nov. 22, 2004), http://www.nbcnews.com/id/6513891#.XfAsDZNKjq0 [https://perma.cc/T8WR-2UT4].

8. *Warshak*, 631 F.3d at 277.

9. *Id.* at 271–81.

10. *Id.* at 283.

11. *Id.*

12. *Id.*

13. *Id.*

14. *Id.*

15. *Id.*

16. *Id.* at 335.

17. *Id.* at 288.

Yet, the court sidestepped addressing the issue surrounding "f" letters by holding that the e-mails should not be excluded from evidence due to the government's good faith reliance on the SCA.[18] This decision has rightly been recognized for extending Fourth Amendment protections to e-mails, as well as for its implications for online privacy. To date, however, Electronic Communications Privacy Act (ECPA) scholars have largely ignored the concurring opinion's discussion of § 2703(f), the statutory provision that the government used to preserve Warshak's e-mails in the first place. The concurrence was the first to recognize and discuss the privacy issues that could arise from improper use of § 2703(f).

In his concurring opinion, Judge Keith expressed his apprehension regarding the government's use of § 2703(f) to "preserve Warshak's stored and future e-mail communications without Warshak's knowledge and without a warrant."[19] According to Judge Keith, "The plain language of § 2703(f) permits only the preservation of e-mails in the service provider's possession at the time of the request, not the preservation of future e-mails."[20] Further, if the service provider had not been compelled by the preservation request to maintain all existing and prospective e-mails, and had followed its existing policy, it would have destroyed Warshak's old e-mails in the ordinary course of business.[21] But because the government relied on § 2703(f) to compel that the service provider preserve all of Warshak's e-mails, "the government used the statute as a means to monitor Warshak after the investigation started without his knowledge and without a warrant."[22] Such conduct was troubling because it was akin to "back-door wiretapping."[23] Judge Keith's chief concern was the government's demand of prospective preservation and disclosure of e-mails under § 2703(f). And though the majority's decision prohibited the government from using "f" letters to order service providers to preserve records not yet created, it did not adequately analyze the constitutionality of § 2703(f).

The following section provides the historical background of the SCA. It also discusses 18 U.S.C. § 2703 and specifically focuses on the language of subsection (f).

18. *Id.* at 292.
19. *Id*. at 334 (Keith, J., concurring).
20. *Id.*
21. *Id.*
22. *Id.*
23. *Id.*

B. Historical Context and Background

The Fourth Amendment of the U.S. Constitution establishes "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[24] While the "meaning of the Fourth Amendment is relatively well-established for investigations involving physical evidence," the same cannot be said of searches and seizures involving digital evidence.[25] Congress enacted the SCA in 1986, as part of the ECPA, after recognizing that the Fourth Amendment does not provide adequate protection to digital communications.[26] The SCA's purpose was to fill in some of the gaps created by technological developments and Fourth Amendment jurisprudence that had combined, in the preceding two decades, to throw the then-existing state of privacy protections into a flux.[27]

1. Searches and Seizures of Communications Prior to the Stored Communications Act

The Fourth Amendment protects against unreasonable searches and seizures.[28] A "search" under the Fourth Amendment occurs in two situations: (1) a physical trespass, by the government, on to "persons, houses, papers, and effects;" or (2) action by the government that violates an individual's reasonable expectation of privacy.[29] A "seizure" involves "some meaningful interference with an individual's possessory interest in [her] property."[30]

To determine whether a search or seizure is reasonable, courts look to a two-prong test articulated by Justice Harlan's concurring opinion in the United States Supreme Court case, *Katz v. United States*.[31] The *Katz* test asks (1) whether an individual has exhibited an actual (subjective) expectation of privacy, and (2) whether society is willing to recognize that subjective expectation as reasonable.[32] If an individual has an actual expectation of privacy that society is willing to recognize as reasonable, and the government has violated this expectation through its conduct or

24. U.S. CONST. amend. IV.

25. ORIN S. KERR, COMPUTER CRIME LAW 389 (4th ed. 2018).

26. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848; *see* KERR, COMPUTER CRIME LAW, *supra* note 25, at 623.

27. *See generally* 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, 1209–13 (2004).

28. U.S. CONST. amend. IV.

29. KERR, COMPUTER CRIME LAW, *supra* note 25, at 401.

30. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

31. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

32. *Id.*

due to its failure to obtain a warrant, then the government has likely violated the individual's Fourth Amendment rights.[33]

The Supreme Court has clarified that the Fourth Amendment protects possessory and liberty interests even when privacy rights are not implicated.[34] This Article limits its analysis to seizures that impact a user's privacy and possessory interests. It will not discuss whether preservation requests involve "searches" within the meaning of the Fourth Amendment.

A seizure is constitutionally valid if it is accompanied by a warrant issued upon probable cause "supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."[35] Although the *Katz* test remains the standard by which we analyze the reasonableness of Fourth Amendment seizures, the Supreme Court's holdings in *United States v. Miller*[36] and *Smith v. Maryland*[37] created the third-party doctrine that curtailed some of the protections created by *Katz*.

In *Miller*, the government subpoenaed Mitch Miller's bank records to use as evidence to prove he was engaged in criminal activity.[38] Miller's banks complied with the subpoena without notifying him.[39] The government charged Miller based on the information it obtained from the banks, and Miller sought to suppress the evidence, arguing the records were obtained illegally and that his Fourth Amendment rights were violated.[40] The Court held that a depositor does not have any expectation of privacy in his banking records because he is revealing the information to the bank in the ordinary course of business.[41]

In *Smith*, the victim of a robbery began receiving threatening calls after she gave the police a description of the robber and his car, a Monte Carlo.[42] After seeing the Monte Carlo drive past her house, she informed

33. There are several exceptions to the warrant requirement of the Fourth Amendment. In certain circumstances, a warrantless search or seizure may not be reasonable but will be deemed permissible if the conduct falls within one of the recognized exceptions. Common exceptions to the warrant requirement include (1) exigent circumstances, Missouri v. McNeely, 569 U.S. 141, 148–50 (2013); (2) consent, Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973); (3) a search incident to lawful arrest, Chimel v. California, 395 U.S. 752, 762–63 (1969); (4) plain view, Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971); and (5) the automobile exception, Carroll v. United States, 267 U.S. 132, 149 (1925).

34. Soldal v. Cook County, 506 U.S. 56, 63–64 (1992).

35. U.S. CONST. amend. IV.

36. United States v. Miller, 425 U.S. 435 (1976).

37. Smith v. Maryland, 442 U.S. 735 (1979).

38. *Miller*, 425 U.S. at 437.

39. *Id.* at 438.

40. *Id.*

41. *Id.* at 440–43.

42. *Smith*, 442 U.S. at 737.

the police.[43] The police later spotted a man who met the description driving a Monte Carlo.[44] The police ran a search on the car's license plate number and discovered that the car was registered to Michael Smith.[45] They asked his telephone company to use a pen register to record the numbers dialed from his home.[46] When the pen register recorded a call from Smith's house to the victim, the police obtained a warrant, searched Smith's house, and discovered a phone book turned to a page with the name and number of the victim.[47] Smith sought to suppress the evidence derived from the pen register.[48] He argued that the police obtained the evidence without a warrant thereby violating his reasonable expectation of privacy.[49] The Court disagreed with Smith.[50] The majority held that Smith did not have a reasonable expectation of privacy because even if he harbored a subjective expectation that the numbers he dialed would remain private, this expectation was not one that society would recognize as reasonable.[51] The Court stated that in general, people recognize that they convey phone numbers to the telephone company in order to facilitate calls, and that the phone company makes permanent records of the numbers they dial for recordkeeping, billing, and other purposes.[52] As such, "[a]lthough subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[53]

Together, *Miller* and *Smith* established the third-party doctrine, which holds that individuals do not have a reasonable expectation of privacy in information they voluntarily reveal to third parties. The decisions also indicated that the Fourth Amendment did not provide sufficiently strong privacy protections in the context of third party records and, by extension, the networked environment.

As the use of the Internet and e-mail communications increased, and as individuals provided more information in the form of data to service providers, it remained uncertain whether the Fourth Amendment applied in the context of computer networks.[54] The concerns raised by the third-party doctrine were further amplified because under the Fourth

43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.* at 738.
50. *Id.* at 742.
51. *Id.*
52. *Id.*
53. *Id.* at 743.
54. KERR, COMPUTER CRIME LAW, *supra* note 25, at 622–23.

Amendment's private search doctrine, an ISP or other service provider (e.g., a telephone company) was authorized to search through the data in its possession and disclose the fruits to law enforcement.[55] In response, Congress passed the SCA to provide statutory privacy rights that supplement the constitutional rights of individuals as relating to searches and seizures.

C. The Stored Communications Act

In enacting the SCA, Congress sought to balance the privacy interests of society—recently undermined and diminished due to the third-party doctrine—with the legitimate needs of law enforcement to access such information.[56]

The SCA is not intended to serve as a catch-all privacy statute; rather, it is narrowly tailored to regulate the retrospective surveillance of communications.[57] The statute balances investigators' needs against the privacy needs of individuals in two ways. First, the statute limits the government's ability to compel service providers to disclose user information in their possession.[58] Second, the statute limits the providers' ability to voluntarily disclose user information to the government.[59] Section 2703 regulates the former,[60] while Section 2702 regulates the latter.[61] Though the SCA has other important sections that define the relevant terms,[62] regulate delayed notice,[63] or establish remedies,[64] this Article will focus primarily on § 2703. Specifically, it will explore and analyze § 2703(f), the subsection of the SCA authorizing the issuance of "preservation letters" or "f" letters.

1. Required Disclosure of Customer Communications or Records

Section 2703 establishes the rules that the government must follow in order to compel a service provider to disclose customer communications or records. The SCA differentiates between electronic communication service providers (ECS) and remote computing service providers (RCS). An ECS is defined as "any service which provides to users thereof the

55. *See* Kerr, *A User's Guide*, *supra* note 27, at 1212.
56. *See id.* at 1214.
57. *See id.*
58. KERR, COMPUTER CRIME LAW, *supra* note 25, at 676.
59. *Id.*
60. 18 U.S.C. § 2703.
61. 18 U.S.C. § 2702.
62. 18 U.S.C. § 2711.
63. 18 U.S.C. § 2705.
64. 18 U.S.C. § 2708.

ability to send or receive wire or electronic communications."[65] And a RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[66]

These are the two types of providers regulated by the SCA. When the government seeks to compel either an ECS or a RCS to disclose customer communications or records, it must satisfy different legal standards depending on whether it is seeking non-content or content information.

