Saint Louis University Law Journal

Volume 65
Number 4 *Tradeoffs: Technology, Privacy, and the Law (Summer 2021)*

Article 3

2021

The Fourth Amendment Limits of Internet Content Preservation

Orin S. Kerr
University of California - Berkeley, orin@berkeley.edu

THE FOURTH AMENDMENT LIMITS OF INTERNET CONTENT PRESERVATION

ORIN S. KERR*

ABSTRACT

Every year, hundreds of thousands of Internet accounts are copied and set aside by Internet providers on behalf of federal and state law enforcement. This process, known as preservation, ordinarily occurs without particularized suspicion. Any government agent can request preservation of any account at any time. Federal law requires the provider to set aside a copy of the account just in case the government later develops probable cause and returns with a warrant needed to compel the account's disclosure. The preservation process is largely secret. With rare exceptions, the account owner will never know the preservation occurred.

This Article argues that the Fourth Amendment imposes significant limits on the preservation of Internet account contents. Preservation triggers a Fourth Amendment seizure because the provider, acting as the government's agent, takes away the account holder's control of the account. To be constitutionally reasonable, the initial act of preservation must ordinarily be justified by probable cause—and at the very least, in uncommon cases, by reasonable suspicion. The government can continue to use the Internet preservation statute in a limited way, such as to freeze an account while investigators draft a proper warrant application. But the current practice, in which investigators order the preservation of accounts with no particularized suspicion, violates the Fourth Amendment.

* Professor, University of California, Berkeley Law School. A version of this article was delivered as the annual Richard J. Childress Memorial Lecture at the St. Louis University Law School on October 2, 2020. Thanks to Michael Levy, Chad Flanders, Bennett Capers, and Neil Richards for comments on that lecture, and Tiffany Light and the editors at St. Louis University Law Journal for excellent editing. Special thanks to the individuals interviewed "on background" for Section II of this Article.

INTRODUCTION

Imagine you are an FBI agent. One day you receive an anonymous tip that a particular person has committed a crime. You go online and search for the person's name, and your search reveals that, like most American adults, the person has a Facebook account. At this point, you only have an unverified tip. You lack reasonable suspicion, much less probable cause, to believe a crime was committed. And you have no particular reason to think the Facebook account was involved. But imagine federal law gave you the power to preserve and set aside the suspect's entire Facebook account now—including every private message and every saved photo—just in case you later had the probable cause needed to access it.

Let me explain how this hypothetical law would work. At any time, you could command any Internet provider to save all of the contents of any account for up to 180 days. In response to your command, the provider would copy the entire account and set aside the copy for you without notifying the account holder. You would be unable to see the contents of the account unless you eventually develop probable cause and obtain a warrant. But you would have 180 days to develop probable cause. If no probable cause emerged, the preservation would end, and the provider would delete the saved copy without notifying the suspect. And if you developed probable cause during the 180-day period, you could get a warrant and compel the provider to hand over the contents of the account that had been previously preserved.

This hypothetical law would have obvious appeal for government investigators. A lot can happen in 180 days. The suspect might delete incriminating files. The suspect might get wise to the investigation and delete his online accounts to prevent the government from accessing them. By saving accounts at the beginning of a case, investigators could ensure that every record in existence at the outset is available if probable cause later develops. And it would all happen behind the scenes, as the provider would not disclose the preservation to the account holder. Even if the government eventually obtained a warrant and filed criminal charges, the preservation would not be disclosed during routine discovery. The entire process would remain secret.

As you might have guessed, this scenario is not just hypothetical. It describes a federal law, 18 U.S.C. § 2703(f), as it is interpreted and used today. The law states that Internet providers, "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" about an Internet account.[1] The provider must then preserve the records for 90 days,

1. 18 U.S.C. § 2703(f)(1).

extended to 180 days if the government renews its request.[2] Since its enactment in 1996, this authority has been routinely used by investigators to preserve online contents such as e-mails, private messages, and stored photos.

Preservation under § 2703(f) occurs on an extraordinary scale but remains almost completely unknown to the public. In recent years, the transparency reports published by major Internet providers have begun to regularly include preservation request information that helps reveal the scale.[3] The reports show that, in 2019, over 310,000 Internet accounts were preserved in response to § 2703(f) requests.[4] That is roughly one preserved account for every 820 adults in the United States in just one year.[5] A single company, Facebook, is responsible for the lion's share of preserved accounts: in 2019, Facebook preserved over 222,000 accounts in response to § 2703(f) requests.[6] That is about one preserved Facebook account for every 1,120 adults in the United States.[7] The scale of preservation is massive.

And it is happening largely in secret. Although transparency reports can now reveal raw numbers for those who know where to look, the law and practice of preservation has long flown under the radar. Little is publicly known about how law enforcement uses § 2703(f) or how providers comply with it. Providers do not notify users if their accounts were preserved, and prosecutors normally do not disclose the fact of preservation to defense counsel.[8]

Judges have not focused on the statute, either. A query in Westlaw's ALLCASES database reveals only a few dozen judicial opinions since 1996 that have even referenced the provision.[9] Within those opinions, the substantive comments consist of a single paragraph in one unpublished district court case, a brief denial of a pro se motion under 28 U.S.C. § 2255, and one or two sentences

2. *See* 18 U.S.C. § 2703(f)(2) ("Records referred to in paragraph (1) shall 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.").

3. *See* Liz Woolery, Ryan Boodish, & Kevin Bankston, *The Transparency Reporting Toolkit* 16 (Dec. 2016), https://na-production.s3.amazonaws.com/documents/Transparency_Reporting_Guide_and_Template-Final.pdf [https://perma.cc/65XE-YXVN] (noting in 2016 that "only a couple of companies currently report on preservation requests," and "encourag[ing] additional companies to begin keeping track of the number of preservation requests and consider adding it to future transparency reports."). By 2020, most but not all major providers include preservation request numbers in their transparency reports. *See infra* Table 1.

4. *See infra* Table 1.

5. *Id.* According to the United States Census Bureau, there were about 328 million people in the United States in 2019, and about 77.8% of those people were adults. *See Quick Facts*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/US/PST045219 [https://perma.cc/WTV9-PQ8Z].

6. *See infra* Table 1.

7. *Id.*

8. *See infra* Section II.

9. This is based on a Westlaw query in the ALLCASES database, conducted on April 19, 2021, searching for opinions that included the text "2703(f)."

of dicta in two opinions by federal magistrate judges.[10] Hundreds of thousands of accounts are preserved every year, but how the regime of preservation works—and whether it is constitutional—has largely escaped scrutiny.

This Article has two goals. The first goal is to reveal for the first time how preservation under § 2703(f) actually works. As part of my research for this article, I interviewed lawyers who have extensive and diverse experience with practices under § 2703(f). These interviews were conducted "on background," with one exception,[11] which means I can report the substance of what I was told but cannot identify the sources or use direct quotes. This is non-traditional for a law review article. It means, among other things, that I will make a lot of factual assertions with no footnotes.[12] However, the candor enabled by this arrangement allows me to present what I believe is an accurate picture, not previously available to the public, of how Internet content preservation works today.

My interviews reveal that preservation under § 2703(f) occurs on a wide scale with little scrutiny because law enforcement and providers consider it a privacy non-event. For law enforcement, broad preservation requests can be made whenever a suspect is identified just in case probable cause later emerges.[13] More often than not, no warrant will follow. Only about half of preservation requests lead to any legal process, and a smaller subset of cases lead to the search warrants needed to compel preserved contents.[14] For providers, preservation is rote and often automated. Providers use snapshot tools that copy entire accounts and set them aside. If the government returns with a warrant, providers take on the sometimes-complex task of assembling the warrant production from two different copies of the account—the preserved copy, and the copy that exists when the warrant is served.[15] Notice is normally not provided, either to users when no litigation has occurred or to defendants if charges are filed, mostly because preservation itself is not considered significant.[16]

The second goal of this article is to articulate the Fourth Amendment limits of Internet content preservation. In my view, existing practices must be sharply curtailed. When the government requests preservation and the provider

10. The single paragraph is United States v. Rosenow, No. 17CR3430 WQH, 2018 WL 6064949, at *10 (S.D. Cal. Nov. 2018) (discussed *infra* note 28). The pro se motion under 28 U.S.C. § 2255 is United States v. Basey, No. 4:14-CR-00028-RRB, 2021 WL 1396274, at *7 (D. Alaska Apr. 13, 2021). The dicta appears in opinions by former Magistrate Judges Orenstein and Smith that are discussed *infra* note 61.

11. The exception was Michael L. Levy, formerly the Chief for Computer Crimes in the U.S. Attorney's Office for the Eastern District of Pennsylvania. I thank Mr. Levy for his interview and feedback.

12. The horror.

13. *See infra* Section II.

14. *See id.*

15. *Id.*

16. *Id.*

complies, the provider acts as the government's agent and becomes a state actor.[17] The process of copying and setting aside the contents of an Internet account is a Fourth Amendment seizure because it interferes with a user's right to control his private communications.[18] For Internet content preservation to be a reasonable seizure, it must be justified at the outset by at least reasonable suspicion—and in most cases, preservation will require probable cause.[19] When probable cause exists, preservation allows the government considerable time to prepare and submit a proper warrant application. But preservation without cause, based only on the hope of developing probable cause someday, is not permitted.

Broadly speaking, this article calls for a shift in how law enforcement, providers, and courts envision content preservation under § 2703(f). Since its enactment, the statute has been understood as allowing a windfall for the government. Whenever the government has wanted an account preserved, it has had the unilateral power and complete discretion to order it preserved. This article hopes to bring Internet content preservation into the traditional framework of Fourth Amendment protection. It presents Internet content preservation as similar in principle from traditional kinds of temporary seizures pending further investigation involving postal mail, packages, and physical computers. Similar constitutional limits established for temporary physical seizures of physical property should apply to Internet content preservation. Section 2703(f) should continue to play an important role in the Stored Communications Act ("SCA"). But the era of unlimited preservation, just in case probable cause might emerge, must end.

With apologies for being autobiographical, I want to add a few words about my history with the topic of this article. I first encountered the § 2703(f) authority when I was a lawyer at the Justice Department from 1998 to 2001. At the time, and for several years later, I saw no reason to question the common assumption that Internet content preservation does not trigger Fourth Amendment limits. That changed for me around 2010, when I wrote *Fourth Amendment Seizures of Computer Data*.[20] An implication of that article, drawn explicitly in it, was that preservation was a government seizure.[21] This led me to think that the Fourth Amendment likely imposed unappreciated restrictions on the § 2703(f) authority. When I would occasionally lecture to defense counsel groups about Internet surveillance, I urged them to make Fourth Amendment

17. *See infra* Section III.

18. *See id.*

19. *See infra* Section IV.

20. Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700 (2010).

21. *See id.* at 723–24 (arguing that "a government request to an ISP to make a copy of a suspect's remotely stored files and to hold it while the government obtains a warrant" is a seizure).

challenges to preservation along those lines. In 2016, I published a blog post tentatively articulating the basic principles I offer in this article.[22]

My understanding is that these arguments helped inspire a very small number of challenges to § 2703(f). The most notable challenge, *United States v. Basey*,[23] was fully briefed in the Ninth Circuit with amicus participation by the ACLU.[24] *Basey* was argued in the Ninth Circuit in August 2019.[25] The Ninth Circuit did not reach the merits in *Basey,* however, because the preservation arguments had not been raised in a timely way before the district court.[26] A second Ninth Circuit challenge was similarly resolved without a merits ruling.[27] Even today, the only Fourth Amendment challenge to § 2703(f) that has been adjudicated on the merits is one unpublished district court case about cell-site location records that rejected the claim in a single cryptic paragraph.[28] That case is currently on appeal to the Ninth Circuit, although it is unclear how directly the preservation issue figures into the appeal.[29]

22. *See* Orin S. Kerr, *The Fourth Amendment and Email Preservation Letters*, WASH. POST (Oct. 28, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/10/28/the-fourth-amendment-and-email-preservation-letters/ [https://perma.cc/8CCG-WL2B] (arguing that "the use of preservation letters for contents raises really serious constitutional concerns").

23. 784 F. App'x. 497, 500 n.1 (9th Cir. 2019).

24. Brief for American Civil Liberties Union & American Civil Liberties Union of Alaska Foundation as Amici Curiae Supporting Defendant-Appellant, United States v. Basey, 784 F. App'x 497 (9th Cir. 2019) (No. 18-30121), 2019 WL 829338 [hereinafter ACLU Basey Brief].

25. The oral argument video in *Basey* is available at https://www.youtube.com/watch?v=q1UE8H52rTs [https://perma.cc/B658-YVCD].

26. *See Basey*, 784 F. App'x. at 499 (concluding that the district court had not reached the merits of a § 2703(f) challenge proposed in the district court because it had not been timely filed, and that the district court had not abused its discretion in denying the proposed motion).

27. *See* United States v. Perez, 798 F. App'x. 124, 126 (9th Cir. 2020) (declining to address how the Fourth Amendment applies to § 2703(f) because it was not clear error for the district court to have found that the evidence compelled was from the warrant copy and not the preservation copy).

28. *See* United States v. Rosenow, No. 17CR3430 WQH, 2018 WL 6064949, at *10 (S.D. Cal. Nov. 2018). In *Rosenow*, the defendant argued to the district court that preserving his Yahoo and Facebook accounts violated the Fourth Amendment. *Id.* The court disagreed, stating that "the preservation requests in this case did not amount to an intrusion subject to Fourth Amendment requirements." *Id*. Part of the court's explanation suggests that the preservation was not a seizure at all. *See id.* ("The preservation requests in this case did not interfere with the Defendant's use of his accounts . . ."). Part of the court's explanation suggests that if it was a seizure, it was a reasonable seizure. *Id.* ("The statutory authorization to preserve a wire or electronic communications account held by a third-party online provider recognizes that the information is easily and readily destroyed and allows its preservation for a short period in order to allow law enforcement to seek further legal process.").

29. *See* Brief of Defendant-Appellant at 32–33, United States v. Rosenow, No. 20-50052 (9th Cir. June 29, 2020). The appellant's brief was filed June 29th, 2020, and the government's answering brief was filed November 11, 2020. *Id.*; Brief of Plaintiff-Appellee, United States v. Rosenow, No. 20-50052 (9th Cir. Nov. 11, 2020). A review of the briefs suggests that the preservation issues are not a substantial part of the appeal. The Fourth Amendment limits on

I include this background to alert readers that the subject of this article has been simmering for a while. Appellate briefs have been written, even though they have not yet led to judicial precedents.[30] I have returned to the issue out of hope that more detailed and certain treatment might push challenges along. Ideally, a better understanding of how Internet content preservation works might help trigger more litigation and oversight. A detailed constitutional analysis, made outside the pressures of litigation but with the benefit of past briefing, can work through my own views and perhaps inform future consideration of the question. And understanding how preservation practices are now hidden, and how lawyers can bring them to light, might help offer a roadmap for litigating challenges.

This article has five Sections. Section I explores the text of the Internet preservation statute, 18 U.S.C. § 2703(f). Section II explains how preservation works based on the "on background" interviews I conducted. Section III explains why Internet preservation triggers a Fourth Amendment seizure. Section IV argues that Internet preservation normally requires probable cause, and at the very least, reasonable suspicion. Section V offers a broader reflection of the proper role of § 2703(f), as well as thoughts on how defense counsel might challenge preservation and how the exclusionary rule might apply.

I. THE STATUTORY TEXT

This Section explains the statutory basis of Internet content preservation. It starts with the text, found in 18 U.S.C. § 2703(f) of the SCA, and the recognized purpose it serves. It then explores three textual ambiguities: when the government can make a preservation request, what remedies exist for violations, and what records the statute covers.

preservation are raised, but the appellant makes the argument only in a single paragraph. *See* Brief of Defendant-Appellant, *supra*, at 32–32. The government's response is also short. *See* Brief of Plaintiff-Appellee, *supra*, at 50–51.

30. The constitutional debate over 18 U.S.C. § 2703(f) has also led recently to what I believe is the first published law review article on the topic. Armin Tadayon, *Preservation Requests and the Fourth Amendment*, 44 SEATTLE L. REV. 105 (2020). Tadayon's article presents an overview of the two sides of the policy and constitutional debate over preservation requests. *See id*. at 121–48. In the article's conclusion, Tadayon proposes (as matter of policy rather than the Fourth Amendment, if I read it correctly) that preservation requests should require at their initiation the same level of cause that the Stored Communications Act requires to disclose those particular records. *See id.* at 148.

A. The Text and Purpose

The preservation authority of 18 U.S.C. § 2703(f) was added to the SCA in 1996.[31] The text, which has not changed since the statute was enacted, reads as follows:

> (f) Requirement To Preserve Evidence.
>
> *(1) In general.—*
>
> A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
>
> *(2) Period of retention.—*
>
> Records referred to in paragraph (1) shall 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.

Section 2703(f) deals with the problem of deleted information.[32] It provides a way to temporarily freeze records so they can be obtained later in preserved form with legal process. The Justice Department's 2009 manual on searching and seizing computers explains the rationale of § 2703(f) as follows:

> In general, no law regulates how long network service providers must retain account records in the United States. Some providers retain records for months, others for hours, and others not at all. As a result, some evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. For example, suppose that 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. To minimize the risk that evidence will be lost, the SCA permits the government to direct providers to "freeze" stored records and communications pursuant to 18 U.S.C. § 2703(f).[33]

31. *See* Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104–132, § 804, 10 Stat. 1214, 1305 (1996).

32. *Cf.* In re Search of Yahoo, Inc., No. 07–3194–MB, 2007 WL 1539971 at *1 n.3 (D. Ariz. May 21, 2007) ("To minimize the risk that electronic information will be lost, Title 18 U.S.C. § 2703(f) permits the Government to direct network service providers to preserve records pending the issuance of compulsory legal process.").

33. U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 139 (2009), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [https://perma.cc/3CSV-S93S] [hereinafter 2009 DOJ Manual]. By way of full disclosure, I authored the original 2001 edition of the manual, which includes a similar discussion. *See* U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 138 (2001) [hereinafter 2001 DOJ Manual].

The preservation authority might be implicated by three different kinds of deletions. First, a provider might have a policy of deleting non-content records, such as login records or past assigned IP addresses, in the ordinary course of business after a certain period of time. Preservation may be useful to ensure the records that the company would otherwise delete are still available. Second, a user might decide to delete specific records, and especially specific contents of his communications, such as e-mails, instant messages, or posts. Preservation might save a copy of the messages before the user deletes them, either as a matter of routine or because he realizes he is under investigation and wants to destroy evidence. Finally, either the user or the provider might decide to delete an account altogether. Preservation may allow the government to obtain evidence from an account that otherwise would no longer exist by the time the government served legal process.

Two aspects of § 2703(f) are particularly notable. The first is its broad scope. A preservation request can be made by any "governmental entity," defined by the statute as "a department or agency of the United States or any State or political subdivision thereof."[34] The requestor does not need to be a law enforcement agency. Any department or agency of any federal, state or local government will do. The preservation authority also applies to investigations of any crime at all, or even outside any investigation.[35] And the statute imposes its mandate on any "provider of wire or electronic communication services or a remote computing service."[36] Translating the technical terms of the SCA into English, that means roughly that any company that provides messaging or storage services must comply with a preservation request.[37] On its face, then, the statute is drafted remarkably broadly: it allows any government agency to compel any Internet provider.[38]

34. 18 U.S.C. § 2711(4) (defining "governmental entity").

35. This broad scope contrasts with a second Internet content preservation authority in federal law, 18 U.S.C. § 2258A(h). That section applies when a provider has come across images of child pornography and sends the required report about the discovered images to the National Center for Missing and Exploited Children (NCMEC) pursuant to 18 U.S.C. § 2258A(a). Under § 2258A(h), the sending of the report "shall be treated as a request to preserve the contents provided in the report for 90 days after the submission" to NCMEC. *Id.* at § 2258A(h)(1). The provider can delete the account after discovering child pornography in it, but the provider must first preserve the contents relevant to its report to ensure it is available for later investigation or prosecution. *Id.* at § 2258A(h)(3).

36. 18 U.S.C. § 2703(f)(1).

37. *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, 1213–18 (2004) (explaining the meaning of "remote computing service" and "electronic communication service" in the Stored Communications Act).

38. The Council of Europe's 2001 Convention on Cybercrime, of which the United States became a signatory in 2006, emphasized the importance of provisions such as § 2703(f) by requiring every signatory nation to have a law to "order or similarly obtain the expeditious

The second notable aspect of § 2703(f) is its brevity. The entire provision, including its title, uses only eighty-five words.[39] Brevity is a virtue, but § 2703(f) leaves a lot uncertain. The remainder of this Section focuses on three statutory ambiguities that result in significant part from this sparse text. The first question is when the government can make a request; the second is the remedy for violations; and the third is what kind of records the statute covers. It is important to understand these areas of uncertainty before considering how the Fourth Amendment might apply to preservation under the statute.

B. When Can the Government Make a Request?

The first uncertainty in § 2703(f) is when the government can make a preservation request. The statute is silent on this. As drafted, the text only regulates providers. When the government makes a request, the language states, the provider "shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."[40] Providers have to comply when a request is made. But when can a request be made?

I think there are three ways to interpret the statute's silence about when requests can be made. First, the statutory silence might reflect an implicit congressional judgment that government use of § 2703(f) should be unlimited by law. That is, perhaps § 2703(f) only regulates provider responses to requests because requests can be made at the government's sole discretion. This is the prevailing view today among government officials and service providers, as the discussion in Section II explains.[41]

There are two other possible interpretations, however. Perhaps the limitation that preservation should occur "pending the issuance of a court order or other process" is designed to limit government requests to cases when legal process is already forthcoming.[42] Under this view, perhaps preservation requests can be

preservation of specified computer data for a period of time as long as necessary, up to a maximum of ninety days," subject subsequent renewal, "to enable the competent authorities to seek its disclosure." Council of Eur., Convention on Cybercrime 8 (2001), https://rm.coe.int/1680081561 [https://perma.cc/JK3P-QTHG]. I believe that the similarity between the 1996 text of § 2703(f) and the 2001 Council of Europe language is no accident: the then-recent United States statute inspired the later Convention provision. *Cf.* Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. ONLINE 58, 62–63 (2017) (noting that DOJ "played a leading role in the Council of Europe Convention on Cybercrime").

39. Canada's equivalent statutory provisions have over 600 words. The preservation demand statute is 353 words long, *see* Canada Criminal Code, R.S.C. 1985 c C-46 § 487.012; and the companion preservation order statute is 269 words, *see* Canada Criminal Code, R.S.C., 1985 c C-46 § 487.013.

40. 18 U.S.C. § 2703(f)(1).

41. This is the government's view, as Section II explains.

42. 18 U.S.C. § 2703(f)(1).

made only when the government is actively seeking the court order or other process required by law to disclose the materials preserved.

Finally, perhaps the lack of text on when requests can be made means that § 2703(f) only dictates the provider response to a request but it does not try to regulate when the government can make requests.[43] On this view, perhaps some other area of law, such as the Fourth Amendment, might independently limit when preservation requests are made.

C. What Are the Remedies for Violations?

Another important question left open by § 2703(f) is the remedy for violations. "[U]pon the request of a governmental entity," the statute provides, the provider "shall take all necessary steps" to preserve.[44] But what if the provider refuses? It's not clear whether the government can compel a reluctant provider into complying, and if so, what source of law authorizes the compulsion. Section 2703(f) issues the command but says nothing about how to enforce it. The statute is simply silent on the remedy.

Neither of the existing remedies provisions of the SCA seems to cover this. One provision, § 2712, authorizes civil damages against the United States for willful violations.[45] This Section is plainly not implicated by a government claim that the provider acted wrongly.

The second provision, § 2707, provides a wide range of remedies for civil claims against entities other than the United States that can be brought by "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter."[46] A governmental entity is clearly not a provider or subscriber. Nor would a government appear to be a "person aggrieved by any violation of this chapter," as the SCA incorporates the Wiretap Act's definition[47] of "aggrieved person" as "a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed."[48]

43. I return to this question in Section V Part B(1), where the answer may relate to the scope of the exclusionary rule.

44. 18 U.S.C. § 2703(f).

45. Section 2712(a) states in relevant part:

> Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages.

46. 18 U.S.C. § 2707(a).

47. *See* 18 U.S.C. § 2711(1) ("the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section").

48. 18 U.S.C. § 2510(11). I use the cautionary word "appears" because I suppose there is a theoretical argument that a "person aggrieved" in § 2707 is different from an "aggrieved person" defined in § 2510(11). It seems more likely that they are the same, however, with the phrase "person aggrieved" used in § 2707 instead of the defined term "aggrieved person" to avoid the awkward

Given that the SCA expressly rejects other remedies for non-constitutional violations of the statute,[49] it is not clear what, if any, remedy exists for a provider's refusal to comply with a preservation request. The most plausible way to test whether a remedy exists for § 2703(f) refusals would be for a government to bring a legal action in court seeking to compel preservation from a noncooperating provider. A court would then consider what powers the court has to enforce the government's request. But how this might work, and on what basis the court might enter the order, is not answered by the statutory text. And the issue appears never to have been litigated, primarily because major Internet providers uniformly consider compliance with § 2703(f) requests to be a routine part of the regime of lawful access under the SCA.[50]

D. What Records Can Be Preserved?

The third and final textual uncertainty in § 2703(f) is what records the law covers. According to the statute, a notified provider must respond to a request by preserving "records and other evidence in its possession."[51] The phrase "records and other evidence in its possession" is not defined in the statute, and a Westlaw search though the USCA database suggests it is unique in the United States Code to § 2703(f). The phrase is particularly puzzling because other parts of § 2703 already break down the world of user records into two categories: "contents,"[52] on one hand, and "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)," on the other.[53] The precise line between these two categories can be murky, but the basic distinction between them has received considerable attention.[54]

phrasing that could otherwise be caused by the subsequent specification in § 2707 of what "aggrieved" the "person," namely, a violation of the SCA. The language here admittedly is not ideal, as the definition of "aggrieved person" in § 2510(11) is drafted in a way specific to the Wiretap Act and does not translate perfectly to the SCA. But the legislative history of § 2510(11) suggests that Congress was trying to define "aggrieved person" to reflect Fourth Amendment law on who has standing to challenge a search or seizure*, see* S. REP. NO. 90-1097, at 114 (1968), and perhaps that same notion applies to "person aggrieved" in § 2707.

49. *See* 18 U.S.C. § 2708 ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.").

50. Notably, providers cannot ordinarily be held liable for complying with § 2703(f) requests because of the good-faith exception of § 2703(e) and § 2707(e). *See* 18 U.S.C. § 2707(e) ("A good faith reliance on . . . a request of a governmental entity under section 2703(f) of this title . . . is a complete defense to any civil or criminal action brought under this chapter or any other law").

51. 18 U.S.C. § 2703(f)(1).

52. 18 U.S.C. § 2510(8) ("contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication); 18 U.S.C. § 2703(a)-(b).

53. 18 U.S.C. § 2703(c).

54. *See, e.g.*, WAYNE R. LAFAVE, ET AL., CRIMINAL PROCEDURE § 4.8 (6th Ed. 2017).