Broadly speaking, non-content information refers to records or other information pertaining to a customer or subscriber.[67] Non-content information includes transactional records, such as network and telephone logs,[68] cell site location information (CSLI),[69] and e-mail addresses of individuals with whom the customer has corresponded.[70] The government may gain access to this category of information either by obtaining customer consent, a court order based on specific and articulable facts, also known as a "2703(d) order" or simply "d" order, or a search warrant.[71]

A subcategory of non-content information, which has been deemed less private and thus afforded less protection, is referred to as Basic Subscriber Information (BSI).[72] Because BSI is the least protected category of information, the government may compel the disclosure of BSI through an administrative, grand jury, or trial subpoena.[73] BSI was separated from other non-content records in the 1994 amendments to § 2703(c). The legislative history of the amendments indicates that the purpose of the separation was to distinguish non-content information from more revealing transactional information that could contain a "person's entire on-line profile."[74] BSI includes the subscriber's name; address; telephone connection records or session times and duration; length of service and the types of service utilized; telephone or instrument number, subscriber number, or other identity, including any temporarily assigned network address; and means and source of payment for such a device (including credit card or bank account number).[75] According to the Department of Justice (DOJ), "[i]n the Internet context, 'any temporarily assigned network address' includes the IP address used by a customer for

65. 18 U.S.C. § 2510(15).

66. 18 U.S.C. § 2711(2).

67. This Article will use the terms "customer," "subscriber," and "user" interchangeably.

68. KERR, COMPUTER CRIME LAW, *supra* note 25, at 680; DOJ Manual, *supra* note 2, at 121.

69. *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 607, 611–12 (5th Cir. 2013).

70. DOJ Manual, *supra* note 2, at 121.

71. KERR, COMPUTER CRIME LAW, *supra* note 25, at 680.

72. *Id.*

73. 18 U.S.C. § 2703(c)(2).

74. DOJ Manual, *supra* note 2, at 122; H.R. REP. NO. 103-827, at 17, 31–32 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3497, 3511–12.

75. 18 U.S.C. § 2703(c)(2)(A)–(F).

a particular session. For example, for a webmail service, the IP address used by a customer accessing her email account constitutes a 'temporarily assigned network address.'"[76]

In contrast, content information concerns the substance of the communication and encompasses the actual files or data on the account. Contents, "when used with respect to any wire, oral, or electronic communication, include any information concerning the substance, purport, or meaning of that communication."[77] For instance, the content of a text message is the actual text message; similarly, the body of an e-mail, the subject lines of an e-mail, or a voicemail all constitute "content."[78] Content information is provided a higher degree of protection than non-content information. To compel the disclosure of content information, the government must obtain a search warrant or provide user notice in combination with either (1) a subpoena or (2) a "2703(d) order."[79]

In some instances, law enforcement may want to compel a service provider to disclose certain information from a user's account yet lack a search warrant, "d" order, subpoena, or other valid legal process. Under such circumstances, 18 U.S.C. § 2703(f) permits the investigators to direct a service provider to preserve the records and other evidence related to the account for ninety days, and potentially up to one hundred eighty days, pending the issuance of valid and compulsory legal process.[80]

2. Preservation Requests and Section 2703(f)

Section 2703(f)(1) of the SCA states that a provider of ECS or RCS "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."[81] Such records and other evidence may "be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity."[82]

As has been noted by Professor Kerr, the language of this provision is odd for several reasons: it contains both mandatory and permissive language; and perhaps more importantly, it uses the term "records and

76. DOJ Manual, *supra* note 2, at 121.
77. 18 U.S.C. § 2510(8).
78. DOJ Manual, *supra* note 2, at 123.
79. KERR, COMPUTER CRIME LAW, *supra* note 25, at 679; 18 U.S.C. § 2703(d).
80. DOJ Manual, *supra* note 2, at 129.
81. 18 U.S.C. § 2703(f)(1).
82. 18 U.S.C. § 2703(f)(2).

other evidence," which is broader than "non-content information."[83] This ambiguity leaves open the question of whether the government can demand that a service provider preserve both content and non-content information, or whether preservation requests apply only to non-content information or metadata. In practice, most service providers who are recipients of "f" letters preserve both the content and non-content information of the relevant user account(s).

Section 2703(f) does not mandate a specific format for a preservation request. Rather, the government may submit a request to a service provider via a phone call, fax, or e-mail.[84] A preservation request does not require any degree of suspicion, need, exigency, or judicial approval.[85] Upon the receipt of a preservation request, the service provider must take all necessary steps to copy and retain all existing records and other evidence pursuant to the request.

As mentioned above in the *United States v. Warshak* discussion, a preservation request does not authorize the monitoring and freezing of prospective records and other evidence not yet created.[86] The court in *Warshak* permitted the freezing of prospective records only because of the government's good faith reliance.[87] Section 2703(f) only permits the government to request that a service provider preserve the records and other evidence it already has in its possession. The government does not obtain access to the information using a preservation request. The "f" letter only preserves any existing evidence while the government obtains a court order or other process.

Such preservation requests are often accompanied by a Non-Disclosure Order (NDO), which permits the investigators to direct service providers not to disclose the existence of the preservation request to the user or any other person (other than necessary to comply with the request). Alternatively, the "f" letter may contain a non-disclosure request in which investigators simply ask the provider not to disclose the existence of the preservation letter.[88]

Although the *Warshak* decision received much attention in the legal community—especially among electronic surveillance scholars and

83. Orin Kerr, Opinion, *The Fourth Amendment and Email Preservation Letters*, VOLOKH CONSPIRACY (Oct. 28, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/28/the-fourth-amendment-and-email-preservation-letters/ [https://perma.cc/MJV3-84YN].

84. DOJ Manual, *supra* note 2, at 140.

85. Kerr, *The Fourth Amendment*, *supra* note 83; Brief of Amici Curiae ACLU et al. in Support of Defendant-Appellant Kaleb Basey at 6, United States v. Basey, 784 F. App'x 497 (9th Cir. 2019) (No. 18-30121), 2019 WL 829338, at *6 [hereinafter ACLU Brief].

86. *See* United States v. Warshak, 631 F.3d 266, 286 (2010); KERR, COMPUTER CRIME LAW, *supra* note 25, at 700; DOJ Manual, *supra* note 2, at 140.

87. *Warshak*, 631 F.3d at 288.

88. *See* 18 U.S.C. § 2705.

practitioners—the public remains generally unaware of the regularity with which the government issues preservation letters and the frequency with which service providers comply with such requests. This is in spite of the fact that the many service providers contain law enforcement exceptions in their Privacy Policies or Terms of Service (TOS) and publish "Transparency Reports" detailing the number and types of requests they receive. Part II of this article surveys various service providers' Privacy Policies and Transparency reports.

II. PRIVACY POLICIES, TERMS OF SERVICE, AND TRANSPARENCY REPORTS

Service providers that offer services to the general public and possess users' data often receive search warrants, subpoenas, preservation requests, or other legal processes from the government. A service provider may be required to disclose any and all information it possesses that is associated with a specific user account or numerous accounts. This may include content or non-content information. Such requests, especially if for content information, will generally require a warrant.

Law enforcement entities are also authorized to demand that a service provider preserve all records and other evidence related to an account. In this scenario, the government will submit a § 2703(f) letter to the service provider in question and request that all records and other information related to the account be preserved.

In an effort to balance user privacy and investigatory needs, service providers will often indicate in their Privacy Policy or TOS[89] that they will comply with legitimate legal process. Google, for instance, states: "We will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to: [m]eet any applicable law, regulation, legal process, or enforceable governmental request."[90] Amazon claims it "does not disclose customer information in response to government demands unless [Amazon is] required to do so to comply with a legally valid and binding order."[91] Facebook's Data Policy explains that the company will

> access, preserve and share [user] information with regulators, law enforcement or others: In response to a legal request (like a search

89. This article uses the phrase "Terms of Service" to refer to Terms of Service as well as Terms of Use.

90. *Privacy Policy*, GOOGLE (Mar. 31, 2020), https://policies.google.com/privacy#infosharing [https://perma.cc/KL68-C64F].

91. *Law Enforcement Information Requests*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF [https://perma.cc/9KDK-2KZK].

> warrant, court order or subpoena) if [it has] a good faith belief that the law requires [it] to do so . . . . Information [Facebook] receive[s] about [a user] (including financial transaction data related to purchases made with Facebook) can be accessed and preserved for an extended period when it is the subject of a legal request or obligation, governmental investigation, or investigations of possible violations of our terms or policies, or otherwise to prevent harm.[92]

Similarly, Twitter's Privacy Policy states that it "may preserve, use, share, or disclose [users'] personal data or other safety data if [Twitter] believe[s] that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request[.]"[93] In its guidelines for law enforcement, Twitter explains that the company accepts requests from law enforcement to preserve records, that it will preserve a temporary snapshot of the relevant account records for ninety days, and that it will not disclose preserved evidence without valid legal process.[94] In order for a preservation request to be valid, Twitter requires the requesting agency to sign the request, have a valid return official e-mail address, be on official law enforcement letterhead, and include the @username and URL of the subject Twitter profile.[95] Such requests can be uploaded via a website provided by Twitter.[96]

Though a service provider may preserve all information related to a specified account or set of accounts pursuant to a § 2703(f) request without informing the account user, service providers regularly tell law enforcement that they will notify the relevant account user(s) prior to disclosing content information. For instance, Amazon explains that "unless prohibited from doing so or [if] there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing content information."[97] Two facts are important to highlight: (1) such statements typically limit user notification to situations in which *content* information is being disclosed and not where *non-content* information is at issue; and (2) law enforcement

---

92. *Data Policy*, FACEBOOK (Apr. 19, 2018), https://www.facebook.com/policy.php#legal-requests-prevent-harm [https://perma.cc/8W3Q-WTD5].

93. *Twitter Privacy Policy*, TWITTER (June 18, 2020), https://twitter.com/en/privacy [https://perma.cc/5DQT-KDYD].

94. *Guidelines for Law Enforcement*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#6 [https://perma.cc/3WXM-XK2K].

95. *Id.*

96. *See Legal Request Submissions*, TWITTER, https://legalrequests.twitter.com/forms/landing_disclaimer [https://perma.cc/8UD2-2KK4] [hereinafter TWITTER, 2016]. Facebook provides a similar online portal through which law enforcement can "expeditiously submit formal preservation requests." *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines/ [https://perma.cc/AM2D-YPPP].

97. *See Law Enforcement Information Requests*, *supra* note 91.

has the option of including an NDO with its preservation request, which prohibits the service provider from disclosing the existence of such a request. An NDO, however, must be approved and signed by a court, which generally requires law enforcement to illustrate to the court a certain amount of existing evidence as to why the account must be preserved. This ensures a degree of oversight by a neutral and detached magistrate thereby protecting user privacy.