Congress's use of the phrase "records and other evidence in its possession" in § 2703(f) prompts the question of whether § 2703(f) requires preservation only of non-content records or whether it also extends to contents of communications.[55] Law enforcement and major providers have assumed, since its enactment, that § 2703(f) covers contents as well as non-content records. The sample § 2703(f) letter that was included in the 2001 Justice Department manual offered language that included requests for "[a]ll stored electronic communications" for the account preserved.[56] The 2009 edition of the manual made the coverage of contents more explicit, as it asks for "contents of any communication or file stored by or for the Account and any associated accounts."[57] The longstanding practice is for preservation requests to ordinarily include contents of the preserved account. Some judges have assumed this is correct, although without analysis of the point.[58]

This is important for two reasons. First, the contents of e-mails and other Internet messages are presumptively protected by the Fourth Amendment, while most non-content records are not.[59] Second, extending § 2703(f) to the contents of communications implies a slightly different role for preservation. Non-content records typically are controlled by the provider, but contents are controlled by users. If § 2703(f) is limited to non-content records, the statute merely helps prevent data from being lost due to decisions by providers to delete records in the ordinary course of business. If § 2703(f) covers the contents of communications, however, the preservation authority becomes a means of ensuring government access to messages that users themselves might otherwise opt to destroy.

55. 18 U.S.C. § 2703(f).

56. 2001 DOJ Manual, *supra* note 33, at 214. The term "electronic communications" is defined in 18 U.S.C. § 2510(12) to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."

57. 2009 DOJ Manual, *supra* note 33, at 225.

58. *E.g.*, in United States v. Dougherty, Crim. No. 19-64-JLS, 2020 WL 3574467 (E.D. Pa. July 1, 2020), the defendant sought a *Franks* hearing based on an agent's claim in a warrant affidavit that AT&T did not retain the defendant's text messages. This was a false statement, the defendant claimed, because the government could have sent AT&T a preservation request and later obtained the messages with a warrant. *See id.* Although the court rejected the request for a *Franks* hearing, its ruling did not take issue with the assumption behind the claim that preservation could have extended to the contents of messages. *See id.* at *5.

59. The contents of e-mails and other messages have been held to be protected; non-content records, with the exception of at least some kinds of cell-site location information, are unprotected. *See* LAFAVE, *supra* note 54, at § 4.4 (summarizing current caselaw on applying the Fourth Amendment to the Internet).

II. INSIDE THE WORLD OF § 2703(F) PRESERVATION

This Section explains how § 2703(f) is used by law enforcement and providers today. The discussion is based primarily on interviews I conducted in October and November 2020 with lawyers who have recent experience with the statute. I conduct the interviews "on background," with one exception, enabling me to share what the lawyers said without disclosing their identifies or quoting them. By interviewing a range of subjects with different experiences, and, where helpful, connecting those interviews to the public transparency reports published by major providers, I was able to piece together how § 2703(f) is being implemented.

This Section presents the fruits of those interviews. It begins with an overview of how both law enforcement and providers perceive the preservation process. It then turns to the nuts and bolts of how preservation requests are made and how providers respond to those requests. It next discusses whether law enforcement follows up with preservation requests and how providers respond if no follow up occurs. It then addresses how providers comply with warrants for previously preserved accounts. It concludes by explaining the lack of notice to users.

A. A Widespread Practice That Has Escaped Scrutiny

Both law enforcement and providers consider preservation under § 2703(f) to be ubiquitous and unobjectionable. Although providers preserve hundreds of thousands of accounts every year,[60] the shared thinking is that this widespread practice does not raise privacy concerns. Governments and providers alike consider preservation merely an anticipatory step separate from disclosure. Because the government needs a warrant to compel *disclosure* of contents, the mere *preservation* of contents is a non-event.

Those in law enforcement believe that there are few limits on the use of § 2703(f). In their view, the statute gives the government discretion about when to preserve account contents and how many accounts can be preserved. Preservation letters are typically submitted early in an investigation just in case probable cause eventually emerges. It is common for law enforcement to issue preservation requests when a suspect has a known e-mail or social media account. The primary recognized limit on § 2703(f) is that the authority only extends to previously made records. As the Department of Justice ("DOJ") manual states, "§ 2703(f) letters should not be used prospectively to order providers to preserve records not yet created."[61]

60. *See infra* Table 1, which provides published preservation numbers for the year 2019.

61. *See* 2009 DOJ Manual, supra note 33, at 140. I agree that § 2703(f) has this limit, as the statute by its terms requires a provider to "take all necessary steps to *preserve* records and other evidence *in its possession*." 18 U.S.C. § 2703(f)(1) (emphasis added). To "preserve" is to maintain the status quo, and a communication not yet created cannot already be "in" a provider's possession.

Providers have a similar view of preservation requests. Preservation is considered a rote process that receives little attention. Providers understand that law enforcement will seek preservation in a very large number of cases, and it is uncommon for requests to receive scrutiny. The basic perception is that preservation is "no harm, no foul," and that it raises no special privacy concerns. When the government follows up a preservation request with legal process, which occurs about half the time, the legal process (rather than the preservation) becomes the focal point. When the government fails to follow up with legal process, on the other hand, the preserved records are simply deleted and forgotten.

The scale of preservation that occurs is quite remarkable. Major Internet providers publish bi-annual transparency reports about law enforcement requests for customer data.[62] Although not every provider includes details about the preservation process in their reports,[63] the major providers have reported the following numbers of preservation requests and preserved accounts by federal, state, or local governments for 2019:[64]

In my view, this precludes applying § 2703(f) prospectively. Some courts have not found this limit obvious, however. Notably, the Sixth Circuit has expressed uncertainty about the point. *See* United States v. Warshak, 631 F.3d 266, 290 n.21 (6th Cir. 2010) ("Some courts and commentators have suggested that § 2703(f) applies only retroactively . . . However, the language of the statute, on its face, does not compel this reading.") (internal citations omitted). Two somewhat adventurous federal magistrate judges have suggested in dicta that § 2703(f) might apply prospectively to require the saving of records that can later be compelled with a single court order. *See* In re Application, 396 F. Supp. 2d 294, 313 (E.D.N.Y. 2005) (Orenstein, M.J.); In re Order, 31 F. Supp. 3d 889, 895 (S.D. Tex. 2014) (Smith, M.J.).

62. *See generally* Isedua Oribhabor & Peter Micek, *The What, Why, and Who of Transparency Reporting*, ACCESS NOW (Apr. 2, 2020, 3:02 PM), https://www.accessnow.org/the-what-why-and-who-of-transparency-reporting/ [https://perma.cc/VBH2-SJY3] (summarizing the history and purpose of transparency reports). Access Now maintains a useful page that provides links to current transparency reports. *See Transparency Reporting Index*, ACCESS NOW, https://www.accessnow.org/transparency-reporting-index/ [https://perma.cc/FMB6-DFRB].

63. Microsoft is an example of a provider that does not include preservation numbers in its transparency report. *See Microsoft Law Enforcement Requests Report*, MICROSOFT, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report [https://perma.cc/SED4-KW78].

64. I obtained the numbers in the chart below by accessing the privacy reports and combining the January to June 2019 numbers with the July to December 2019 numbers. I selected the year 2019 because it was the most recent calendar year for which the reports were available. I excluded requests from foreign governments.

TABLE 1: PRESERVATION IN 2019 IN RESPONSE TO § 2703(F) REQUESTS

Provider	*Number of Requests*	*Accounts Preserved*
Facebook[65]	131,600	222,800
Google[66]	23,210	57,509
Verizon[67]	7,196	17,445
Apple[68]	4,998	9,319
Twitter[69]	2,255	4,068
Dropbox[70]	695 (2nd half only)	800 (2nd half only)

These numbers show that Facebook receives by far the highest number of preservation requests. Facebook preserves about four times as many accounts as Google, which reports the second-highest number of preservation requests. In 2019 alone, over 222,000 Facebook accounts were preserved—a rate of about one account for every 1,120 adults in the United States.[71]

Facebook dominates the preservation request numbers for several reasons. First, surveys suggest that about seventy percent of American adults in 2019 were Facebook users.[72] Second, Facebook's rule that users must register in their

65. *Transparency: United States*, FACEBOOK, https://transparency.facebook.com/government-data-requests/country/US [https://perma.cc/FP6W-GJKU.

66. *Transparency Report: Global Requests for User Information*, GOOGLE, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US&legal_process_breakdown=expanded:0,1&lu=legal_process_breakdown [https://perma.cc/T343-TJH3].

67. *Government Data Requests*, VERIZON, https://www.verizonmedia.com/transparency/reports/government-data-requests.html [https://perma.cc/QYH5-WCMQ]. Verizon's page notes:

> The chart below shows the number of preservation requests we received within this reporting period, as well as the number of accounts specified in those requests. If information we preserved is subsequently sought by the government agency with legal process, the request (and our response) will be reflected as Government Data Request in the reporting period during which the request was made.

68. *Apple Transparency Report: Government and Private Party Requests*, APPLE 9 (Jan.–June 2019), https://www.apple.com/legal/transparency/pdf/requests-2019-H1-en.pdf [https://perma.cc/ZVL5-PN9D]; *Apple Transparency Report: Government and Private Party Requests*, APPLE 9 (July–Dec. 2019), https://www.apple.com/legal/transparency/pdf/requests-2019-H2-en.pdf [https://perma.cc/V9U2-7PDX].

69. *Information Requests*, TWITTER, https://transparency.twitter.com/en/reports/information-requests.html#2019-jul-dec [https://perma.cc/NL9L-N72K].

70. *Transparency at Dropbox: Reports*, DROPBOX, https://www.dropbox.com/transparency/reports [https://perma.cc/6UJK-6HF7] (tab at "Request Type;" then "Preservations;" data only available for second half of 2019).

71. U.S. CENSUS BUREAU, *supra* note 5. That amounts to over 255 million adults.

72. *See* Andrew Perrin & Monica Anderson, *Share of U.S. Adults Using Social Media, Including Facebook, Is Mostly Unchanged Since 2018*, PEW RESEARCH CENTER (Apr. 10, 2019),

own name makes it unusually easy to identify if a person has an account and which account belongs to them.[73] Third, Facebook offers a range of tools to locate other users, including by their names.[74] This means that investigators often can quickly check if a suspect has a Facebook account and, if so, can send a preservation request to preserve that account.

Table 1 also indicates that preservation requests often cover multiple accounts. The ratios vary from provider to provider, but a two-to-one ratio between preserved accounts and requests seems common. This likely reflects a range of practices, with many preservation requests covering just one account and others seeking the preservation of many accounts at once.

B. How Government Agents Make Preservation Requests

The major Internet providers have web portals that enable government agents to submit law enforcement requests and court orders, including preservation requests.[75] Several portals have public-facing pages,[76] although a government e-mail address is needed to set up an account.[77]

The process of making a preservation request is simple. Once logged in to an account through the portal, the government agent can simply click on the appropriate boxes and enter the account name and request preservation.[78] The statute does not require a formal request in a letter on government letterhead,

https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/ [https://perma.cc/Z9QA-VTBD] ("Roughly seven-in-ten adults (69%) say they ever use the platform").

73. *See Terms of Service*, FACEBOOK § 3, https://www.facebook.com/terms.php [https://perma.cc/7CZK-D262] ("[Y]ou must . . . [u]se the same name that you use in everyday life.") A person might nonetheless provide a false name, of course, but the norm on Facebook is to provide a real one.

74. *See generally* Tim Fisher, *6 Best Ways to Use Facebook to Find People Online*, LIFEWIRE (Apr. 16, 2020), https://www.lifewire.com/ways-you-can-use-facebook-to-find-people-online-3482276 [https://perma.cc/NU8H-J8GV].

75. *See, e.g.*, Joe Rossignol, *Apple to Launch a Global Law Enforcement Web Portal to Streamline Data Requests by End of 2018,* MACRUMORS (Sept. 6, 2018), https://www.macrumors.com/2018/09/06/apple-to-launch-law-enforcement-support-program/ [https://perma.cc/V678-LKVU].

76. *Law Enforcement Online Requests*, FACEBOOK, https://www.facebook.com/records/login/ [https://perma.cc/EYL5-GV58]; *Law Enforcement Request System*, GOOGLE, https://lers.google.com/signup_v2/landing [https://perma.cc/MKW2-K7ZT].

77. *See, e.g.*, *Law Enforcement Request System: Request Access to LERS*, GOOGLE, https://lers.google.com/signup_v2/requestaccount [https://perma.cc/2FGU-2JCZ] ("To request a LERS account, enter your official government-issued email address below.").

78. *See* Det. James Williams, *The Unofficial Guide to Facebook's Law Enforcement Portal Version 2*, SACRAMENTO SHERIFF'S DEP'T, https://netzpolitik.org/wp-upload/2016/08/facebook-law-enforcement-portal-inofficial-manual.pdf [https://perma.cc/587J-XDD2].

although some provider privacy policies may require that.[79] It is common, especially on the federal level, for law enforcement to roughly follow the model preservation request letter provided in the Justice Department's search and seizure manual.[80] Justice Department prosecutors also have access to a standard form Microsoft Word template that will fill in the appropriate addresses of providers to help complete the letter.[81]

One noteworthy aspect of preservation is the lack of attention to particularity. A preservation request will often ask the provider to preserve everything about the account. It will seek the preservation of every record, every file, and every message associated with the account that the provider can access from the moment of the account's creation until the time of preservation. This is notably different from the scope of a warrant that can be obtained. Warrants must comply with the Fourth Amendment's particularity requirement, which requires probable cause for the items to be disclosed and typically date restrictions for Internet accounts.[82] Consistent with the view that preservation is not a significant privacy event, it is generally understood that preservation need not comply with the particularity requirement. It is therefore common for the government to preserve very broadly.

C. Following Up on Preservation Requests

After the government has sought preservation, and requested any extensions, agents will either come back eventually with legal process or else not follow up and let the preservation lapse. According to the interviews I conducted, these alternative paths happen roughly equally often. That is, a ballpark estimate is that the government follows up on preservation requests with some kind of legal process—whether with a warrant for contents, or less process for non-content records—only about half the time.

79. The privacy polices do not have the force of law, of course, but investigators will nonetheless comply with them in order to secure preservation. *See, e.g.*, *Safety Center: Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines/ [https://perma.cc/G6ST-KKXJ].

80. *See* 2009 DOJ Manual, *supra* note 33, at 225. *See* Telephone Interview with Michael Levy, former Chief for Computer Crimes in the U.S. Attorney's Office for the Eastern District of Pennsylvania (Summer 2020).