As noted above, service providers often include law enforcement compliance information in their Privacy Policy or TOS. Nonetheless, users rarely read or understand these policies. A Brookings Institution survey found that three quarters of online users rarely read the TOS.[98] Further, according to the *New York Times*, the vast majority of privacy policies exceed the college reading level, and over half of Americans may struggle to understand these dense and lengthy texts.[99] It remains questionable whether users have a firm appreciation of how effortlessly investigators can request the preservation of user account information and how frequently service providers comply with such requests. As user awareness of privacy issues has increased, companies have attempted to provide more transparency regarding their privacy practices. One outcome is the publication of Transparency Reports. Service providers may choose to publish Transparency Reports disclosing the statistics about the quantity and types of requests they have received. The next section focuses on preservation request statistics published in Transparency Reports.

First, Google began reporting on the number of requests for user or account information in the first half of 2011.[100] As indicated by the data, Google's first indication of receiving preservation requests from law enforcement is during the period between July 2014 through December 2014.[101] During that time period, Google received 4,290 preservation requests from investigators in the United States.[102] That number has

98. Darrell M. West, *Brookings Survey Finds Three-Quarters of Online Users Rarely Read Business Terms of Service*, BROOKINGS (May 21, 2019), https://www.brookings.edu/blog/techtank/2019/05/21/brookings-survey-finds-three-quarters-of-online-users-rarely-read-business-terms-of-service/ [https://perma.cc/YH2J-ENSR].

99. Kevin Litman-Navarro, Opinion, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html [https://perma.cc/KVG2-C9L3].

100. *Transparency Report*, GOOGLE, https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period [https://perma.cc/9NT7-6FCB].

101. This is according to the data available in Google's Transparency Report. *See id.* It is possible that Google did not maintain any data regarding the receipt of preservation requests prior to this date.

102. *Id.*

steadily increased during each reporting term with the exception of one term. The number of preservation requests between January and June 2016 was 5,817; this figure dropped to 5,717 for the period between June and December 2016.[103] In its most recent reporting term (July 2018–December 2018), Google received 9,578 preservation requests.[104] It is important to note that a single preservation request does not necessarily seek the preservation of a single user's account; rather, a single preservation request may seek to preserve information associated with multiple accounts.[105] As such, the actual number of individual user accounts implicated in § 2703(f) requests is likely to be significantly higher than the published numbers.

Second, Facebook provides a more detailed breakdown of the information concerning data requests. Facebook categorizes the requests it receives as "Preservation Requests" and "Preservation Accounts Preserved." At the time of writing this Article, Facebook's data regarding preservation requests covers the period between the first half (H1) of 2016 through the second half (H2) of 2018.[106] According to this data, from January 2016 through June 2016, the company received 31,894 preservation requests from law enforcement entities in the United States.[107] During this same period, the number for Preservation Accounts Preserved was 56,714.[108] Similar to Google, the number of preservation requests to Facebook steadily increased during each reporting period since 2016, with the exception of H2 2017, during which the number of requests decreased from 48,836 (H1 2017) to 47,127 (H2 2017).[109] In its latest figures (H2 2018), Facebook reveals that it received 56,404 Preservation Requests and preserved information from 95,799 user accounts.[110]

Finally, Twitter has a similar story. It began providing preservation request records in 2016, and the company explains that it received 1,283 preservation requests in H1 2016, affecting 3,311 accounts.[111] By H2

103. *Id.*

104. *Id.*

105. *Id.* ("A single user data request may seek information about multiple accounts, so the number of accounts requested may be higher than the number of total requests. Additionally, one person can have multiple Google accounts, or the same account may the subject of several different requests for user information.").

106. *Government Requests for User Data*, FACEBOOK TRANSPARENCY, https://transparency.facebook.com/government-data-requests [https://perma.cc/T5ME-3AE4].

107. *Id.* During this same period, Facebook received approximately 6,806 preservation requests from other countries' law enforcement agencies. *Id.*

108. *Id.*

109. *Id.*

110. *Id.*

111. *Transparency Report: Information Requests*, TWITTER, https://transparency.twitter.com/en/information-requests.html#information-requests-jan-jun-2016 [https://perma.cc/E5FW-6TGB] [hereinafter TWITTER, 2016 Report]. This number does not include preservation extension requests.

2018, Twitter had received 3,265 preservation requests from investigators in the U.S. with 1,187 accounts specified.[112] This means that law enforcement agencies were only able to identify about one-third of the specified accounts for which they sought information.[113] These figures indicate that investigators often lack specific information about which user accounts may contain evidence related to an investigation. Further, since investigators need not meet the high threshold of a warrant when issuing a preservation request, they appear to cast a wider net when issuing such requests.

Part II provided some statistics as to the quantity of preservation requests issued by investigators in the United States. The companies examined are not the only entities which receive and comply with law enforcement requests. Nor are they the only service providers that disclose the statistics related to such requests. These companies were selected and discussed primarily due to their market size and influence. Part III discusses the policy and legal considerations surrounding § 2703(f).

III. POLICY AND LEGAL CONSIDERATIONS

This Article has discussed the historical context and background of the SCA, the language of 18 U.S.C. § 2703(f), and the figures surrounding the issuance of preservation requests. Part III aims to impartially present and evaluate both the benefits and harms of using "f" letters as a law enforcement tool.

A. Benefits of Section 2703(f)

Proponents of § 2703(f) make several arguments as to why preservation requests, as the mechanism and provision currently exist, are valuable and constitutionally valid. First, the existing regime guarantees that potential evidence of a crime will not be destroyed or lost before investigators can obtain valid legal process to compel the disclosure of the preserved information. Second, it permits the government to preserve evidence in a minimally intrusive way. Third, preservation of records and other evidence does not constitute a search or seizure, and even if it does, the user has consented to the preservation. Finally, the preservation of account information pursuant to § 2703(f) is reasonable under the Fourth Amendment.

---

112. *Transparency Report: Information Requests*, TWITTER, https://transparency.twitter.com/en/information-requests.html#information-requests-jul-dec-2018 [https://perma.cc/NG5U-ZG4G].

113. *See id.* The total figures, which include preservation requests from other nations, are similarly disturbing: the company received 3,970 account preservation requests, 1,514 of which identified specific accounts. *Id.*

1. Preservation Requests Help Protect Evidence

When § 2703(f) was drafted in 1996, the nature of the Internet, electronic surveillance, and data processing and storage were vastly different than today. It was common for a service provider to delete account records every thirty to sixty days in the 1990s.[114] As such, it was sometimes necessary for investigators to request the preservation of evidence while they obtained valid legal process.[115]

This was a real concern for law enforcement as acknowledged by the DOJ: If "a crime occurs on Day 1, agents learn of the crime on Day 28, begin work on a search warrant on Day 29, and obtain the warrant on Day 32, only to learn that the network service provider deleted the records in the ordinary course of business on Day 30," then the relevant evidence has been lost and valuable governmental resources have been wasted.[116] Section 2703(f) minimizes this risk by requiring a service provider to freeze the records while the government presents evidence to a neutral magistrate in the hope of obtaining a subpoena, warrant, or (d) order. Should the government fail to do so, the service provider is free to delete the records after ninety days, or one hundred eighty days if the government obtained a preservation extension, thereby ensuring that the government does not gain access to the preserved information without valid legal process.

Having the authority to issue a preservation request while continuing the investigation also provides investigators the opportunity to comprehensively examine the evidence and reduces the burden on the judiciary. A lot of time and resources could be wasted if investigators were required to obtain judicial approval for a preservation request without first being certain that the relevant records even exist. As the process currently functions, investigators can request the preservation of records, investigate further, and if relevant evidence exists, advocate for a neutral magistrate to issue the legal process authorizing the government to access the records. Alternatively, law enforcement may discover that the records sought do not exist or do exist but do not contain relevant evidence. If the records do not exist, then the issuance of a preservation letter does not cause any harm; the service provider simply notifies the government that it does not have any relevant information in its possession to preserve. If the records do exist but are irrelevant, because investigators have not obtained access to the data, they can refocus their inquiry elsewhere. In this case, the service provider will delete the records in the ordinary course of business.

114. Kerr, *The Fourth Amendment*, *supra* note 83.

115. *Id.*

116. DOJ Manual, *supra* note 2, at 131.

2. Preservation Requests are a Minimally Intrusive Process

In addition to protecting potentially valuable evidence, preservation letters are also a minimally intrusive investigative method. A § 2703(f) request does not preserve any content or non-content information prospectively. It does not permit the disclosure of information to the government without valid legal process. And, it offers a way to further investigatory needs without interfering with a user's use of her account.

As the court stated in *Warshak*, "the plain language of § 2703(f) permits only the preservation of e-mails in the service provider's possession at the time of the request, not the preservation of future e-mails."[117] This holding has been incorporated into the DOJ's current approach on searching and seizing computers and obtaining electronic evidence. The DOJ Manual directs agents not to use "f" letters prospectively to order service providers to preserve records not yet created.[118] This limitation is noteworthy. By restricting the preservation of account information to the data the service provider has in its possession at the time of the request, the provision ensures that the government does not circumvent the higher standards prescribed for conducting real time surveillance denounced in *United States v. Warshak* and that any privacy intrusion by the government is minimal.

Moreover, a § 2703(f) letter does not, by itself, mandate the disclosure of information; it only requires the preservation of existing account information. A service provider is not obligated to disclose preserved information—and is free to delete the information in the ordinary course of business once the preservation request period ends—if the government fails to obtain valid legal process. Consequently, a preservation of information, by itself and without further disclosure, has no bearing on the privacy of a user.

Preservation letters are also minimally intrusive because they do not interfere with a user's use of her account. When a service provider receives a § 2703(f) request, it typically does not notify the account user, does not restrict access to the account, and does not terminate the account. In fact, the DOJ's Sample Language for Preservation Requests states:

> I request that you not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the Account, or

117. United States v. Warshak, 631 F.3d 266, 335 (6th Cir. 2010) (Keith, J., concurring).

118. DOJ Manual, *supra* note 2, at 140. If agents want providers to record future communications, they must rely on the pen register statute or the Wiretap Act. *Id.*

> otherwise alert any user of the Account as to your actions to preserve the information described below, please contact me as soon as possible and before taking action.[119]

Hence, the service provider will ordinarily make a copy of the account information and maintain it for the duration of the request period. This approach to preserving evidence is beneficial and constitutionally valid for three reasons. First, it does not interfere with a user's possessory interest in her account since the user is not made aware that her data was electronically preserved. If a user has no idea that her information has been copied, and if the information is deleted without the government ever gaining access to it, then the government has not interfered with the user's use of her account. Second, the service provider is permitted to delete any copied account information if the government does not obtain valid legal process. And third, the user is free to use or delete her account as she deems suitable, even if a copy of the account is preserved by the service provider.[120]

Section 2703(f) prohibits the government from preserving account information prospectively or gaining access to the user's data without valid legal process. Even when account information is preserved, the user may continue using her account. In fact, as evinced by the DOJ's sample language, the government endeavors to ensure the user is not made aware of the preservation request and asks that the service provider not alert the user when preserving the data in the account. Proponents of "f" requests agree that these safeguards guarantee the preservation of account information pursuant to a § 2703(f) request is minimally intrusive.