81. *See* Telephone Interview with Michael Levy, former Chief for Computer Crimes in the U.S. Attorney's Office for the Eastern District of Pennsylvania (Summer 2020).

82. *See, e.g.*, Info. Associated with Four Redacted Gmail Accounts, 371 F. Supp. 3d 843, 844 (D. Or. 2018) (holding warrants for online account held overbroad under the Fourth Amendment "in light of Google's ability to date-restrict the emails it discloses to the government."); In re Search of Google Email Accounts, 92 F. Supp. 3d 944, 953 (D. Alaska 2015) (denying a warrant application for a Gmail account as overbroad because it was "not tailored to its narrow probable cause showing for the limited time periods"). *Cf.* People v. Coke, 461 P.3d 508, 516 (Colo. 2020) (finding a warrant for a cell phone violated the particularity requirement because it was not limited to "the alleged victim or to the time period during which the assault allegedly occurred.").

When the government decides that it need not or cannot follow up with legal process, the government does not provide notice to providers to stop preserving the account. For example, if investigators conclude that a suspect is completely innocent, they do not contact the provider and ask it to delete the preserved contents. The government's understanding is that no follow-up is needed to cancel preservation: when the ninety-day period ends, providers will eventually delete the files on their own.

When the government follows up with legal process, that process can take the form of a subpoena, a § 2703(d) court order, or a probable cause warrant.[83] The major Internet providers require a search warrant to turn over contents of communications under Fourth Amendment caselaw.[84] As noted earlier, the warrant generally will be narrower than the prior preservation request. The warrant must comply with the particularity clause of the Fourth Amendment and its evolving standards on remote content accounts, while the preservation is not understood to be subject to those standards.

It is common for warrant materials that follow preservation orders to make reference to the preservation order, either in the warrant itself or in a cover letter or other comment. Investigators include this reference to help providers comply with warrants. As explained below, executing the warrant may require providers to either disclose both the preserved contents and the current contents, or else to patch together material from both.[85] Alerting the provider to the prior preservation in the warrant can help the provider do that effectively.

D. How Providers Comply with Preservation Requests

Providers execute preservation requests by making a copy of the full contents of the relevant account and storing it separately. Several providers have described the process in their public transparency reports. Apple's transparency report refers to preservation as "a one-time data pull of the requested existing user data available at the time of the request" that is then held "for 90 days (up to 180 days if Apple receives a renewal request)."[86] Twitter's report refers to preservation as "a temporary snapshot of the relevant account records" that is then held "for 90 days pending service of valid legal process."[87]

83. *See generally* Kerr, *supra* note 37.

84. *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (holding that accessing the contents of e-mails from an Internet service provider requires a warrant under the Fourth Amendment).

85. See *infra* Section II Part E..

86. *Apple Transparency Report: Government and Private Party Requests*, APPLE 9 (July–Dec. 2019), https://www.apple.com/legal/transparency/pdf/requests-2019-H2-en.pdf [https://perma.cc/KT6Q-PPWD].

87. *Guidelines for Law Enforcement*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support#6 [https://perma.cc/L3CG-WE9A].

Providers typically implement preservation using a software program referred to as a "snapshot tool" that copies all of the files and then stores them elsewhere for later retrieval. At several major providers, preservation is automatic. The government agent's request to preserve is carried out by the software without human intervention. No person reviews the request before it is implemented. Other major providers retain human review of preservation requests, requiring a person to review the request and implement it: given the time-sensitive nature of preservation requests, the human review generally is given high priority. Human review remains the norm at smaller providers, which generally lack the large number of requests that would justify creating the programs to make preservation automatic.

Major providers that automate the preservation processes retain occasional human review of preservation requests in case abuses or irregularities occur. For example, a preservation request that seeks preservation of a very large number of accounts at once may be flagged for review and prompt an inquiry from the provider seeking a justification. Requests to preserve accounts of public figures may also prompt review. A request made based on an assigned IP address instead of an account name may need special review to associate the request with the correct account. Providers also often watch for preservation requests made seriatim, such as requests every hour to preserve the same account. The concern motivating this review is that the § 2703(f) authority is supposed to permit only a one-time snapshot, rather than ongoing monitoring.[88] Repeated preservation could in theory amount to a wiretap, which would implicate the civil and criminal liability of the Wiretap Act.[89] Providers use human review to watch out for that or other law enforcement strategies that could exceed the permitted scope of § 2703(f).[90]

Providers that have automated the process typically set the preserved material to delete automatically when the preservation period ends.[91] This was not the case in the past, however, before the process was widely automated. It was not uncommon for providers to hold on to preserved contents beyond the required period: they might set the files aside and simply forget to come back to

88. *Cf.* 2009 DOJ Manual, supra note 33, at 139.

89. *See id.* at 140 ("§ 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the electronic surveillance statutes discussed in Chapter 4 [on the Wiretap Act]").

90. Apple's published law enforcement guidelines hint at this role: "An attempt to serve more than two preservation requests for the same account will result in the second request being treated as a request for an extension of the original preservation, and not a separate preservation of new data." *Legal Process Guidelines*, APPLE, https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/X5DS-B3K5].

91. If a renewal request is made, it must be made in time for the provider to process it before the initial 90-day period elapses and the contents are deleted. *See, e.g.*, *Apple Transparency Report: Government and Private Party Requests*, *supra* note 85, at 9.

delete them. This could result in preservation beyond the statutory window, such as the ninth-month preservation period in *United States v. Basey* involving preservation that occurred in 2014.[92]

Providers also occasionally extend preservation beyond the statutory requirement as a courtesy to governments. Twitter's transparency report identifies a representative circumstance when this can occur. Although the statute only requires preservation for two ninety-day periods, the report explains that Twitter "may process multiple extension requests if requesters represent that they are engaged in a process for international cooperation (i.e., MLAT or letters rogatory), given these processes can take several months."[93] Providers also routinely preserve accounts in response to requests received directly from foreign governments,[94] although it is not required by § 2703(f).[95] Preservation directly from foreign governments raises no Fourth Amendment issues because foreign governments are not state actors for Fourth Amendment purposes.[96] Further, the practical relevance of preservation for foreign governments is somewhat limited in the case of contents because disclosure is ordinarily prohibited unless a domestic warrant has been obtained.[97]

E. The Impact of Preservation on Subsequent Disclosure

After a provider has preserved an account, the government may come back with legal process seeking disclosure. In some cases, the government will seek disclosure only of non-content records such as basic subscriber information or e-mail headers without subject lines. The government can generally obtain non-content records with less process than a search warrant, such as a subpoena or a

92. In *Basey*, the government sent a preservation letter on February 7, 2014, and followed up with a search warrant on November 11, 2014. *See* ACLU Basey Brief *supra* note 24.

93. *Information Requests*, TWITTER, https://transparency.twitter.com/en/reports/information-requests.html#2019-jul-dec [https://perma.cc/F6KD-JJZD].

94. This practice is detailed in transparency reports, which often break down preservation requests by country. *See, e.g.*, *Apple Transparency Report: Government and Private Party Requests*, *supra* note 85, at 22. Preservation requests listed as coming from other countries are generally going to be for preservation requests made under the law of those countries. If a foreign government works with U.S. authorities under an MLAT and the US authority submits a preservation request, that would be listed as a United States preservation. Or it might be both: It is common for requests involving mutual legal assistance to come both from the foreign government and from either the Justice Department's Office of Internal Affairs or the FBI's MLAT unit.

95. A foreign government cannot make a request under § 2703(f) because the statute only applies to requests from governmental entities, which means only federal, state, and local governments. *See* 18 U.S.C. § 2703(f)(1); 18 U.S.C. § 2711(4).

96. *See, e.g.*, United States v. Olaniyi, 796 F. App'x. 601, 603 (11th Cir. 2019).

97. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 409–10 (2014). The new provisions of the Cloud Act likely will change that in coming years, as the Cloud Act will permit disclosure pursuant to foreign warrants of qualifying foreign governments. *See generally* ORIN S. KERR, 2021 CASELAW AND STATUTORY SUPPLEMENT FOR COMPUTER CRIME LAW 102–05 (2020) (explaining the relevant provisions of the Cloud Act).

§ 2703(d) order, as is expressly permitted by the SCA[98] and (with an exception for cell-site location information) by Fourth Amendment law.[99] When the government follows up a preservation request with legal process for unprotected non-content records, the provider may nonetheless retain the preserved account records for the remainder of the ninety-day period in case the government returns with more legal process such as a warrant for contents.

Matters are more complicated when the government follows up a preservation request with the search warrant generally required to compel disclosure of contents under the Fourth Amendment and the SCA.[100] The government generally obtains a two-stage warrant that divides the work of culling the information sought in the warrant between the provider and investigators.[101] At the first stage, the provider will gather the relevant kind of files sought by the warrant, subject to the date restrictions typically found in the warrant, and will produce that set of files to the government.[102] At the second stage, government investigators will search through those produced files and separate out the contents relevant to the crime as specifically described in the warrant. [103]

Preservation can play an important role in production under this two-stage approach because the combination of preservation under § 2703(f) and subsequent search warrant compelling disclosure under § 2703(a) results in the provider possessing two copies of the account contents. The first copy is made at the time of the preservation request in response to that request. We can call this the *preservation copy*. The second copy is made when the provider receives a warrant. At that stage, the provider will make a second copy of the account and prepare that for winnowing and disclosure. We can call this the *warrant copy*.

The existence of two copies of the account complicates how providers help execute Internet search warrants because the contents to be turned over in response to the warrant may be spread between the two copies. Each copy may have responsive contents that the other copy lacks. The preservation copy may have files that the user deleted by the time of the warrant copy. The warrant copy may have files made after the creation of the preservation copy. In addition, the two copies will often have different scope because the government typically will preserve broadly but obtain warrants more narrowly. While initial preservation

98. *See* 18 U.S.C. § 2703(c).

99. *See* LAFAVE, *supra* note 54, at § 4.4 (summarizing Fourth Amendment caselaw as applied to the Internet).

100. *See generally* 18 U.S.C. § 2703(a); United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).

101. This procedure has been widely approved in the caselaw. *See, e.g.*, In the Matter of Search of Information Associated with [redacted]@mac.com, 13 F. Supp. 3d 157, 162, 164 (D.D.C. 2014).

102. *See id.* at 160–62 (describing the two-step procedure).

103. *See id.*

will typically cover the entire account, a subsequent warrant is likely to be significantly narrower to satisfy the Fourth Amendment's particularity requirement.

A hypothetical example can show how preservation often complicates the provider's task of complying with Internet content warrants. Imagine investigators send a request in June that seeks preservation of an entire account— all contents and all non-content records— up to that date. In response, the provider generates and stores the preservation copy. Over the next few months, the government investigates the crime and develops probable cause. In September, the government obtains a warrant and serves it on the provider. The warrant is narrower than the preservation request. It requires the provider to turn over only the contents of private messages from the account during the window of probable cause—say, from January through August. The provider will respond to the warrant by creating the warrant copy, which consists only of private messages from January through August that existed in the account when the warrant was received in September.

The provider can produce these contents in compliance with the warrant in two ways. The easier path is for the provider to send the government two productions. The provider will produce the warrant copy, as filtered down to satisfy the date restriction and file types sought; and it will also produce the preservation copy, as filtered down by the same conditions. In my example, the warrant copy will contain the private messages from January through August that existed in the account in September when the warrant was served. The preservation copy will have the private messages from January through June that existed in June when the account was preserved. The provider will send the government both productions, which are likely to overlap significantly. The government can them look through either or both copies for the evidence as it executes stage two of the warrant.

The more difficult way for the provider to execute stage one of the warrant is to do the extra work of going through the two copies and patching them together into a single production. In that case, the provider will start by filtering down both the preservation copy and the warrant copy to the correct date windows and file types, compare the resulting data sets, remove duplicates, and combine them. The result is a curated and combined data set that is sent on to the government as "the account" in compliance with its duty to execute stage one of the warrant.

F. Lack of Notice to Users

A final point to consider in the § 2703(f) process is the lack of notice to users. The entire process is largely hidden from users and their counsel. Providers do not notify users about preservation. And when the government obtains a warrant and later brings charges, it ordinarily does not notify users that a preservation previously occurred. Preservation is hidden not because it is

considered controversial. To the contrary, it is hidden primarily because it is not considered significant enough to disclose.

The provider's practice not to notify users about preservation reflects a policy choice. The SCA authorizes the government to obtain court orders in some circumstances that prohibit providers from notifying anyone that "a warrant, subpoena, or court order" was obtained.[104] But the statute does not apply to preservation requests, as they are not warrants, subpoenas, or court orders. The Justice Department's sample preservation letter includes language asking the provider not to provide notice of the preservation, but that request has no legal force.[105] Whether providers disclose preservation, and at what stage, is entirely up to them.

Providers do not notify users of preservation for two reasons. The most important reason is that they do not consider preservation to be a privacy event. If the government preserves an account but never follows up with a warrant, the thinking runs, the extra copy of the account will be deleted eventually. In the end, the preservation will have had zero consequence. On the other hand, if the government follows up with a warrant that compels disclosure, users normally will be notified of the disclosure pursuant to the providers' privacy policies assuming no non-disclosure order has been obtained. Either way, providers reason, the prior preservation is not significant enough to justify notifying the user.

A second reason providers do not notify users is the perceived administrative burden of notification. If providers notify users of preservation, they might deem it proper to provide notice in some cases but not in other cases. But when a provider decides that a particular preservation justified notice, it would, as a courtesy to the government, defer to the government's preference between having preservation with notice or no preservation at all.[106] This could

104. 18 U.S.C. § 2705(b). The statute states in relevant part:

> A governmental entity acting under section 2703 . . . may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.

Id. This provision is the subject of considerable First Amendment litigation. *See, e.g.*, LAFAVE, *supra* note 54, at § 4.8 (summarizing litigation).

105. The sample language in the 2009 DOJ Manual 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 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.