3. No Government Action, No (Fourth Amendment) Problem

As federal law currently stands, the preservation of account information is constitutionally valid because it is carried out by a private entity and not the government. In order for the Fourth Amendment to apply, the conduct at issue must be by a government agent. While private parties can be considered a government agent for the purposes of the Fourth Amendment, the government contends that a service provider preserving account information pursuant to a § 2703(f) request is not acting as an agent of the government because it is merely complying with a legal duty.[121] Accordingly, the preservation of account information does not create an agency relationship and does not violate the Fourth Amendment.

---

119. DOJ Manual, *supra* note 2, at 225.

120. Kerr, *The Fourth Amendment*, *supra* note 83.

121. Appellee's Answering Brief at 20, United States v. Basey, 784 F. App'x 497 (No. 18-30121), 2019 WL 2234564, at *20 (9th Cir. 2019) [hereinafter DOJ Brief].

4. Preservation Requests Are Reasonable Under the Fourth Amendment

Even if there is an agency relationship, the government has argued in a recent case that the preservation of account information is not a seizure.[122] The government further maintains that if a preservation request constitutes a search or seizure, it is one that is reasonable and consequently constitutionally permissible. Notwithstanding these arguments, the government also believes that two exceptions to the Fourth Amendment apply to preservation requests.

A seizure involves "some meaningful interference with an individual's possessory interest in [her] property."[123] Because a user maintains unhindered access to her account despite the service provider's copying of the account information, the government is not meaningfully interfering with the user's possessory interest. So, according to the government, preservation of account information is not a seizure within the meaning of the Fourth Amendment.

To determine whether searches and seizures are reasonable, courts rely on the two-pronged *Katz* test mentioned in Part I. The government's position regarding the use of "f" letters is that users do not have a subjective expectation of privacy because the TOS inform users that service providers will comply with valid legal process, which may entail the preservation of user account information. The existence of the third-party doctrine also supports the proposition that users do not have a reasonable expectation of privacy in their preserved account information. According to this doctrine, individuals do not have a legitimate expectation of privacy in information they voluntarily turn over to a third party. Since users willingly provide their information to service providers, they do not have a reasonable expectation of privacy in this information. Because the Fourth Amendment prohibits only unreasonable searches and

122. *Id.* at 21. In *United States v. Basey*, the defendant sought to argue that the long-term use of "f" letters was unconstitutional. *Id.* at 10-14. In that case, the government relied on "f" letters to copy and preserve the defendant's account information for nine months. *Id.* at 21–22. The District Court declined the defendant's motion to suppress the evidence obtained through the use of § 2703(f) and the defendant appealed to the Ninth Circuit. *Id.* at 9. Though the Ninth Circuit declined to address the merits of the constitutional argument and upheld the lower court's ruling on procedural grounds, *Basey*, 784 F. App'x at 497, in its brief to the Ninth Circuit the DOJ argued that a preservation of account information is not a seizure, DOJ Brief, *supra* note 121, at 21-25. According to the DOJ Brief, when the government sends out a § 2703(f) request, the government does not meaningfully interfere with the user's possessory interest in his property since the government "obtains no information at all, and the account owner retains full and unhindered access to his account." DOJ Brief, *supra* note 121, at 22. Further, since the "f" letter "requires only temporary preservation of information . . . [t]his temporary mandate does not constitute a meaningful interference with an account holder's possessory interest." DOJ Brief, *supra* note 121, at 22.

123. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

seizures, and because users do not have a reasonable expectation of privacy in such information, their Fourth Amendment rights are not violated by the government's use of "f" letters.

The government claims that consent is the first exception to the warrant requirement for seizures.[124] It argues that consent exception applies to preservation requests because if users want to use a service, they generally have to agree to the TOS.[125] Customarily, the TOS will contain a provision that declares the company will share user information to comply with all applicable laws and regulations. The government contends that users, through their acceptance of the TOS, have consented to their service provider preserving their account information.[126] Because users have consented, consent is a well-recognized exception to the Fourth Amendment's warrant requirement, and service providers have common authority over the servers on which the account information resides, the preservation of the account information does not violate the Fourth Amendment.

The second exception to the warrant requirement is one involving exigent circumstances. Under this exception a warrantless seizure may be constitutional if the government has probable cause to believe that the item or place in question contains evidence of a crime, and it seeks to prevent the imminent destruction of that evidence.[127] Data is especially easy to pulverize. It follows that § 2703(f) serves a compelling government interest in that it permits electronic evidence, which can be "deleted irretrievably in an instant," to be preserved long enough for investigators to obtain appropriate legal process under exigent circumstances.[128]

As the process currently exists, there is a strong and valid argument that it provides a fair balance between a compelling government interest in obtaining evidence and protecting the privacy of individuals. Records are preserved only temporarily, are not accessed by the government without the appropriate legal process, and the service provider can delete copied records after the preservation period concludes. Preservation requests do not apply prospectively, do not hinder a user's access to her records, and are generally minimally intrusive. Importantly, the preservation of records by a service provider is not a seizure. Even if the preservation of account information constituted a seizure, it is reasonable. Because users have consented to the TOS and are on notice that a service provider will comply with applicable laws and regulations, users do not

124. DOJ Brief, *supra* note 121, at 25.
125. *Id.* at 25–27.
126. *Id.* at 25.
127. Ker v. California, 374 U.S. 23, 40 (1963).
128. DOJ Brief, *supra* note 121, at 28.

have a reasonable expectation of privacy in their account information, which is in the possession of the service provider. The preservation of account information pursuant to § 2703(f) also falls within the consent exception to the warrant requirement if a user has consented to the service provider's TOS. Finally, the ease with which a user can erase electronic information—which may be valuable evidence of a crime—justifies the warrantless preservation of electronic evidence by the government through a preservation request under the exigent circumstances exception.

B. Harms of Section 2703(f)

Critics of 18 U.S.C. § 2703(f) maintain that the provision is outdated, circumvents privacy protections by avoiding judicial oversight, is relied upon excessively, contains textual inconsistencies,[129] lacks Fourth Amendment safeguards, and violates the Fourth Amendment because it infringes on users' reasonable expectation of privacy and constitutes a seizure. The following subsections examine each of these assertions.

1. New Technology, New Concerns

Section 2703(f) was drafted in the 1990s. At that time, copious long-term storage by service providers was not possible. In fact, an important milestone in data storage occurred in 1996 when "digital storage became more cost-effective for storing data than paper."[130] In the 1990s, advanced corporate hard-drives stored approximately two gigabytes of data.[131] Today, consumer-friendly computers are typically equipped with 250 gigabyte hard drives, while corporate hard drives can store terabytes of data.[132] This growing storage capacity has correlated with users creating significantly more quantities of data. In 2012, IBM estimated that "90% of the data in the world today has been created in the last two years."[133] In

129. Kerr, *The Fourth Amendment*, *supra* note 83.

130. R. J. T. Morris & B. J. Truskowski, *The Evolution of Storage Systems*, 42 IBM SYS. J. 205, 206 (2003).

131. Rex Farrance, *Timeline: 50 Years of Hard Drives*, PCWORLD (Sept. 12, 2006), https://www.pcworld.com/article/127105/article.html [https://perma.cc/JEE5-J62P]; Lucas Mearian, *Data Storage -- Then and Now*, COMPUTERWORLD (Mar. 14, 2014), https://www.computerworld.com/article/2473980/data-storage-solutions-143723-storage-now-and-then.html#slide8 [https://perma.cc/XE2B-RKPH].

132. One terabyte is 1,000 gigabytes, one petabyte is 1,000 terabytes, and one exabyte is 1,000 petabytes. Storage capacity can be enhanced by using a Redundant Array of Independent Disks ("RAID"), essentially putting together multiple hard drives.

133. IBM, *What Is Big Data?*, FACEBOOK (Mar. 19, 2012), https://www.facebook.com/IBM/posts/90-of-the-data-in-the-world-today-has-been-created-in-the-last-two-years/293229680748471/ [https://perma.cc/NJ4L-Y2K5]; *see also* Bernard Marr, *How Much Data Do We Create Every Day?*

2017, individuals produced 2.5 quintillion bytes of data.[134] This figure is likely drastically higher today given the growth of Internet of Things (IoT) devices,[135] and it will only continue to increase in large part due to the rapid expansion of the technology industry combined with the ubiquity of wireless networks and the industry's decision to create more interconnected smart devices.

This evolution of data creation and storage capability allows service providers to store substantially more data for considerably longer durations. This concern was highlighted by the Supreme Court in *Riley v. California*.[136] In that case, a unanimous Court acknowledged that most adults now carry phones, which are capable of storing more sensitive information for a longer duration. Therefore, allowing the police to search a phone without a warrant is different from allowing them to occasionally search an item or two.[137]

Accordingly, while relying on "f" letters may have been prudent in the 1990s, their use may no longer be necessary.[138] This is because thirty years ago a service provider routinely deleted records every thirty to sixty days.[139] In today's environment, however, a service provider can and does store data for longer periods. Because companies now have the ability to maintain user data for longer, the government has ample opportunity to seek valid legal process and obtain the records using a warrant, (d) order, or subpoena without the need to preserve the evidence using "f" letters. If there are exigent circumstances and investigators are concerned that certain records may be deleted or destroyed, the government may still rely

---

The Mind-Blowing Stats Everyone Should Read, FORBES (May 21, 2018), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#6c85825460ba [https://perma.cc/4T38-2XRF].

134. *Id.*

135. The Internet of Things has been defined as "the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data." *Internet of Things*, THE NEW OXFORD AM. DICTIONARY (Angus Stevenson & Christine A. Lindberg eds., 3d ed. 2010); "The IoT is a giant network of connected things and people—all of which collect and share data about the way they are used and about the environment around them." Jen Clark, *What Is the Internet of Things?*, IBM BLOG (Nov. 17, 2016), https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/ [https://perma.cc/8C29-WKTN].

136. Riley v. California, 573 U.S. 373, 394 (2014).

137. *Id.* at 393–94.

138. It is also worth noting that many companies now rely on monetizing user data. As such, businesses are incentivized to store any and all data for longer durations. *See* Abhas Ricky, *What Should Be Your Data Monetization Strategy to Compete in the Borderless Economy?*, FORBES (May 8, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/05/08/what-should-be-your-data-monetization-strategy-to-compete-in-the-borderless-economy/#2048c7794095 [https://perma.cc/YQH8-NURF]; Jathan Sadowski, *Companies Are Making Money from Our Personal Data – But at What Cost?*, THE GUARDIAN (Aug. 31, 2016), https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon [https://perma.cc/L8ZJ-R5UV].