2009 DOJ Manual, *supra* note 33, at 225.

106. The Justice Department's sample language for a preservation request reflects this concern: "If compliance with this request might result in a permanent or temporary termination of service to

be resource-intensive, as both sides would need to sort out their notice preferences in each case. Providers can simply bypass this time-consuming process by not notifying users about preservation.

A second stage of notice issues arises if criminal charges are eventually brought and the evidence against the defendant includes preserved content that was later disclosed pursuant to a warrant. At that stage, the question is whether the government will notify the defense of the earlier preservation. The ordinary practice is for the government not to provide such notice. Prosecutors have discovery obligations, of course. In some jurisdictions, those obligations will require disclosing information relevant to the filing of a Fourth Amendment motion to suppress—an obligation that might variously be based on *Brady v. Maryland*,[107] local rules,[108] agency standards,[109] the Fourth Amendment itself,[110] or other sources.[111] Despite this obligation, prosecutors ordinarily do not notify defense counsel of prior preservation based on the belief that preservation does not raise any Fourth Amendment issues.[112] Because the § 2703(f) process is thought to operate outside the Fourth Amendment, prosecutors do not think to include notice of preservation in discovery.

The primary exception to this non-disclosure practice is the acknowledgment of preservation through reference in search warrants turned over to the defense. Warrants to compel contents under 18 U.S.C. § 2703(a) may

---

the Account, or 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." *Id.*

107. 373 U.S. 83, 87 (1963). There is some authority that "the suppression of material information can violate due process under *Brady* if it affects the success of a defendant's pretrial suppression motion." Biles v. United States, 101 A.3d 1012, 1020 (D.C. 2014). The matter is not firmly established, however. *Compare id.* at 1029–31 (Thompson, J., concurring) (arguing that *Brady* only covers evidence that is exculpatory or impeaching, and that it does not include material that is relevant to a motion to suppress).

108. *See, e.g.*, D. Mass., L.R. 116.2(a) (June 1, 2018) (defining exculpatory information that must be disclosed by the government to include "information that tends to . . . cast doubt on the admissibility of evidence that the government anticipates offering in its case-in-chief.").

109. U.S. DEP'T OF JUST., *The Justice Manual* § 9–5.001.C.2 (requiring disclosure of information that "might have a significant bearing on the admissibility of prosecution evidence").

110. *See* Orin Kerr, *Did the Ninth Circuit Create a New Fourth Amendment Notice Requirement for Surveillance Practices?*, LAWFARE (Sept. 9, 2020, 7:01 AM), https://www.lawfareblog.com/did-ninth-circuit-create-new-fourth-amendment-notice-requirement-surveillance-practices [https://perma.cc/RQS3-ZURC] (discussing the constitutional notice requirements apparently introduced by United States v. Moalin, 973 F.3d 977 (9th Cir. 2020)).

111. *See, e.g.*, STANDARDS FOR CRIM. JUST. DISCOVERY § 11-2.1(c) (AM. BAR ASS'N 2020) ("[T]he prosecutor should disclose to the defense . . . [a]ny information, documents, or other materials relating to any governmental electronic surveillance of the defendant's person, communications, possessions, activities, or premises, or to legal authorization of the surveillance, that pertains to the case."). Notably, there is no requirement of notice that the warrant was obtained if charges are not brought. *See id.*

112. *See* Telephone Interview with Michael Levy, former Chief for Computer Crimes in the U.S. Attorney's Office for the Eastern District of Pennsylvania (Summer 2020).

mention the fact of prior preservation to help the provider comply fully with the warrant. When the government discloses the warrant materials to defense counsel as part of its discovery obligations, alert defense counsel might notice a reference to prior preservation. But this requires careful scrutiny by the defense and awareness of the workings of § 2703(f). The fact of preservation is otherwise generally hidden from defendants.

III. CONTENT PRESERVATION IS A FOURTH AMENDMENT SEIZURE

Having studied the preservation statute and explored current practices, we turn finally to Fourth Amendment law. This Section considers the threshold Fourth Amendment question: does content preservation under § 2703(f) cause a Fourth Amendment seizure? This Section argues that it does. When a provider preserves contents pursuant to a government request, the provider's act of copying and saving the contents of the account is a Fourth Amendment seizure. That seizure must then be analyzed for its constitutional reasonableness, which is the subject of Section IV.

This Section has three Parts. It starts by explaining why provider preservation in response to a preservation request is government action that the Fourth Amendment regulates. The provider acts as the government's agent in response to government compulsion, making its acts attributable to the government. The analysis then explains why that government action amounts to a seizure under the Fourth Amendment. Preservation interferes with the account holder's possessory interest by transferring control of personal communications to the government.

Finally, this Section responds to the core argument of those who see no Fourth Amendment concerns with preservation, namely, the "no harm, no foul" claim. According to this view, Fourth Amendment law need not consider preservation because it is merely anticipatory. Preservation, it is argued, has no effects of its own. But that argument is flawed. Preservation surrenders a person's control over their most private communication. That is a classic Fourth Amendment harm at the core of the constitutional limit on government seizures.

An important limitation is worth flagging here. My argument is limited to the preservation of stored contents, such as e-mails, instant messages, pictures, attachments, and other remotely stored files. It does not apply to non-content records, such as login records or basic subscriber information. I draw this distinction because users generally have Fourth Amendment rights in their stored contents but generally have no Fourth Amendment rights in their non-content records.[113] The known category of non-content records that crosses this line, cell-site location records, presents its own issues that may require its own

113. *See* LAFAVE, *supra* note 54, at § 4.4.

preservation analysis.[114] The analysis here concerns preservation only of contents.

A. Content Preservation is Government Action

The first step in my argument is establishing that content preservation under § 2703(f) is government action regulated by the Fourth Amendment and not private action outside it. This is straightforward. Content preservation is government action because it occurs in response to a government command.

Let's go back to first principles. The Fourth Amendment applies to acts of private individuals acting as "instrument[s] or agent[s]" of the Government.[115] "Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities."[116] The easiest case for agency is when the government has "compelled a private party to perform a search."[117] But compulsion isn't required.[118] The main question is, was the private party acting "on his own initiative," or was the private party acting pursuant to the "encouragement, endorsement, and participation" of the government?[119]

Content preservation in response to a § 2703(f) letter readily satisfies the Fourth Amendment test for state action. When the government makes a § 2703(f) request, the government is directly compelling the private party to act. "[U]pon the request of a governmental entity," the law states, the provider "*shall take all necessary steps* to preserve records and other evidence" in its possession.[120] The records "*shall 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."[121] The government directs, and the law requires the provider to act as the government's agent.

Commonwealth v. Gumkowski shows how provider preservation under this scheme counts as state action.[122] In *Gumkowski*, the service provider Sprint was approached by a state trooper who requested emergency assistance in a murder

114. A wrinkle with applying these principles to cell-site location records is that users generally don't know that the records exist and cannot control them. It is not clear to me how the Fourth Amendment seizure test might apply to copying records that a person cannot control and does not know exists.

115. Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).

116. Skinner v. Railway Labor Executives' Assn., 489 U.S. 602, 613–614 (1989).

117. *Id.* at 614.

118. *See id.* (noting that absence of compulsion "does not, by itself, establish that the search is a private one.").

119. *Id*. at 613–614.

120. 18 U.S.C. § 2703(f) (emphasis added).

121. *Id.* (emphasis added).

122. 167 N.E.3d 803, 812 (Mass. 2021).

investigation.[123] The state trooper asked Sprint to disclose a suspect's cell-site location records without a warrant.[124] The SCA permits a provider to disclose records to the government at its discretion if, "in good faith," it "believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency."[125] Sprint opted to reveal the records under that standard. The Massachusetts Supreme Judicial Court later ruled that Sprint's response to the state trooper's request was Fourth Amendment state action: "if law enforcement instigates the search by contacting the cell phone company to request information, there is State action. That Sprint could have refused to provide records in response to [the state trooper's] request does not change the fact that he instigated the search."[126]

Caselaw from the physical world advances the point. In *United States v. Hardin*, the government asked an apartment building manager to enter a specific apartment in his building to see if the defendant, who had a warrant out for his arrest, was inside.[127] The apartment manager agreed, and he went to that apartment and used his key to enter.[128] After entering the apartment, the manager confirmed the defendant was inside and relayed that information to the police.[129] The Sixth Circuit ruled that the apartment manager was a state actor for Fourth Amendment purposes.[130] "[T]he manager was acting as an agent of the government" under the Fourth Amendment, according to the court, "because the officers urged the apartment manager to investigate and enter the apartment, and the manager, independent of his interaction with the officers, had no reason or duty to enter the apartment."[131]

Under *Gumkowski* and *Hardin*, Internet providers following § 2703(f) will count as state actors. Like Sprint in *Gumkowski*, and the building manager in *Hardin*, an Internet provider that receives a preservation notice is acting to help the government. The government instigates the process, and the provider follows the government's direction. Of course, a provider (or a building manager) can act on its own and remain a private actor.[132] But when the government approaches a provider and asks it to act *for the government*, a complying

123. *See id.* at 808–10.
124. *See id.* at 810 n.6.
125. 18 U.S.C. § 2702(c)(4).
126. *Gumkowski*, 167 N.E.3d at 812.
127. 539 F.3d 404, 407 (6th Cir. 2008).
128. *Id.*
129. *Id.* at 407–08.
130. *Id.* at 420.
131. *Id.*
132. *See, e.g.*, United States v. Adkinson, 916 F.3d 605, 610 (7th Cir. 2019) (per curiam) (holding that T-Mobile was a private actor when it investigated robberies of its own stores, conducted a tower dump of T-Mobile phones in the area to identify a suspect, and then turned the information over to the government).

provider is a state actor. If anything, the case for state action is clearer with preservation because § 2703(f) is mandatory. The provider in *Gumkowski* and the manager in *Hardin* volunteered to follow the government's request. It was their choice. In contrast, § 2703(f) gives providers no choice but to comply. Although the remedy for violations is unclear,[133] the statute is phrased as a direct command: the provider "*shall take all necessary steps* to preserve records and other evidence" for the government.[134]

This conclusion is particularly straightforward when providers automate the preservation process. As previously explained in Section II, some major providers directly automate preservation. To preserve an account, the government accesses the provider's portal and fills out an online form. Submission of the form directly carries out the preservation without human intervention. Although the provider has designed and built the tool, the government uses it. The state action is obvious. The same principle should apply when the provider has not automated the process and requires a person working for the provider to carry out the preservation process. Whether or not the provider has decided to automate, the process is a government-mandated process which constitutes state action under the Fourth Amendment.[135]

The government argued in *Basey* that preservation under § 2703(f) does not trigger government action because preservation merely requires a provider to keep a record it already has in its possession.[136] "[W]hen a party complies with a legal duty to preserve information in its possession," the government reasoned, "it does not become a government agent."[137] The government relied on *California Bankers Ass'n v. Shultz*,[138] a case involving a challenge to regulations requiring banks to maintain certain business records. In response to the claim that the record-keeping made the banks agents of the government, the Court disagreed, stating that "[s]uch recordkeeping requirements are scarcely a novelty."[139] According to the government, the principle of *Shultz* covers preservation.[140]

I disagree for two reasons. First, the government's argument fails to grapple with the reality of the preservation process. As Section II showed, providers do not comply with § 2703(f) requests by simply keeping a record that they already

133. *See* Section I, Part C.

134. 18 U.S.C. § 2703(f)(1) (emphasis added).

135. *Cf.* Smith v. Maryland, 442 U.S. 735, 744–45 (1979) ("We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.").

136. *See* Appellee's Answering Brief, *United States v. Basey*, No.18-30121 (9th Cir. Aug. 14, 2019) [hereinafter DOJ Basey Brief].

137. *Id.* at 20–21.

138. 416 U.S. 21, 25 (1974).

139. *Id.* at 45.

140. *See* DOJ Basey Brief, *supra* note 130, at 20–21.

have. True, the process is labeled "preservation." But what actually happens behind the scenes is a dynamic process of entry, copying, and storage. Providers preserve a user's account by going into the account, using a snapshot program to copy the records, and putting the copy aside for the government.[141] This is closely akin to Sprint's response in *Gumkowski* and the manager's entry in *Hardin*. Indeed, the process closely resembles the process of complying with legal process, except that the very last step of disclosure is missing. Just as a provider is a state actor when it executes a search warrant for Internet contents,[142] so is a provider a state actor when it conducts preservation.

Second, the government's reliance on *Shultz* is misplaced. Nothing in *Shultz* sheds light on whether preservation triggers Fourth Amendment state action. In *Shultz*, banks had argued that their Due Process rights were violated by the "unreasonable burdens" imposed on them by bank recordkeeping requirements about certain suspect kinds of financial transactions.[143] The burdens were unreasonable, the banks argued, "by seeking to make the banks the agents of the Government in surveillance of its citizens."[144] The Court rejected the claim that the regulatory burden was so unreasonable as to violate Due Process by noting that such burdens were common—"scarcely a novelty"[145]—and that recordkeeping requirements were far lesser burdens than other regulatory approaches that were clearly lawful.[146] Nothing in this reasoning or conclusion helps identify who is a Fourth Amendment state actor.

B. Content Preservation Is a Seizure

The next step is establishing that preservation constitutes a Fourth Amendment seizure. As noted earlier, I made this argument in depth in a prior article, *Fourth Amendment Seizures of Computer Data*.[147] I will offer only a brief summary here. In that article, I contended that "copying data 'seizes' it under the Fourth Amendment when copying occurs without human observation and interrupts the course of the data's possession or transmission."[148] I used e-mail preservation under § 2703(f) as an example of a data seizure: "a government request to an ISP to make a copy of a suspect's remotely stored files

141. *See supra* Section II.

142. *See* In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197, 214 (2d Cir. 2016), *vacated as moot*, United States v. Microsoft, 138 S. Ct. 1186 (2018).

143. *Shultz*, 416 U.S. at 45.

144. *Id.*

145. *Id.*

146. *Id.* at 46–47.