139. Kerr, *The Fourth Amendment*, *supra* note 83.

on the exigent circumstances exception to the Fourth Amendment in lieu of looking to § 2703(f) to preserve account information. However, as the law currently stands, law enforcement officers use preservation requests because the process is simply easier.

Not only is § 2703(f) outdated but the privacy concerns it implicates have become more common with technological advances. One such example is the application of Artificial Intelligence (AI) and Big Data to the information obtained through a preservation request. Big Data is a field that allows for the analysis of extremely large data sets to reveal patterns, trends, and associations. When the government requests the "preservation of all stored communications, records, and other evidence" in the possession of a service provider, it is potentially gaining access to an extremely large data set.[140] The government can consolidate these large sets of data and use AI and other modern technology to create a detailed log not just of a person's movement—which was the concern of the Supreme Court in *Carpenter*[141]—but also a detailed account of all of a person's activities, likes, dislikes, and opinions. This type of surveillance may have been a worry of dystopian science fiction novels in the past, but modern technology has made it a legitimate, palpable, and fully realized concern.

2. The Preservation Request Process Lacks Judicial Oversight

The lack of judicial oversight is another concern. The Fourth Amendment protects the privacy of individuals through various safeguards. These include requiring the government to have probable cause that a crime has been committed or that evidence of the crime is present in the place to be searched or item to be seized; particularly describing the place to be searched and the persons or things to be seized; requiring that there be a risk that evidence will be destroyed; mandating law enforcement to seek legal process within a reasonable time; or requiring oversight by a neutral and detached judge. None of these protections exist under § 2703(f).

a. Probable Cause

One of the ways that the Fourth Amendment protects people and places against unreasonable searches and seizures is by requiring that the government obtain a warrant based on probable cause when searching or

140. DOJ Manual, *supra* note 2, at 225.

141. Carpenter v. United States, 138 S. Ct. 2206 (2018); *see* discussion *infra* Part IV.

seizing people, places, or things.[142] The concept of probable cause has been interpreted as context-dependent, and the Supreme Court has defined it as "a fair probability that contraband or evidence of a crime will be found in a particular place."[143] Probable cause depends on the totality of circumstances, and it is a threshold that the government must meet when submitting an affidavit to a judge for a warrant.

Yet, § 2703(f) lacks this safeguard. The provision "gives law enforcement the power to unilaterally, and without suspicion or judicial approval, compel . . . service providers," through a phone call, fax, e-mail, or letter, to preserve their users' account information.[144] The text of the statute provides no specific guidance for making a request. When issuing a § 2703(f) letter, the government is not required to provide a judge with an affidavit supporting a fair probability that evidence of a crime will be found in the account records sought to be preserved. As such, a preservation request does not satisfy the Supreme Court-established requirement of proving probable cause prior to conducting a seizure.

The ambiguity of § 2703(f)'s language is also problematic. Whereas most provisions in § 2703 refer to "content" or "records," subsection (f) refers to "records and other evidence."[145] As noted above,[146] there is a difference between content and non-content information or records. The former is the substance of a communication, whereas the latter encompasses transaction records, routing information, or logs. Practitioners and scholars have analogized this distinction to a physical envelope containing a letter; the content is the substance of the letter inside the envelope, while the non-content information is the address on the outside of the envelope. The service provider in this example would be the post office or entity delivering the envelope. Clearly, the post office must read the outside of the envelope in order to deliver it. Yet, it would be inappropriate and illegal—absent the existence of exceptions or a warrant—for the post office or law enforcement to intercept, open, and read the content or substance of the letter.

But because § 2703(f) relies on vague language—i.e., records and other evidence—it is unclear whether content falls within the purview of the subsection. In practice, when a service provider receives a preservation request it copies both the content and non-content information associated with the account or accounts. Preserving non-content information without a warrant is similar to a litigation hold. A company involved in a legal

142. U.S. CONST. amend. IV.
143. Illinois v. Gates, 462 U.S. 213, 238 (1983).
144. ACLU Brief, *supra* note 85, at 3.
145. 18 U.S.C. § 2703(f)(1).
146. *See supra* Part I.

action may receive notice in anticipation of a lawsuit or investigation, ordering it to preserve documents and other materials relating to that lawsuit or investigation.[147] This litigation hold temporarily prevents the destruction of the company's records and other relevant evidence in the ordinary course of business and ensures the availability of such evidence for the discovery process.

A service provider relies on non-content information when conducting its business. For example, when a user posts a message on a social media platform, the platform or service provider needs the routing information in order to successfully transmit and publish that communication. Though this non-content information relates to the content created by the user, the user does not have ownership of the routing or transactional information. As such, requiring a company to retain the non-content information pursuant to a preservation request is deemed to be within the bounds of § 2703(f).

In contrast, if investigators, lacking a warrant, request that a social media company preserve the files uploaded by its users, they would effectively circumvent the higher threshold for obtaining content information. This distinction is important because while a service provider may have control over the content since its platform is being used, the content is in fact something that the user has a greater interest in and actually owns (as opposed to the non-content information). Preserving content information pursuant to a § 2703(f) letter is analogous to law enforcement asking a landlord to access a tenant's dwelling (or several tenants' dwellings), document everything inside, and preserve all the documented information only for investigators to possibly return ninety or 180 days later to legitimize the initial warrantless entry. Though the preservation of non-content information can be detrimental to Fourth Amendment protections, the warrantless preservation of content information is particularly harmful.

In showing that probable cause exists, investigators must particularly describe "the place to be searched[] and the persons or things to be seized."[148] According to the Supreme Court, "[t]he manifest purpose of this particularity requirement was to prevent general searches"[149] and to prohibit "the seizure of one thing under a warrant describing another."[150] This was the Founders' response to the "general warrants" and "writs of assistance," which permitted the British King's agents to carry out wide-

147. *Litigation Hold*, BLACK'S LAW DICTIONARY (9th ed. 2009).
148. U.S. CONST. amend. IV.
149. Maryland v. Garrison, 480 U.S. 79, 84 (1987).
150. Marron v. United States, 275 U.S. 192, 196 (1927).

ranging searches and seizures during the colonial era. The continued usage of such writs, despite the Founders' denunciation of these "worst instrument[s] of arbitrary power," ultimately contributed to the revulsion against the Crown.[151] This constitutional requirement has also been codified; Rule 41(e)(2) of the Federal Rules of Evidence requires that the warrant identify the person or property to be searched and identify any person or property to be seized.

Some circuits have established a multi-factor test to determine whether the specificity or particularity requirement is met. The Ninth Circuit, for instance, considers

> one or more of the following factors: "(1) whether probable cause exists to seize all items of a particular type described in the warrant; (2) whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued."[152]

In a traditional investigation of physical space or one involving tangible evidence, determining whether the particularity requirement is satisfied can be straightforward. For instance, if investigators believe that evidence of a crime exists inside a home, they may seek a warrant to search the entire house; however, a magistrate will generally not authorize the government to seize all the contents of the house because such a warrant would be overbroad.

Analyzing searches and seizures involving digital evidence on a physical computer are more complex. "Most computer warrants are executed in two stages. First, the computer hardware is taken away; second, the computer is searched for electronic evidence. The physical search comes first, and the electronic search comes second."[153] Essentially, investigators search the house or relevant location for the computer, seize the computer, and perform the digital search at a later time. Imagine a scenario in which law enforcement is authorized to seize a specific hard drive and search for evidence of a crime. The physical seizure is uncomplicated. However, the digital search and seizure are complicated. Is the government authorized to search every folder and directory on the hard drive, or must it limit its search to those files and folders that relate

151. Stanford v. Texas, 379 U.S. 476, 481–82 (1965).

152. United States v. Adjani, 452 F.3d 1140, 1148 (9th Cir. 2006) (quoting United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986)). The Ninth Circuit has also held that "[w]arrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible." *Id.* at 1147–48.

153. KERR, COMPUTER CRIME LAW, *supra* note 25, at 548.

to the investigation? Courts generally issue warrants that include a list of specific items to be searched, accompanied by a "'catch-all' provision allowing the seizure of any computer and electronic storage devices."[154] Such warrants have generally been held to be sufficiently particular, thereby simplifying the physical and electronic search process.[155]

Applying the particularity requirement to the seizure of purely intangible evidence is more challenging.[156] The Federal Rules of Evidence provide some flexibility for searching and seizing electronic evidence. Specifically, Rule 41(e)(2)(B) sanctions a two-step process that authorizes investigators, when possessing a warrant, to seize a storage media containing electronic evidence for later review. The government, however, must have a warrant to seize the evidence in the first place, a safeguard that is lacking under § 2703(f).

As noted previously, there is no legally prescribed format for a preservation request.[157] When seeking to preserve account information, the government typically issues a letter to the service provider identifying an account or range of accounts by username, e-mail address, or telephone number. While investigators are sometimes aware of the specific identity of an individual whose account information they seek, occasionally the government is only able to identify an account based on an IP address. Therefore, the government is unaware of the identity of the specific individual.

As mentioned in Part II, preservation requests do not necessarily demand the preservation of a single user's account; rather, a single preservation request may require the service provider to preserve information associated with multiple accounts.[158] In the second half of 2018, for instance, Facebook received a total of 71,400 Preservation Requests and preserved information from 119,600 accounts.[159] Of these, 56,404 preservation requests were from U.S. law enforcement alone, resulting in the preservation of information from 95,799 accounts. Data provided by Twitter also reveals that the company has received 3,265

154. *Id.* at 554.

155. *See* United States v. Burgess, 576 F.3d 1078, 1090 (10th Cir. 2009).

156. It is important to note that the particularity requirement only applies if the government is searching or seizing people, places, or things. It remains debatable whether preserving information pursuant to an "f" letter is a seizure. *Infra* Section V.B.5.e argues that preservation requests are seizures under the Fourth Amendment.

157. DOJ Manual, *supra* note 2, at 140.

158. *See Transparency Report*, *supra* note 100. "A single user data request may seek information about multiple accounts, so the number of accounts requested may be higher than the number of total requests. Additionally, one person can have multiple Google accounts, or the same account may [sic] the subject of several different requests for user information." *Id.*

159. *Government Requests for User Data*, *supra* note 106.

preservation requests from investigators in the U.S. in the second half of 2018; investigators, however, only identified 1,187 specific accounts.[160] This means that the government was only able to specifically identify about one-third of the accounts for which it sought information. The DOJ's Sample Language for Preservation Requests under 18 U.S.C. § 2703(f) asks service providers to preserve "[a]ll records and other information relating to the Account and any associated accounts."[161] This discrepancy in the number of preservation requests issued and specific accounts identified, as well as the DOJ's broad language seeking the preservation of information relating to the account and *any associated accounts*, reveals that investigators are not sufficiently meeting the particularity requirement. Rather, they are casting a wide net and hoping to capture and preserve evidence potentially related to an investigation. In practice, this leads to the seizure of a significant amount of irrelevant and private data, thus running afoul of the Fourth Amendment.

3. Preservation Requests Are Used Excessively

Constitutional safeguards exist to curb government power, prevent abuse, and ensure that if the government seeks to surveil an entity, it has cause to do so. By requiring a subpoena, (d) order, or warrant that mandates oversight by a neutral and detached magistrate and a finding of probable cause, the Constitution and statutory laws make it more challenging for law enforcement to surveil individuals or to seize and search people or their property.

Preservation letters lack any such safeguards. They are often issued without law enforcement having any suspicion, need, or exigency.[162] In fact, the DOJ recommends that investigators seek the preservation of evidence as soon as possible when they have reason to believe that electronic evidence exists.[163] The government argues that it is simply preserving evidence but not accessing it until it returns with valid legal process. In reality, investigators often do not return with valid legal process and the service provider destroys the preserved information at the conclusion of the ninety (or one hundred eighty) days—or in the ordinary course of business. Alternatively, "[w]hen investigators do return with a court order authorizing a search of the targeted account, they commonly wait months to do so."[164] Extending a preservation request, and even more

160. TWITTER, 2016 Report, *supra* note 111.
161. DOJ Manual, *supra* note 2, at 226.
162. ACLU Brief, *supra* note 85, at 2.
163. DOJ Manual, *supra* note 2, at 58.
164. ACLU Brief, *supra* note 85, at 6.

so, returning with legal process, occur so infrequently that in one case a court noted that

> this is the first time the Court can remember the government indicating it renewed its preservation request for the one-time, additional time of 90 days, as allowed under § 2703(f)(2). It is also the first time the Court can remember the government *seeking* a search warrant within that one-time renewal period, as seems to be the intent of subsection (f).[165]

As the practice currently exists law enforcement is simply using § 2703(f) to compel service providers to preserve a significant number of online accounts "just in case a need for the information arises later in the course of an investigation."[166] Facts and figures released by service providers in Transparency Reports support this inference.

Facebook received 56,404 preservation requests from U.S. law enforcement entities in the second half of 2018.[167] In the same period, it preserved 95,799 accounts.[168] But the numbers for search warrants, subpoenas, court orders, and (d) orders are significantly lower for the second half of 2018. Facebook received only 23,801 search warrants related to 36,652 accounts; 8,360 subpoenas for 13,728 accounts; 408 court orders for 510 accounts, and 786 (d) orders for 2,481 accounts.[169] This shows that § 2703(f) is often used as a powerful tool by law enforcement to arbitrarily preserve significant, and potentially irrelevant, amounts of data without cause or necessity. Such conduct largely sidesteps the procedural barriers put in place to prevent government overreach and abuse.[170]

---

165. *In re* Three Hotmail E-mail Accounts, No. 16-MJ-8036-DJW, 2016 WL 1239916, at *12 n.78 (D. Kan. Mar. 28, 2016) (denying application for search warrant).

166. ACLU Brief, *supra* note 85, at 6.

167. *Government Requests for User Data*, *supra* note 106.

168. *Id.*

169. *Id.*

170. In addition to these legal concerns, there are also significant financial concerns because complying with preservation requests is often time consuming and costly. When a service provider receives a preservation request, the company must first determine if it has any corresponding data. To do so, it must have the appropriate technological infrastructure in place to query its database for the information. If the company determines that it does not have the corresponding data, it must then inform the requesting agency that such data does not exist. At this point, the requesting agency may resubmit the request with further information, which would then require the company to once again search through its database. If the company does have the relevant information, it must have the system architecture in place to preserve the relevant data for up to 180 days (which takes up additional resources) and, if the government returns with the appropriate legal process, to then disclose a copy of the data to the government. Depending on the company's policy, it may also be required to notify the account user of the preservation request. In some instances, the preservation request may be overbroad,

4. Preservation Requests Violate Users' Reasonable Expectation of Privacy

The Fourth Amendment protects an individual from unreasonable searches and seizures. A person has a reasonable expectation of privacy when she has exhibited a subjective expectation of privacy and that expectation is one that society is willing to recognize as reasonable.[171] The third-party doctrine under *Miller* and *Smith* severely diminished privacy protections by establishing that individuals have no reasonable expectation of privacy in information they voluntarily provide to a third party. Yet, a recent case, *Carpenter v. United States*,[172] appears to have limited the third-party doctrine's application in certain circumstances.[173]

In *Carpenter*, the government obtained Carpenter's CSLI using court orders. Using these records—which covered a 127-day period—the government charged the defendant. Carpenter moved to suppress the evidence, arguing that the seizure of the CSLI violated his Fourth Amendment because the records had been obtained without a warrant supported by probable cause.[174] The Supreme Court held that the government's warrantless acquisition of the CSLI violated the defendant's Fourth Amendment right against unreasonable searches and seizures.[175] The majority reasoned that the seizure of an individual's CSLI was an "entirely different species of business records—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers."[176] Of particular concern to the Court was the government's ability to use third party records—CSLI in this case—to create a "detailed log of a person's movement over several years."[177] While a user's account information may not provide as detailed a log as would her CSLI, the data from an individual's account can be used to establish a person's movements and conduct over a period of time.

For instance, if the government requests that a service provider—a social media platform, an electric scooter company, or a

---

which will require the company to push back against the government request and negotiate what will in fact be disclosed. All of this requires significant time, resources, and legal sophistication. For this reason, many companies choose to hire a subpoena compliance team who specializes in responding to such requests, which, again, costs significant resources.

171. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

172. Carpenter v. United States, 138 S. Ct. 2206 (2018).

173. Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE BLOG (June 22, 2018), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/449J-NZSR].

174. *Carpenter*, 138 S. Ct. at 2208–09.

175. *See id.* at 2217.

176. *Id.* at 2222.

177. *Id.*

ridesharing company—preserve a user's account information, that data can be used to establish a comprehensive record of the individual's movements. An individual's movement can reveal a lot of details regarding her interests and private life. This would arguably be in conflict with the holding of *Carpenter* since the records are preserved pursuant to a government request without a warrant.

One court has considered the applicability of *Carpenter* to preservation requests. In *United States v. Rosenow*, the defendant, relying on *Carpenter*, asserted that the government unlawfully seized his private communications by issuing preservation requests to third parties without a warrant based on probable cause.[178] The government countered that the preservation of Rosenow's account was "not a meaningful interference with the Defendant's possessory interest in his account" because he "was free to continue to use his account."[179] The court agreed with the government and held that, because the "preservation requests in this case did not interfere with the Defendant's use of his accounts and did not entitle the Government to obtain any information without further legal process[,] . . . the preservation requests . . . did not amount to an intrusion subject to Fourth Amendment requirements."[180] Before addressing the possessory interest argument,[181] this Article will address whether users have a reasonable expectation of privacy in their account information, which would require the government to obtain a warrant, (d) order, or subpoena prior to submitting a preservation request.

As discussed in Part II, users rarely read or understand TOS or Privacy Policies.[182] When individuals do read these documents the majority of them may struggle to understand these legally sophisticated texts.[183] An individual who does not understand the TOS or Privacy Policy of her service provider can reasonably argue that she had a subjective expectation of privacy in her account. Nonetheless, courts are unlikely to find that she had a reasonable expectation of privacy because society may not recognize this expectation as objectively reasonable because virtually all service providers require their users to agree—in some form—to their TOS, thereby making individuals aware of the existence and function of these documents. Critics of § 2703(f) may assert that average users do not understand these documents as they are full of legalese. Because an

178. United States v. Rosenow, No. 17-CR-3430, 2018 WL 6064949, at *10 (S.D. Cal. Nov. 20, 2018).

179. *Id.*

180. *Id.*

181. *See* discussion *infra* Sections IV.B.5.b, IV.B.5.c.

182. West, *supra* note 98.

183. Litman-Navarro, *supra* note 99.

average individual cannot understand the TOS or Privacy Policy, she cannot provide informed consent to the terms and therefore has a subjective expectation of privacy. Moreover, because the majority of society is unable to fully appreciate the TOS or Privacy Policy, as well as the implications of such documents, then an individual's subjective expectation of privacy may be objectively reasonable.

Alternatively, critics also argue that users have an expectation of privacy in their account information because most take proactive measures to prevent others' access to their account. In *United States v. Haydel*, the government searched Haydel's parents' residence pursuant to a warrant.[184] In the course of the search, law enforcement discovered incriminating evidence in a cardboard box located under the bed of Haydel's parents.[185] Haydel claimed that the records were seized in violation of the Fourth Amendment, and the court sought to determine whether he "had a legitimate expectation of privacy for records secreted in his parents' home and under their bed."[186] Analyzing the facts, the court found that Haydel's parents had given him permission to use their home and had given him a key, thereby providing him unencumbered access.[187] The court stated that Haydel owned the records that were seized and found that he "had the authority to exclude persons other than his parents and their guests from the home."[188] This, the court believed, made it sufficiently clear that Haydel "exhibited a subjective expectation that the contents of the box stowed under his parents' bed were to remain private."[189] As such, the court held that Haydel had a legitimate expectation of privacy in the area searched.[190]

Similarly, individuals have a reasonable expectation of privacy in their account information because they utilize access controls, such as a username and password, to prevent others' access to their account. Similar to *Haydel*, where the defendant's parents permitted him to use their residence and provided him a key, service providers allow users to use their infrastructure but provide users a "key" to access their own accounts. Further, because users have unique login credentials and can exclude others from their accounts, they clearly exhibit a subjective expectation that the information in their account remain private. Therefore, users have a legitimate expectation of privacy in their account information.

---

184. United States v. Haydel, 649 F.2d 1152, 1154 (5th Cir. 1981).

185. *Id.*

186. *Id.*

187. *Id.* at 1155.

188. *Id.*

189. *Id.*

190. *Id.* The court ultimately held that the Fourth Amendment was not violated because the search warrant authorized the search and made the object of the search clear. *Id.* at 1158.