147. Kerr, *supra* note 20, at 700.

148. *Id.* at 703.

and to hold it while the government obtains a warrant would also constitute a seizure."[149]

The starting point for this conclusion is *United States v. Jacobsen*, which states that property is seized "when there is some meaningful interference with an individual's possessory interests in that property."[150] Whether copying data is a seizure raises a conceptual puzzle because copying creates additional copies. Does the meaningful interference with the possessory interest occur only when a person loses control of the original? Or does meaningful interference also occur when the person loses control of copies the government has made?[151] Put another way, if the government makes a copy but leaves the suspect with the original, has the data been seized because the government has gained a copy of the information? Or has no seizure occurred because the suspect has not lost access to the original?

The answer to this puzzle should be that copying data for later government use constitutes a seizure. The essence of the seizure power is taking government control.[152] Copying constitutionally protected data achieves that: "In a world of data, whether an individual has access to a particular copy of her data has much less significance than whether the government has obtained a copy of the data for possible government use in the future."[153] Losing access to a particular copy of data can be an inconvenience, to be sure. But what matters in a data environment is whether the government has private data at its disposal. In a digital environment, data "reigns supreme. Government control of data provides the link that empowers the prosecution to charge people with crimes that will take away their freedom."[154] When a government agent collects constitutionally protected data and sets it aside for possible access, the government has seized the data under the Fourth Amendment.

Courts have generally assumed this result to be correct, although express holdings about this issue are rare.[155] The point is perhaps most easily shown by comparison to the warrant process under 18 U.S.C. § 2703(a) for compelling contents held by Internet providers. When the government serves a warrant on a

149. *Id.* at 723–24.

150. 466 U.S. 109, 113 (1984).

151. Kerr, *supra* note 20, at 704–09.

152. *Id.* at 711.

153. *Id.* at 712.

154. *Id.* at 713.

155. Courts have widely assumed this result in the copying of digital media on a suspect's physical device, such as a laptop, cell phone, thumb drive to later search it. The Second Circuit expressly held this in a panel decision that was later vacated on rehearing en banc. *See* United States v. Ganias, 755 F.3d 125, 137 (2d Cir. 2014) (holding that the Government's retention of electronic copies of the defendant's personal computer "deprived him of exclusive control over those files," which was "a meaningful interference with [the defendant's] possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment."), *vacated*, United States v. Ganias, 824 F.3d 199 (2d Cir. 2016) (en banc).

provider that requires disclosure of account contents, courts have generally assumed (and occasionally have expressly held)[156] that the copying of contents that precedes disclosure to the government is a "seizure."[157] The similarity between executing an Internet warrant under § 2703(a) and content preservation under § 2703(f) requires the same result for both. The process is the same except for the last step. When preservation occurs, the information is copied and set aside, just as it would be for a warrant. It is just not (yet) disclosed. If copying contents and setting aside the new copy for the government is a seizure when the government executes a warrant, it is not less a seizure when the government orders preservation.

C. The Problem With "No Harm, No Foul"

The main counterargument to my conclusion that preservation triggers a Fourth Amendment seizure asks if this is simply 'no harm, no foul.' That is, should the law of preservation reflect the principle of *de minimis non curat lex*—that the law does not bother with trifles?[158] After all, preservation of contents is only a preliminary step. The provider holds files securely and does not turn them over unless the government has a warrant. No one other than the provider and the government will know that preservation even occurred. Given that the user retains access to his files, one might ask, what exactly is the harm if the government directs a copy to be made and saved without disclosure?

But there is a harm. It's a harm at the core of the seizure power: Loss of control. Users ordinarily control the contents of their private accounts. They can decide to create private content. They can decide to store it. And just as users are free to decide what ideas they will write, what pictures they will take, and what communications they will save, they are also free to undo those choices by deleting those files in their accounts—or even to delete their accounts altogether. Ordinarily, users can make their online accounts their virtual homes, filled with

156. Search of Info. Assoc. with [Redacted]@Mac.Com, 25 F. Supp. 3d 1, 7 (D.D.C. 2014) (Facciola, MJ) ("Even if, as Professor Orin Kerr has stated, a search does not occur until the data is exposed to possible human observation . . . the seizure of a potentially massive amount of data without probable cause has still occurred—and the end result is that the government has in its possession information to which it has no right.").

157. In speaking of how SCA warrants are obtained, courts have spoken of the process of copying the contents of the account as the part of the warrant that is a seizure. *See, e.g.*, United States v. Bowen. 689 F. Supp. 2d 675, 684 (S.D.N.Y. 2010) ("[T]he Defendants' enterprise was so pervaded with criminal activity, and the target e-mail accounts were such essential instrumentalities of that enterprise, that *seizure* of the entire account was appropriately authorized pursuant to the all records exception.") (emphasis added).

158. It is not clear that this principle applies to Fourth Amendment claims, but this Section assumes that it does for purposes of replying to it. *Compare* Hessel v. O'Hearn, 977 F.2d 299, 299 (7th Cir. 1992) (considering the doctrine of de minimis non curat lex as applied to a Fourth Amendment claim) *with* Arizona v. Hicks, 480 U.S. 321, 321 (1987) ("A search is a search, even if it happens to disclose nothing but the bottom of a turntable.").

as many or as few of their private thoughts, private pictures, and personal videos as they wish. They control the accounts, what is in them, and whether to have them.

Preservation eliminates that control. Users who want to delete a private message will *think* they can delete it. Users who want to delete their entire account will *think* it is gone. But when contents are preserved, users can't do that. The entire world of their private messages will already be secretly saved and set aside for the government at its whim. Preservation makes creation of contents a one-way street. You can decide to create and remotely save your contents, but you can't decide to undo that. What a person chooses to save is no longer under their control. The government can at any time take that control away by issuing a preservation request that freezes the full scope of a person's online life today and sets it aside for possible government access tomorrow.

Reasonable people can disagree about how much harm this triggers. To some, it may be creeping Big Brotherism—a step toward a world where the government can store for later access every electronic thought a person has ever had. To others, it may only be a small afront, as the data still will be disclosed only with a warrant. But whichever side one falls on, the copying counts as some kind of Fourth Amendment seizure. The government takes control of a person's online world that a person wanted to delete, and secretly holds it just in case a reason to access it later emerges. This is a seizure, and the question becomes when that seizure is constitutionally reasonable. The next Section takes on that question.

IV. THE REASONABLENESS OF PRESERVATION SEIZURES

This Section considers when preservation is reasonable under the Fourth Amendment. The Supreme Court has explained that the reasonableness of a warrantless seizure breaks down into two questions. First, was the seizure "justified at its inception"?[159] Second, was it "reasonably related in scope to the circumstances which justified the interference in the first place"?[160] Applying this framework to preservation focuses the analysis on two questions. First, how much cause is needed to initiate preservation? And second, how long can preservation go on?

The Section offers the following answers. First, a preservation request ordinarily will require at least reasonable suspicion—and in most cases probable cause—at the outset. This conclusion follows from the large body of caselaw about temporary seizures of physical items such as computers, packages, and mail. Reasonable suspicion is generally sufficient for a brief investigatory hold of property, normally on the order of minutes or hours, to investigate criminal

159. Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 185 (2004) (quoting United States v. Sharpe, 470 U. S. 675, 682 (1985)).

160. *Id.*

activity. Probable cause is generally required for a longer detention, on the order of days, allowing the officers time to obtain a search warrant authorizing the property to be searched. These principles should also apply to digital seizures of stored Internet contents.

Second, how long preservation can last depends on whether the basis of the preservation is reasonable suspicion or probable cause. Preservation based on reasonable suspicion will be rare and must be very brief, making it far less consequential in practice than preservation based on probable cause. When the initial preservation is justified by probable cause, it can extend for a considerable period of time—on the order of several weeks, and perhaps months—before a warrant is obtained.

This Section proceeds in six Parts. First, it explains how preservation fits within existing doctrine about temporary warrantless seizures pending further investigation. Second, it explores the caselaw allowing brief seizures based on reasonable suspicion. Third, it considers precedents on temporary warrantless seizures. The fourth Part puts the pieces together, explaining why preservation should require at least reasonable suspicion and, in most cases, will require probable cause. The next Part explains the flaws in the government's contrary position that preservation does not require cause. The Section concludes by considering how long preservation can extend.

A. Preservation and the General Problem of Temporary Warrantless Seizures Pending Further Investigation

It helps to start by identifying the general problem. Government agents often hold a person's property temporarily while they conduct a criminal investigation or seek a warrant to search the property. This temporary holding allows the government to control the property and prevent its disappearance or destruction. Under the Fourth Amendment, the temporary warrantless seizure of the person's property must be "justified at its inception," which requires sufficient reason to believe that the property contains evidence.[161]

An early example of the genre is *United States v. Van Leeuwen*, a case involving the temporary detention of two suspicious packages being sent through the postal mail.[162] Acting on a belief that the packages contained illegally imported coins, officials detained the packages and prevented their delivery for twenty-nine hours.[163] During that time, officials conducted an investigation, developed probable cause, and obtained a warrant to search them.[164] Searching the packages revealed the coins inside and led to charges.[165]

161. *Id.*
162. 397 U.S. 249, 249 (1970).
163. *Id.* at 250.
164. *Id.*
165. *Id.*

The defendant claimed that temporarily detaining the packages violated his Fourth Amendment rights, but the Supreme Court unanimously disagreed.[166] Based on "the facts of this case," the Court ruled, a "29-hour delay between the mailings and the service of the warrant cannot be said to be unreasonable within the meaning of the Fourth Amendment."[167]

Van Leeuwen is just one example of a recurring dynamic. Evidence can be located inside many different containers. It may be helpful for law enforcement to hold on to those containers temporarily—ensuring later government access to them and protecting them from outside interference—while agents investigate and obtain a warrant permitting a search. Investigators might hold on to packages sent through the mail, as in *Van Leewen*.[168] Or the government might hold on to a suspect's luggage, as in *United States v. Place*.[169] They might hold on to a suspect's personal computer, as in *United States v. Mitchell*.[170] They might even hold on to an entire house, as in *Illinois v. McArthur*, where the police prevented a person from entering his home for two hours while they obtained a warrant to search it.[171] In all of these cases, agents seized the property temporarily without a warrant in anticipation of obtaining one. The initial seizure can be permitted, the courts say, by sufficient suspicion that the property contains evidence.

In my view, preservation under § 2703(f) presents a new variation of this traditional problem. When the government submits a preservation request, it directs a temporary seizure of a suspect's property without a warrant. The seizure is designed to prevent the suspect from destroying the evidence that the property may contain. The seizure takes control of the property and sets it aside for later government access with a warrant that permits the property to be searched. Both with physical property and with digital contents, the warrantless seizure of property must be justified by sufficient cause to satisfy Fourth Amendment reasonableness.

To draw the analogy more directly, Internet contents copied and set aside under § 2703(f) are like the suspicious packages detained in *Van Leeuwen.* A snapshot of a suspicious account is a virtual container much like *Van Leeuwen*'s physical containers. The virtual container stores a world of personal messages, e-mails, photographs, videos, and other personal contents, just like a physical container might contain stolen items or illegal drugs. Seizing the container sets it aside unopened unless the government has a search warrant that justifies opening it. The parallels between physical and virtual containers suggest that

166. *Id.* at 253.
167. United States v. Van Leewen, 397 U.S. 249, 253 (1970).
168. *See id.*
169. 462 U.S. 696 (1983).
170. 565 F.3d 1347 (11th Cir. 2009) (per curiam).
171. 531 U.S. 326, 328 (2001).

roughly similar Fourth Amendment standards should apply. Seizing a virtual container must satisfy the Fourth Amendment reasonableness standard much like seizing physical containers did in *Van Leeuwen*.

Of course, one important fact distinguishes detaining a physical container from preserving Internet contents: physical containers cannot be copied. When the government seizes a physical container, it prevents the possessor from having access to it. In contrast, copying a virtual container deprives its possessor of information control without eliminating access to the possessor's copy. When contents are held remotely, as is the case under § 2703(f), the copying occurs in secret if no notice is provided. The owner of the property will not realize he has lost exclusive control. The question is how these factual differences alter the reasonableness calculus in the context of Internet content preservation.

To answer that, we need to study two types of seizures recognized in the caselaw. First, when the government has reasonable suspicion that the property contains evidence, it generally can conduct a brief investigatory hold—normally on the order of minutes or hours—to investigate criminal activity. This is the familiar *Terry* stop applied to property.[172] Second, when the government has probable cause to believe property contains evidence, the government can seize the property for "a reasonable amount of time"[173]—typically days or possibly weeks—while it applies for and obtains a warrant. With these two kinds of seizures explained, we can then consider how the switch from physical to virtual seizures should alter the reasonableness balance.

B. Reasonable Suspicion Traditionally Permits a Very Brief Detention to Investigate

The first kind of temporary warrantless seizures are brief investigatory holds of property based only on reasonable suspicion. Courts have allowed brief seizures of property, generally on the order of minutes or hours, to enable investigators to pause the scene and attempt to gather probable cause that might justify further action.