Finally, if information obtained pursuant to a warrantless preservation request is combined with Big Data analysis it may violate a user's legitimate expectation of privacy in her data. Modern technology allows the government to use large sets of data to establish patterns, trends, and associations, which can lead to an extremely detailed account of an individual's daily activities and interests. One cause of concern for the majority in *Carpenter* was the government's ability to use CSLI to obtain information that "is detailed, encyclopedic, and effortlessly compiled."[191] If the government demands that a service provider preserve a user's account information pursuant to a § 2703(f) request and subsequently creates a detailed log of a person's movements—something that is within the capability of modern law enforcement—the individual's legitimate expectation of privacy may be violated.[192]

5. Preservation Requests Constitute Unreasonable Seizures

The preservation of account information pursuant to a § 2703(f) request is a violation of the Fourth Amendment because it constitutes an unreasonable seizure. A "seizure" involves "some meaningful interference with an individual's possessory interest in [her] property."[193] This interference must be by the government or its agent.[194] A meaningful interference does not necessarily require the government to search the property; rather, preventing a user from using her property as she deems suitable—which may include deleting the account information or prohibiting others from accessing the information—also constitutes a meaningful interference with property.

a. Account Information Is "Property" Within the Meaning of the Fourth Amendment

The Fourth Amendment's protection of "effects" has generally been understood to extend to personal property[195] and "possessions."[196] While effects and possessions have traditionally been viewed as tangible items,

191. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

192. Even when the government gains access to the preserved information with a warrant, (d) order, or subpoena, the evidence found in the preserved information may be considered fruits of the poisonous tree because the initial seizure was without valid legal process.

193. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

194. *Id.*

195. *See* Oliver v. United States, 466 U.S. 170, 177 n.7 (1984).

196. State v. Davis, 929 A.2d 278, 295–96 (Conn. 2007); People v. Smith, 360 N.W.2d 841, 849 (Mich. 1984); Andrew G. Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 828 (2016).

various states, courts, and jurists have argued that the Fourth Amendment protects both tangible and intangible property.[197]

The Texas Property Code has defined the term to include "property held in any digital or electronic medium."[198] Other state legislatures have also considered intangible digital assets to be property. For example, in 2007, the Indiana state legislature considered a bill that regarded electronic documents as "estate property."[199] According to the ACLU, since 2013, at least forty-six states have enacted "laws regulating fiduciary duties with respect to digital assets, all of which explicitly recognize a deceased or incapacitated user's legal interest in access to their email communications."[200] In addition to state legislatures, state courts have also recognized intangible digital assets as property.

In *Ajemian v. Yahoo!, Inc*., a Massachusetts state court declared that an e-mail "account is a form of property often referred to as a 'digital asset.'"[201] In *Eysoldt v. ProScan Imaging*, the court conceded that the general rule at common law had only permitted converting tangible chattels. But the court stated that the law, which has changed, allows the conversion of intangible property rights and therefore permitted action for conversion of a web account as intangible property.[202]

Given these developments and the evolution of Fourth Amendment jurisprudence as related to digital assets, it is reasonable to consider data—which encompasses account information—as property within the meaning of the Fourth Amendment.

b. Individuals Have a Possessory Interest in Their Account Information

Individuals whose account information is preserved pursuant to a § 2703(f) request have a possessory interest in such digital assets. Possessory interest is generally defined as the right to control property, including the right to exclude others or to delete or destroy property.[203]

---

197. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. CHI. LEGAL F. 121, 135 (2008). *See generally* Ferguson, *supra* note 196; United States. v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010); Hoffa v. United States, 385 U.S. 293, 301 (1966) (finding that protections of the Fourth Amendment are surely not limited to tangibles).

198. TEX. PROP. CODE ANN. § 111.004(12) (West 2017). Similarly, "Missouri amended its state constitution in 2014 to protect 'persons, papers, homes, effects, and electronic communications and data, from unreasonable searches and seizures.'" ACLU Brief, *supra* note 85, at 16.

199. Alberto B. Lopez, *Posthumous Privacy, Decedent Intent, and Post-Mortem Access to Digital Assets*, 24 GEO. MASON L. REV. 183, 194 (2016).

200. ACLU Brief, *supra* note 85, at 17–18.

201. Ajemian v. Yahoo!, Inc., 84 N.E.3d 766, 768 (Mass. 2017).

202. Eysoldt v. ProScan Imaging, 957 N.E.2d 780, 786 (Ohio Ct. App. 2011).

203. *Possessory Interest*, BLACK'S LAW DICTIONARY (9th ed. 2009); ACLU Brief, *supra* note 85, at 15.

One need not be the *owner* of property to have Fourth Amendment protections concerning that property.[204] Other factors—in addition to ownership—that courts consider include:

> whether the defendant has a possessory interest in the thing seized . . . , whether he has the right to exclude others from that place, whether he has exhibited a subjective expectation that it would remain free from governmental invasion, whether he took normal precautions to maintain his privacy and whether he was legitimately on the premises.[205]

The right to exclude others is one of the fundamental elements of having possessory interest in real or personal property and has been a long-recognized principle of common law and jurisprudence. William Blackstone recognized this right in his *Commentaries on the Laws of England*.[206] The Supreme Court has recognized this right in numerous cases.[207] And various circuit courts have also recognized the right to exclude others as fundamentally valuable and a quintessential property right.[208]

---

204. United States v. Salvucci, 448 U.S. 83, 91 (1980) ("While property ownership is clearly a factor to be considered in determining whether an individual's Fourth Amendment rights have been violated, . . . property rights are neither the beginning nor the end of this Court's inquiry.").

205. United States v. Haydel, 649 F.2d 1152, 1155 (5th Cir. 1981).

206. 2 WILLIAM BLACKSTONE, COMMENTARIES *8 ("The only question remaining is, how this property became actually vested; or what it is that gave a man an exclusive right to retain in a permanent manner that specific land, which before belonged generally to every body, but particularly to nobody. And, as we before observed that occupancy gave the right to the temporary use of the soil, so it is agreed upon all hands that occupancy gave also the original right to the permanent property in the substance of the earth itself; which excludes every one else but the owner from the use of it.").

207. Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) ("One of the main rights attaching to property is the right to exclude others and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude.") (citing BLACKSTONE, *supra* note 206); Kaiser Aetna v. United States, 444 U.S. 164, 176 (1979) (the right to exclude others is one of the most essential sticks in the bundle of rights that are commonly characterized as property); Rawlings v. Kentucky, 448 U.S. 98, 111–12 (1980) (Blackmun, J., concurring) ("In my view, that 'right to exclude' often may be a principal determinant in the establishment of a legitimate Fourth Amendment interest."); Int'l News Serv. v. Associated Press, 248 U.S. 215, 250 (1918) (Brandeis, J., dissenting) ("An essential element of individual property is the legal right to exclude others from enjoying it. If the property is private, the right of exclusion may be absolute; if the property is affected with a public interest, the right of exclusion is qualified.").

208. Hendler v. United States, 952 F.2d 1364, 1374 (Fed. Cir. 1991) ("In the bundle of rights we call property, one of the most valued is the right to sole and exclusive possession—the right to *exclude* strangers, or for that matter friends, but especially the Government."); United States v. King, 227 F.3d 732, 744 (6th Cir. 2000) ("[C]ourts have considered a number of factors in identifying those expectations which qualify for Fourth Amendment protection . . . includ[ing] whether the defendant has the right to exclude others."); United States v. Perea, 986 F.2d 633, 639–40 (2d Cir. 1993) ("One need not be the owner of the property for his privacy interest to be one that the

Having a possessory interest in property also means having the right to dispose of or destroy that property. In *Buchanan v. Warley*, the Court held that "[p]roperty is more than the mere thing which a person owns. It is elementary that it includes the right to acquire, use, and dispose of it."[209] Similarly, in *United States v. General Motors Corp.*, the Supreme Court described property rights in a physical thing as "the group of rights inhering in the citizen's relation to the physical thing, as the right to possess, use and dispose of it."[210] To "dispose of" can mean "to get rid of by throwing away or giving or selling to someone else," or "to destroy" the item.[211]

Users ordinarily protect their account by using login credentials (i.e., usernames and passwords), two-factor authentication, and other methods to control access to their information. While a service provider may be able to gain access to its users' account, it would be atypical for a service provider to do so without user notice and consent. It follows that users have control over their account and property. Given the routine usage of access controls, account users clearly expect and rely on the ability to exclude others from their accounts.

Finally, users often have the option to delete their account information—whether such information comprises e-mails, photographs, or other content—or their account entirely. Certain service providers differentiate between "deactivating" and "deleting" an account. For instance, Facebook states that if a user "deactivates" her account, she will be able to reactivate it whenever she desires and that "some information may remain visible to other[users]."[212] In contrast, if a user "deletes" her account, the user cannot regain access. The user's information will not be accessible while the account's deletion is pending and copies of some

---

Fourth Amendment protects, so long as he has the right to exclude others from dealing with the property."); United States v. Haydel, 649 F.2d 1152, 1154–55 (5th Cir. 1981) (reasoning that courts consider "whether the defendant has a possessory interest in the thing seized . . . [and] whether he has the right to exclude others from that place"); Presley v. City of Charlottesville, 464 F.3d 480, 492 n.2 (4th Cir. 2006) (Traxler, J., concurring in part, dissenting in part) ("A Fourth Amendment seizure occurs whenever 'there is some meaningful interference with an individual's possessory interests in that property.' . . . In this case, the City significantly interfered with perhaps the most important aspect of real property ownership—the right to exclude others from one's property.") (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)); United States v. Caymen, 404 F.3d 1196, 1201 (9th Cir. 2005) ("An essential element of individual property is the legal right to exclude others from enjoying it . . . .") (quoting Int'l News Serv. v. Associated Press, 248 U.S. 215, 250 (1918) (Brandeish, J., dissenting)).

209. Buchanan v. Warley, 245 U.S. 60, 74 (1917).

210. United States v. Gen. Motors Corp., 323 U.S. 373, 378 (1945).

211. *Dispose* (*dispose of*), THE NEW OXFORD AM. DICTIONARY (3d ed. 2010). As relating to real property, the term can refer to transferring or selling the property.

212. *Deactivating or Deleting Your Account*, FACEBOOK, https://www.facebook.com/help/125338004213029 [https://perma.cc/C5MH-TLG8].

material—which will be disassociated from personal identifiers—may remain in Facebook's database.[213] Considering this distinction between "deactivation" and "deletion," a reasonable user may believe that she has destroyed her account entirely, along with the information the account contains, by "deleting" her account. If this user's account information is preserved pursuant to a § 2703(f) request before the account is fully deleted, her possessory interest in that account has been interfered with.

Because users exert control over their accounts, and such control entails excluding others from access to the account and its information or destroying their information or accounts in their entirety, users have a possessory interest in their digital accounts.

c. *Preserving Account Information Meaningfully Interferes with the Users' Possessory Interest*

When the government compels a service provider to preserve the "records and other evidence in its possession," the government is interfering with the user's possessory interest in her account since the user is no longer capable of excluding others from her account, deleting her account or the information within it, or exercising general control over her account.

A meaningful interference can occur when the character or nature of the property is fundamentally altered. Property owners are typically authorized to exclude others from their property. Therefore, a meaningful interference with an owner's possessory interest occurs when her right to exclude others is infringed on. In his dissenting opinion in *United States v. Karo*, Justice Stevens, joined by Justice Brennan and Justice Marshall (concurring in part and dissenting in part), declared that the owner of property has a right to exclude others—including the government—from it, along with a right to use it exclusively for his own purposes.[214] Investigators in *Karo* installed an electronic tracking device inside a container without a warrant.[215] While the majority held that the installation of the tracking device did not amount to a meaningful interference with the defendant's interest in their possession, Justice Stevens argued that "the attachment of the beeper . . . constituted a 'seizure.'"[216] By attaching a tracking device to an individual's property, the government had converted the property to its own use and infringed on that exclusionary

213. *Id.*

214. United States v. Karo, 468 U.S. 705, 729 (1984) (Stevens, J., concurring in part and dissenting in part).

215. *Id.* at 708 (majority opinion).

216. *Id.* at 729 (Stevens, J., concurring in part and dissenting in part).

right.[217] In other words, when the government attached an electronic bug to the property, it profoundly altered the character of the property, which resulted in a meaningful interference with the property owner's possessory interest. Whether the property owner becomes aware or not is irrelevant as such knowledge is not required to constitute a meaningful interference.

Account information is comprised of intangible data—ones and zeros. This data can be stored, transferred, or destroyed. When a service provider preserves account information pursuant to a § 2703(f) letter, the account user is usually not notified. Rather, the service provider simply creates a new copy of the information contained in the account and stores the new copy separate from the original. As argued above,[218] account information constitutes property despite its intangible nature. Because a user is customarily not notified when a service provider preserves her account information pursuant to a § 2703(f) request, the user has not consented to the copying of her property nor has she consented to the transfer of her property.[219] Most users are apt to believe that they are capable of destroying their account information should they choose to and are likely unaware that a copy of their information has been created and exists independent of their control. While a user can still delete the original copy of her property, she is unable to destroy the new duplicate of her account information, which remains her property. This is a meaningful interference with the property of the user because the character of the property, after a new copy is created, is profoundly different. Users believe they are not only capable of excluding others from their data but that if they were to delete their account information, their data will be destroyed. By mandating a copy, the government, through its agents, has infringed upon the users' right to exclude others and destroy their own property. Because the government has directed a procedure that deprives a user of control over her data, it has meaningfully interfered with that user's possessory interest in her property.

217. *Id.*

218. *See* discussion *supra* Section III.B.5.a.

219. Some may argue that the law enforcement provision in Terms of Service (TOS) inform users that service providers will comply with valid law enforcement requests and that, by agreeing to the TOS, the user has consented. However, as argued previously, users often do not read the TOS and their agreement to use the service is not always equated with consent to its terms.

d. Service Providers Become Government Agents When Preserving Account Information Pursuant to a Preservation Request

The Supreme Court has held that the Fourth Amendment proscribes only government action.[220] It does not apply to a search or seizure, even an arbitrary one, if performed by a private entity.[221] The Fourth Amendment prohibits unreasonable searches and seizures "if the private party acted as an instrument or agent of the Government."[222] When the government compels a service provider to copy account information pursuant to a § 2703(f) letter, it is directing the private entity, thereby making the service provider an agent of the government.

To determine if a private party is an instrument of the government, courts examine two factors: (1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the private party intended to assist law enforcement efforts or to further its own ends through its actions.[223] Both prongs must be satisfied in order for private conduct to become a government action.[224] When the government compels a service provider to preserve account information pursuant to a § 2703(f) request, the government clearly instigates the preservation and knows and acquiesces to the conduct—i.e., the copying of the records and other evidence in the service provider's possession. Moreover, the performing party, the service provider in this scenario, copies account information pursuant to the government's demand to assist law enforcement and not for its own purposes. Since both prongs are satisfied, the private search becomes a government search, and service providers serve as government agents.

---

220. United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("This Court has also consistently construed this protection [of the Fourth Amendment] as proscribing only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'" (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting))).

221. Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614 (1989).

222. *Id.*

223. United States v. Soderstrand, 412 F.3d 1146, 1153 (10th Cir. 2005); United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982); United States v. Simpson, 904 F.2d 607, 610 (11th Cir. 1990) (citing *Miller*, 688 F.2d at 657); United States v. Paige, 136 F.3d 1012, 1017–18 (5th Cir. 1998); United States v. Jarrett, 338 F.3d 339, 344 (4th Cir. 2003); United States v. Feffer, 831 F.2d 734, 737 (7th Cir. 1987); United States v. Malbrough, 922 F.2d 458, 462 (8th Cir. 1990); United States v. Hardin, 539 F.3d 404, 418 (6th Cir. 2008); *see also* United States v. D'Andrea, 648 F.3d 1, 10 (1st Cir. 2011) (stating that relevant factors in "distinguishing private and government action for Fourth Amendment purposes [include]: 'the extent of the government's role in instigating or participating in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests'" (quoting United States v. Pervaz, 118 F.3d 1, 6 (1st Cir. 1997))).

224. United States v. Souza, 223 F.3d 1197, 1201 (10th Cir. 2000).

e. *Preservation of Account Information Violates the Fourth Amendment*

When the government requires a service provider to preserve records and other evidence in a user's account, the ensuing copying of the account information without a warrant, subpoena, or (d) order is tantamount to an unreasonable seizure that violates the Fourth Amendment.

A seizure involves some meaningful interference by the government, or its agent(s), with an individual's possessory interest in her property. Because service providers involved in preserving account information pursuant to "f" letters are acting at the behest of the government to further a law enforcement objective, they are agents of the government. The law enforcement objective in issuing a § 2703(f) letter is to preserve records and other evidence in a user's account pending legal process. To comply with this demand, a service provider must make an exact copy of all the information contained in a user's account in the service provider's possession. The "records and other evidence" preserved comprise of data created by the user. Although intangible, this data nonetheless constitutes digital assets or property and falls within the meaning of "effects" as described and protected by the Fourth Amendment.

Because account information is property, users have certain rights related to such digital assets. These rights include the right to exert control over this property, which includes the ability to exclude others from accessing the data, as well as transfer or destroy the data. It is nearly universally mandatory to protect user accounts with login credentials. The purpose of such access controls is to exclude others from accessing the account information. When a user protects her account with access controls, she is exhibiting a desire to exclude others from her property. Further, users often believe they can dispose of their data at will. In fact, certain platforms' ephemeral services are precisely the reason users utilize such service.

For instance, Snapchat, Wickr, or Confide are services that provide self-destructing messages. These platforms advertise that they enable users to share content that will be automatically destroyed within a particular time after the content is received. When a service provider copies all account information pursuant to a preservation request, that provider—acting as an instrument of the government—is profoundly changing the nature of the property. In other words, the user believes that her digital assets will be destroyed either within a set time limit or when she chooses to dispose of the data. Yet, even if the original data is deleted, a copy of the digital assets will continue to exist, thereby fundamentally altering the transient nature of the property. Because a user is no longer able to delete her messages and an exact copy of the data remains for the

government to use, the government has meaningfully interfered with the user's possessory interest in her property.

The warrantless seizure of account information pursuant to a § 2703(f) letter is unreasonable. The government may seize property without a search warrant under certain circumstances. If the government has probable cause to seize property, a case-specific exigency that requires immediate police action exists, the seizure is temporary and proportional to the nature of the exigency, and the government makes reasonable efforts to obtain a warrant, then a warrantless seizure may be deemed reasonable.[225] As argued above, the government often lacks probable cause when submitting preservation requests and merely hopes that the preserved accounts contain potentially incriminating evidence. Further, the data shows that the government often does not obtain legal process and return to the service provider for the preserved information. This not only demonstrates that a case-specific exigency does not exist but also that the government often fails to make reasonable efforts to obtain a warrant. The government's seizure of all information relating to the account, and any associated accounts, is likely overbroad and not proportional. Finally, when account information is preserved, it is often not temporary. In some cases, the government has copied and preserved account information for nine months without obtaining a warrant.[226]

Proponents of the existing process for preservation of account information may argue that the government is simply copying the information pending valid legal process and that neither the government nor the service provider search the account until a warrant has been issued. Alternatively, the government may argue that it did not take possession of the account.[227] This argument lacks merit because the Supreme Court has found that the Fourth Amendment "protects two types of expectations, one involving 'searches,' the other 'seizures.'"[228] Accordingly, even when the account information is preserved but not reviewed or searched, it nonetheless constitutes a seizure within the meaning of the Fourth Amendment.[229] Therefore, the preservation of account information by a service provider pursuant to a § 2703(f) request is a meaningful

225. United States Court of Appeals for the Ninth Circuit, *18-30121 USA v. Kaleb Basey*, YOUTUBE (Aug. 5, 2019), https://www.youtube.com/watch?v=q1UE8H52rTs [https://perma.cc/RM98-Y52D].

226. ACLU Brief, *supra* note 85, at 1.

227. *Id.* at 20.

228. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

229. In *Soldal v. Cook County*, the Supreme Court rejected the argument that because the government had not searched a mobile home after it seized and carried the mobile home away, it had not violated the Fourth Amendment. *See* ACLU Brief, *supra* note 85, at 21.

interference with the possessory interest of the account user, constitutes a seizure, and violates the Fourth Amendment.

IV. REMEDY AND CONCLUSION

Part III's discussion highlights both the value of preservation letters as an investigative tool and the legitimate concerns of privacy advocates when law enforcement relies on § 2703(f) to preserve both the non-content and content information of a user's account.

A potential remedy that can balance the needs of the government and privacy interests of individuals is to establish a process that enables investigators to preserve account information while requiring the government to meet a higher threshold when seeking the disclosure of the preserved information. As the process for preservation requests currently functions, the government requests that a service provider preserve all account information for ninety or one hundred eighty days. The government can then spend the ensuing ninety or one hundred eighty days investigating further, finding a justification for the initial preservation, and obtaining a warrant at the conclusion of this preservation period to gain access to the content and non-content information.

The new process should mandate that investigators be aware of facts establishing probable cause, or a lower threshold like a (d) order, at the time the preservation request was made. Essentially, while investigators can request the preservation of account information, they may not compel the disclosure of the preserved data without proving to the court that the government was aware of the facts establishing the basis for the legal process they were seeking at the time investigators submitted the preservation request. In other words, if the government requests the preservation of evidence and submits a warrant to require the disclosure of content and non-content information ninety days later, the government must prove to the court that at the time it submitted the "f" letter it had a reasonable basis to suspect that an account user had or was committing a crime or that evidence of a crime was present in the account to be seized. Similarly, if investigators seek the disclosure of information pursuant to a (d) order, they must prove to the court that, at the time the preservation was made, the government had specific and articulable facts showing there were reasonable grounds to believe that the information to be compelled was relevant and material to an ongoing criminal investigation.

This higher threshold makes a preservation request what it should be: a mechanism to prevent evidence from being destroyed—evidence that investigators can obtain but for the administrative delay of getting legal process. Such a remedy would satisfy investigative needs while abating the privacy harms suffered by users.