The leading case is *United States v. Place.*[174] In *Place*, officers temporarily detained luggage belonging to a suspected drug courier who had just arrived on a flight from Miami.[175] After holding the luggage for ninety minutes, the officers brought in a drug-sniffing dog. The dog alerted for the presence of drugs inside the smaller of the two bags.[176] Because it was late on a Friday afternoon, agents

172. *See generally* Terry v. Ohio, 392 U.S. 1, 1 (1968).
173. Illinois v. McArthur, 531 U.S. 326, 334 (2001).
174. 462 U.S. 696, 697 (1983).
175. *Id.* at 698–699.
176. *Id.* at 699.

held the luggage over the weekend and obtained a warrant to search the smaller bag on Monday morning.[177] The search revealed over a kilogram of cocaine.[178]

Place addressed two questions. First, could a temporary detention of luggage be permitted at all based on less than probable cause? The Court held that a very brief detention to investigate whether the luggage contained drugs could be justified by mere reasonable suspicion, not probable cause.[179] "[W]hen the police briefly detain luggage for limited investigative purposes,"[180] the Court reasoned, the balancing framework of *Terry v. Ohio*[181] could apply. This was true because "[w]hen the nature and extent of the detention are minimally intrusive of the individual's Fourth Amendment interests, the opposing law enforcement interests can support a seizure based on less than probable cause."[182]

Place next held that the 90-minute detention of the luggage in that case was unlawful because it exceeded what reasonable suspicion could justify.[183] Although a very brief detention could be permitted with only reasonable suspicion, the ninety-minute detention was so long that "the general rule requiring probable cause for a seizure" instead applied.[184] The Court reasoned that the reasonableness of detaining a person's luggage fell within the *Terry* framework for detaining a person.[185] Because a person was unlikely to leave while his luggage was detained, "the limitations applicable to investigative detentions of the person should define the permissible scope of an investigative detention of the person's luggage on less than probable cause."[186]

In that setting, a ninety-minute seizure was too long to be reasonable without probable cause. "We have never approved a seizure of the person for the prolonged 90-minute period" based only on reasonable suspicion, the Court noted.[187] The ninety-minute delay was also out of bounds because it wasn't needed: agents had failed to "diligently pursue their investigation" to minimize the time of delay.[188] Finally, agents had failed to inform the suspect of what was happening, further exacerbating the unreasonableness of the stop.[189] For all

177. *Id.*
178. *Id.*
179. *See Place*, 462 U.S. at 700.
180. *Id.* at 705.
181. 392 U.S. 1, 30 (1968).
182. *Place*, 462 U.S. at 703.
183. *Id.* at 710.
184. *Id.* at 708.
185. *Id.* at 706.
186. *Id.* at 709.
187. *Place*, 462 U.S. at 709–10.
188. *Id.* at 709.
189. *Id.* at 710.

those reasons, the ninety-minute detention was unreasonable without probable cause.[190]

Reasonableness is inherently fact-sensitive, and *Place* deals with only one set of facts. But its framework has been applied broadly to other temporary seizures, and the caselaw suggests that seizures based on less than probable cause are typically limited to seizures on the order of hours—not days or weeks. *Place* allows officers a brief time to freeze the situation and determine if they can get probable cause. But precedents involving physical containers indicate that this brief time is, well, brief.

Consider *United States v. LaFrance*, which involved the temporary seizure of a FedEx package believed to contain cocaine.[191] Acting based on reasonable suspicion, agents asked FedEx to hold on to the package pending further word.[192] The package's delivery was delayed for 135 minutes before a dog sniffed the package, alerted, and gave the police probable cause.[193] The First Circuit held that this brief detention could be permitted under *Place* based merely on reasonable suspicion.[194] First, the officers had acted expeditiously to obtain the dog sniff.[195] Second, the duration of the delay was slightly less of an intrusion on Fourth Amendment interests than in *Place* because the delay did not interfere with the owner's liberty interests. The property owner was dispossessed of his property, but his freedom was not practically restrained.[196] Finally, the lack of information given to the owner about the seizure was deemed "likely irrelevant" because the seizure was from a third party and not the owner, so that information would not mislead the owner and impair his ability to travel.[197] On the whole, the court concluded, the 135-minute detention was reasonable.[198]

Other cases have allowed somewhat longer detentions based on reasonable suspicion. Although not a model of clarity, *Van Leeewen* had seemed to approve a 29-hour detention of a package.[199] Circuit court cases after *Place* have similarly allowed detentions of postal mail for a day, or in some cases, even longer.[200] Many of the cases resemble the facts of *LaFrance*, in which in which

190. *Id.*

191. 879 F.2d 1, 2 (1st Cir. 1989).

192. *Id.* at 3.

193. *Id.* at 3, 7.

194. *Id.* at 4.

195. *Id.* at 8.

196. *LaFrance*, 879 F.2d at 9.

197. *Id.*

198. *Id.* at 10; *see also* United States v. Gonzalez, 781 F.3d 422, 429 (8th Cir. 2015) (allowing a three-and-a-half-hour delay in similar circumstances).

199. Perhaps unsurprisingly, in light of that description, it is an opinion by Justice Douglas. *United States v. Van Leeuwen*, 397 U.S. 249, 253 (1970).

200. *See, e.g.*, United States v. Lozano, 623 F.3d 1055, 1055 (9th Cir. 2010) (allowing twenty-two-hour delay).

officers detain a postal package based on reasonable suspicion pending a dog sniff. When it takes a long time to get a drug-sniffing dog to confirm or dispel the suspicion, courts have been relatively lenient in allowing a delay as long as officers worked expeditiously to bring in the dogs.

A particularly long delay was permitted in *United States v. Aldaz*, in which a postmaster in "a small bush community" in rural Alaska, reachable only by air, detained packages based on reasonable suspicion that it contained drugs.[201] Because the nearest trained dogs were in Anchorage, 700 miles away, agents waited for a plane and flew the packages to Anchorage where they could be sniffed, and the probable cause either established or dispelled.[202] Waiting for the planes delayed the packages for two to three days.[203] The Ninth Circuit ruled that the delay was nonetheless reasonable, as officers moved as quickly as they could under the circumstances and it was unfair to penalize the government for "the inevitable delays of bush mail."[204]

C. Probable Cause Traditionally Permits a Warrantless Seizure to Allow a Search Warrant to Be Obtained

The second type of caselaw on temporary detentions involves detentions of physical property based on probable cause. In this scenario, the government seizes a container without a warrant, based on probable cause to believe it contains evidence or contraband. Armed with probable cause, the government can then apply for a warrant to search the property. Courts give the government "a reasonable amount of time" to apply for a warrant.[205] The permitted window of delay between the warrantless seizure and obtaining the warrant is typically on the order of days, or at most weeks, not months.

Recent circuit court decisions on seizing personal computers demonstrates both sides of the legal line. In *United States v. Mitchell*, the Eleventh Circuit held that a 21-day warrantless seizure was too long under the circumstances of that case.[206] During an interview with federal agents at his home, Mitchell admitted that there was child pornography on a desktop computer he used.[207] A federal agent opened up the computer, removed the hard drive, and took it into government custody.[208] Three days later, the agent traveled out of state for a two-week training program.[209] The agent applied for and obtained a warrant

201. 921 F.2d 227, 228 (9th Cir. 1990).
202. *Id.* at 231.
203. *Id.*
204. *Id.*
205. Illinois v. McArthur, 531 U.S. 326, 334 (2001).
206. 565 F.3d 1347, 1353 (11th Cir. 2009) (per curiam).
207. *Id.* at 1349.
208. *Id.*
209. *Id.*

three days after he returned from training, a total of 21 days after the hard drive was seized.[210]

Mitchell held that the twenty-one-day delay was unconstitutional "in light of all the facts and circumstances"[211] based on a "careful balancing of governmental and private interests."[212] First, taking the hard drive away was a substantial interference with Mitchell's possessory interest. "Computers are relied upon heavily for personal and business use," the court noted.[213] "Individuals may store personal letters, e-mails, financial information, passwords, family photos, and countless other items of a personal nature in electronic form on their computer hard drives."[214] As a result, "the detention of the hard drive for over three weeks before a warrant was sought constitutes a significant interference with Mitchell's possessory interest."[215] The interference with Mitchell's possessory interest was significant even though Mitchell had admitted that child pornography would be found on the computer. The computer likely contained "other, non-contraband information of exceptional value to its owner," and the government could not be sure that Mitchell was correct that the computer contained contraband images "until an agent examine[d] the hard drive."[216]

On the flip side, the government offered "no compelling justification" for the delay in obtaining the warrant.[217] The agent just didn't think there was a hurry.[218] He could have applied for the warrant before the he left for his two-week training, but he did not.[219] And the agent leaving for his training was not a valid justification for the delay, the court reasoned, as another agent could have taken over the case while the main agent was away.[220] Given that a person's computer was "the digital equivalent of its owner's home, capable of holding a universe of private information,"[221] any additional delay would infringe on the owner's possessory rights by delaying when the device could be returned "if the search reveals nothing incriminating."[222] Because the twenty-one-day seizure

210. *Id.*

211. *Mitchell*, 565 F.3d at 1351 (quoting United States v. Mayomi, 873 F.2d 1049, 1054 n. 6 (7th Cir.1989)).

212. *Id.* (quoting Soldal v. Cook County, 506 U.S. 56, 71 (1992)).

213. *Id.*

214. *Id.*

215. *Id.*

216. *Mitchell*, 565 F.3d at 1351.

217. *Id.*

218. *See id.*

219. *Id.*

220. *Id.*

221. *Mitchell*, 565 F.3d at 1352 (quoting Kansas v. Rupnick, 125 P.3d 541, 552 (Kan. 2005)).

222. *Id.* (quoting United States v. Mitchell, No. CR407-126, 2007 WL 2915889, at *7 (S.D. Ga. Oct. 3, 2007)).

deprived Mitchell of his possessory interest without justification, it exceeded the permitted time window and violated the Fourth Amendment.[223]

The Second Circuit's recent decision in *United States v. Smith* sounds a similar note.[224] An officer seized the suspect's tablet computer when he observed what appeared to be child pornography on the computer's open screen during a traffic stop.[225] The government waited thirty-one days before submitting a warrant to search it, which the Second Circuit ruled was an unreasonable amount of time, and therefore violated the Fourth Amendment.[226]

The Second Circuit in *Smith* applied a four-factor test that considered the length of the delay, the importance of the seized property to the defendant, whether the defendant had a reduced property interest in the seized item, and the strength of the state's justification for the delay.[227] First, thirty-one days was excessive: "if the police have probable cause to seize an item in the first place," the court reasoned, "there is little reason to suppose why they cannot promptly articulate that probable cause in the form of an application to a judge for a search warrant."[228] Second, "personal electronic devices like a modern cell phone or tablet computer" deserved special privacy protection generally in light of the personal items they store, although the defense did not point to the particular importance of that tablet computer.[229] Third, the defendant owned the property and did not consent to its seizure.[230] And finally, the record did not show "any particular investigation or police duty that specifically delayed [the officer] in applying for a search warrant for the seized tablet."[231]

Now contrast *Mitchell* and *Smith* with the Eleventh Circuit's decision in in *United States v. Laist*.[232] *Laist* was a child pornography case in which the defendant admitted that he had child pornography on his computers.[233] Laist showed the officers a sample image and signed a consent form allowing the

223. *Id.* at 1353.

224. 967 F.3d 198, 202 (2d Cir. 2020).

225. *Id.* at 202–03.

226. *Id.*

227. *Id.* at 206. The *Smith* court adopted these standards from an earlier round of the *Smith* case, which had remanded for fact-finding. *See* United States v. Smith, 759 F. App'x. 62, 65 (2d Cir. 2019) ("General relevant considerations include the length of the delay, the importance of the seized property to the defendant, whether the defendant had a reduced property interest in the seized items, and the strength of the state's justification for the delay."). The court also noted in its second opinion in *Smith* that "[o]ther federal appeals courts have set forth similar relevant factors that essentially seek to balance the individual's possessory interest against the government's continuing interest in retaining the property for investigation or prosecution." *Smith*, 967 F.3d at 206 n.1.

228. *Smith*, 967 F.3d at 207.

229. *Id.* at 208.

230. *Id.* at 209.

231. *Id.* at 210.

232. 702 F.3d 608 (11th Cir. 2012).

233. *Id.* at 610.

officers to seize and search his computers. But before the officers took the computers away, they allowed Laist to copy "whatever he wanted" to a separate computer so he would have files he needed for legitimate purposes.[234] About a week after agents took the computers away, Laist revoked his consent.[235] The government continued to hold Laist's computers as it prepared search warrants, but it did not apply for a warrant until twenty-five days after it had received the revocation of Laist's consent.[236] The magistrate judge then took six days to review and grant the warrant, although that time was not considered relevant in considering the reasonableness of the government's seizure.[237]

Laist ruled that the 25-day delay in *Laist* was reasonable.[238] Although the seizure following Laist's withdrawal of consent interfered with his possessory interest, that interference was diminished by Laist's retaining effective control over the non-contraband contents.[239] Laist copied files he wanted before the seizure, and "there is no indication in this record that the FBI would have denied a [later] request to retrieve additional non-contraband material on the computer."[240] "Since the possessory interest in a computer derives from its highly personal contents," the court reasoned, "the fact that Laist had a real opportunity to copy or remove personal documents reduces the significance of his interest."[241] The interference was further diminished by Laist having shown an image of child pornography on the computer to the officers before the seizure.[242]

On the flip side in *Laist*, "the government acted diligently, and thus reasonably," in obtaining the warrant.[243] Although the government had taken twenty-five days to apply for the warrant, the agents had started preparing the warrant immediately and had gone through several drafts.[244] The case was unusually complex, and the affidavit they submitted was long and detailed. The agents also had been very busy with other cases.[245] As a result, although the twenty-five-day delay was "far from ideal," the officers had been "sufficiently diligent to pass muster under the Fourth Amendment."[246] The case was therefore distinguishable from the slightly shorter delay ruled unconstitutional in *Mitchell*,

234. *Id.* at 611.
235. *Id.*
236. *Id.* at 614 n.2.
237. *Laist*, 702 F.3d at 614–15.
238. *Id.* at 616.
239. *Id.*
240. *Id.*
241. *Id.*
242. *Laist*, 702 F.3d. at 616.
243. *Id.*
244. *Id.* at 616–17.
245. *Id.* at 617 ("An investigation of this scope and complexity requires more time to prepare a warrant.").
246. *Id.*

where there was no good reason for the delay and there had been a greater interference with the computer owner's possessory interest.[247]

As *Mitchell*, *Smith*, and *Laist* show, the reasonableness of a seizure based on probable cause is not only about the period of the delay. Whether the inquiry is expressed formally as a multi-factor test (as the Second Circuit does) or a weighing of government and security interests (as other circuits do),[248] what matters in this totality-of-the-circumstances inquiry is the balance between the extent of the seizure's interference with the possessor's interests in the seized property and the government's diligence in pursuing a warrant.[249] The more the seizure interferes with the owner's interests, the more brief the seizure must be. Conversely, it is important that officers show diligence in seeking a warrant.

D. Preservation Should Require At Least Reasonable Suspicion – and in Most Cases, It Should Require Probable Cause

The critical question is how to determine the reasonableness framework for Internet content preservation. The Supreme Court has explained that the reasonableness of a warrantless seizure has a two-fold requirement: it must be "justified at its inception" and then "reasonably related in scope to the circumstances which justified the interference in the first place."[250] It is therefore helpful to analyze the reasonableness of Internet content preservation under the same two lenses. First, what kind of cause is needed to justify preservation at its inception? Next, how long can preservation extend so that it is reasonably related in scope to the circumstances which justified the interference in the first place? This Section begins with the first question, the needed cause to justify preservation at its inception.

In my view, justifying Internet content preservation at its inception will ordinarily require at least reasonable suspicion—and in most cases, it should require probable cause. This is the lesson taught by the caselaw on temporary physical seizures analyzed in Parts B and C above. At the inception stage of the seizure, the similarities between seizing physical contents and seizing digital contents are compelling. In both contexts, the government takes control of the person's property and sets it aside to investigate. The initial seizure triggers a transfer of control from the citizen to the government. In both cases, the transfer of control is merely anticipatory. The government sets aside the container without opening it. But the seizure negates the user's control of the property and gives that control to the government.

Justifying this transfer of control should require the same initial cause for temporary digital seizures that it requires for temporary physical seizures. As

247. *Laist*, 702 F.3d. at 617–18.

248. *See* United States v. Smith, 967 F.3d 198, 206 n.1 (2d Cir. 2020) (citing cases).

249. *See also* Illinois v. McArthur, 531 U.S. 326, 326 (2001).

250. Terry v. Ohio, 392 U.S. 1, 20 (1968).

United States v. Place emphasized, "the general rule" under the Fourth Amendment is that "probable cause [is required] for a seizure."[251] At the same time, the government can "briefly detain luggage for limited investigative purposes"[252] under the balancing framework of *Terry v. Ohio*[253] based only on reasonable suspicion. "When the nature and extent of the detention are minimally intrusive of the individual's Fourth Amendment interests, the opposing law enforcement interests can support a seizure based on less than probable cause."[254] Justifying Internet content preservation should trigger the same framework. The general rule should be that probable cause is required, although some brief preservation for limited investigative purposes can be justified by reasonable suspicion.

I am not arguing that the reasonableness framework for physical seizures should be adopted wholesale for Internet content preservation. As noted earlier, digital seizures are different from physical seizures in an important way.[255] When the government seizes physical property, it interferes with two Fourth Amendment possessory interests: the possessory interest in control and the possessory interest in use. A physical seizure takes both. When there is only one item, and it cannot be copied, taking control of it necessarily eliminates the owner's access and use. In contrast, when the government copies Internet contents, it interferes with the interest in control without affecting the interest in use. The government gets a new copy, but the user retains control over the old one. Control is lost, but use is retained.

This difference should alter the reasonableness of Internet content preservation, in my view, but not at the first step of justifying the seizure at its inception. Recall that the reasonableness of a warrantless seizure has two steps: it must be "justified at its inception," and the scope of the seizure must be "reasonably related in scope to the circumstances which justified the interference in the first place."[256] This distinction neatly tracks the two possessory interests. Justification at a seizure's inception is primarily about loss of control. The government gains control at the moment of inception. In contrast, the scope of the seizure is more about the property owner's loss of use. After the initial seizure occurs, it can go on for a long time. The longer it goes, the greater the deprivation of use. From this perspective, the reasonableness of Internet content preservation at its inception should track the reasonableness of physical seizures at their inception. The difference in the reasonableness framework should occur

251. 462 U.S. 696, 708 (1983).
252. *Id.* at 705.
253. *Terry*, 392 U.S. at 19–20.
254. *Place*, 462 U.S. at 703.
255. *See supra* note 146 to 151 and associated text.
256. *Terry*, 392 U.S. at 20.

at the second step (the scope of the seizure) rather than the first step (the initial seizure).

Although the scope of seizures will be addressed later, it is worth flagging now why most preservation will require probable cause and not just reasonable suspicion.[257] The *Terry* framework that permits seizures based on reasonable suspicion is quite limited. As Section IV, Part B showed, the *Terry* authority allows the government to freeze the scene only briefly. The government can hold on to physical property on the scene as it assesses probable cause, enabling investigators to bring in drug-sniffing dogs or ask the suspect questions.[258] The temporary seizure is reasonable because otherwise the property would be physically taken away and the government might not be able to get it back.

Internet content preservation should normally require probable cause because it does not typically occur with the limited purpose or for the limited time that *Terry* allows. This is implicit in the technology itself. Because providers host accounts, and they cooperate with government investigations under the SCA, investigators that are able to preserve a specific account under § 2703(f) also have technological access to its contents with a search warrant under § 2703(a) as long as the account remains operating. With the provider able to access contents at any time, government-directed preservation will tend to have a long time horizon. Freezing a scene briefly to make sure property doesn't get away, as *Terry* permits, typically won't be needed. Instead, preservation will be undertaken just in case a suspect deletes incriminating files, or his entire account weeks or months down the road. In the ordinary case, preservation will not fit within the *Terry* reasonable suspicion framework.

The need for probable cause is particularly strong given the personal and sensitive nature of Internet contents subject to seizure under § 2703(f). Precedents on the search and seizure of personal computers and cell phones have already recognized the deeply personal nature of electronic messages. As the Second Circuit noted in *Smith*, the "age of digital storage" enables the government to seize "immense amounts of personal data," much of which "will be deeply personal and have nothing to do with the investigation of criminal activity."[259]As the Supreme Court recognized in *Riley v. California*, digital storage devices such as modern cell phones, "as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[260]

The same principle applies to the electronic seizure of remotely stored Internet contents. Section 2703(f) is widely used by law enforcement precisely

257. *See infra* Section IV, Part F.

258. *See supra* Section IV, Part B.

259. United States v. Smith, 976 F.3d 198, 207 (2d Cir. 2020) (quoting United States v. Ganias, 824 F.3d 199, 218 (2d Cir. 2016) (en banc)).

260. 573 U.S. 373, 393 (2014).

because so much of what people do, say, and think is recorded in their online accounts. E-mail accounts can store tens of thousands of personal messages.[261] Facebook accounts will include all of a person's Facebook private messages, all of their uploaded photographs, and all of their status updates.[262] A world in which so many Americans detail their most personal thoughts and personal events in their private accounts is a world in which an extraordinary amount of their private lives is available to be preserved under § 2703(f). As cases like *Riley* and *Smith* suggest, the extraordinary detail and personal nature of so much digital information weighs strongly toward requiring probable cause for most Internet content preservation.

E. DOJ's Flawed Argument That Preservation Does Not Require Cause

DOJ offered a very different view of preservation's reasonableness in *Basey*.[263] DOJ argued that, if preservation causes a seizure, it is a reasonable seizure without any cause. According to DOJ, "[t]he privacy impact of preservation requests on account holders is minimal."[264] Preservation does not block user access and does not compel disclosure.[265] Further, the duration of preservation is "brief, and afterwards the provider is free to delete the preserved information."[266] On the other hand, preservation advanced a "compelling" government interest: "Electronic evidence is critical in a wide range of criminal investigations, and it can be deleted irretrievably in an instant."[267] "Balancing these interests," DOJ argued, "the government's reliance on the preservation rules of § 2703(f) is reasonable."[268]

I am not persuaded. The existing caselaw on reasonableness has not permitted temporary seizures pending further investigation without cause. As Section IV Parts B and C showed, "the general rule" is that probable cause is required to justify such a seizure.[269] The exception to the general rule, applicable in narrow circumstances, permits a brief seizure based only on reasonable suspicion.[270] I am aware of no authority permitting temporary warrantless seizures to investigate further without *any cause at all*.[271] Notably, DOJ's *Basey*

261. *See* Mike Barton, *How Much Is Your Gmail Account Worth?*, WIRED (July 25, 2012), http://www.wired.com/insights/2012/07/gmail-account-worth [https://perma.cc/BS82-FKSC].

262. Det. James Williams, *supra* note 78, at 17–22 (listing the items that Facebook stores for each account).

263. *See* DOJ Basey Brief, *supra* note 130, at 29.

264. *Id.* at 28.

265. *Id.*

266. *Id.*

267. *Id.* at 29.

268. DOJ Basey Brief, *supra* note 130, at 29.

269. United States v. Place, 462 U.S. 696, 708 (1983).

270. *See supra* Section IV, Part B.

271. Perhaps the case closest to that position is *Maryland v. King*, which held that the government can conduct a search of person's cheek using buccal swab to obtain their DNA sample

brief points to no such authority. Such a rule would be particularly inappropriate given the highly sensitive and personal documents that the government seizes on a massive scale under § 2703(f).

In addition, DOJ's characterization of the preservation process does not ring true. The seizure is not "brief," as DOJ claims. The statute requires preservation for two ninety-day periods. It is hard to see how a seizure lasting half of a year could count as "brief" in light of the caselaw discussed earlier. Whether the privacy impact of preservation is minimal misses that preservation is a seizure, not a search. It requires justification because it takes control of a person's private communications, not because it exposes them—a step that itself would require a warrant, not just some amount of cause.

Finally, the risk that valuable electronic evidence "can be deleted irretrievably in an instant" does not differentiate electronic seizures from physical seizures.[272] The concern justifying temporary warrantless physical seizures has always been that a seizure now may be needed to ensure that important evidence is not lost. Recall the many cases in which the government seizes a package suspected of containing drugs.[273] Unless the government held on to the package, the package and its contents could be gone forever. Drugs might be flushed down the toilet, moved to an unknown place, or consumed. The ease of deleting digital evidence is nothing new and does not justify a different rule.

F. The Permitted Period of Preservation

The final reasonableness question is the scope of preservation.[274] This is primarily a question of time. After preservation of contents has begun, how many days can elapse before either a warrant is obtained to compel the contents, or the preservation ends without disclosure and the contents are deleted? I think there are two very different answers, depending on whether the basis for the preservation was reasonable suspicion or probable cause. If the preservation was based only on reasonable suspicion, the preservation normally must be quite

after arresting them for a serious offense. 569 U.S. 435, 447–66 (2013). The Court reasoned that the pressing need to learn someone's identity upon their arrest makes the swab reasonable in light of the diminished expectation of privacy of a person who has been arrested. *See id.* But if *King* is the government's best case for the reasonableness of § 2703(f) preservation without cause, that only signals the weakness of the government's position. *King*'s balancing of interests relied heavily on the fact that the person searched was already arrested and the information obtained was limited to identity information. In contrast, the debate over § 2703(f) is about whether a suspect's voluminous and private electronic documents can be seized without cause at the outset of case. The natural fit is with precedents like *Place* and *MacArthur*, not *King*. *See id.*

272. DOJ Basey Brief, *supra* note 130, at 28.

273. *See supra* Section IV Parts A–C.

274. Terry v. Ohio, 392 U.S. 1, 20 (1968) (requiring the that the extent of a seizure be "reasonably related in scope to the circumstances which justified the interference in the first place.").

brief. On the other hand, if the initial preservation is based on probable cause, then it can generally be quite long—on the order of many weeks or even months.

Internet content preservation based only on reasonable suspicion should be quite rare and quite brief. As noted above, the preservation process doesn't fit *Terry*'s reasonable suspicion framework very well. Reasonable suspicion seizures are about quickly freezing a scene to investigate further.[275] In the case of a physical package, the seizure might be permitted to bring in drug-sniffing dogs, or to ask its owner some questions.[276] The delays are short, typically from minutes to hours—at most a few days when the investigation cannot be done more quickly. [277]

Internet preservation won't normally fit this framework, because preservation usually is aimed at a different problem. Content preservation exists because a suspect might, at some point, delete incriminating files or even his entire account. Preservation will implicate this concern in the short-term sense, primarily when exigent circumstances exist. For example, if the police learn that a suspect knows he is under investigation, and that he told people that morning that he is going to delete his account that day, an exigency would exist that would justify quick preservation based on reasonable suspicion. But such a scenario will be rare. In the ordinary case, preservation occurs with a longer time horizon just in case the suspect at some point deletes his contents. A brief preservation permitted by reasonable suspicion is possible, but it should be uncommon.

A different picture appears when the government has probable cause. In such a case, the permitted window of delay between preservation under § 2703(f) and serving a warrant under § 2703(a) can be quite long. With probable cause existing to justify initial preservation, the Fourth Amendment interest in a prompt warrant application becomes modest. The user is not denied access to his account during the preservation. The user does not know preservation has occurred, so his experience accessing the account is the same regardless of how long the preservation occurs. And after the contents of an account have been set aside, it makes no obvious difference whether the information preserved is disclosed now or disclosed later. Either way, the same information is disclosed. The duration of the seizure is therefore relatively unimportant.

The Eleventh Circuit's ruling in *United States v. Laist*, discussed earlier, is helpful on this point.[278] In the course of upholding a twenty-five-day delay before officers submitted a warrant application to search Laist's computers, the Eleventh Circuit emphasized that Laist had been given the opportunity to copy

275. *See supra* Section IV, Part B.
276. *Id.*
277. *Id.*
278. *See supra* notes 226 to 243.

any files he needed—"whatever he wanted"—before the seizure occurred.[279] "Since the possessory interest in a computer derives from its highly personal contents," the court reasoned, "the fact that Laist had a real opportunity to copy or remove personal documents reduces the significance of his interest" and helped make the delay reasonable.[280] This is all the more so with purely electronic copying that does not interfere with the user's access to his files at all.

It's worth asking: does the period of delay matter at all when the initial preservation was justified by probable cause? Does it matter if the government comes back with a warrant after a day, versus after a year? Precedents on physical seizures suggest that delay should matter because officers must be diligent in seeking a warrant. If the police are not diligent in obtaining the warrant, the seizure is not likely to be upheld as reasonable.[281] Should the same be true of electronic preservation based on probable cause?

When the government has probable cause at the inception of the preservation, a significant delay between preservation and the warrant should be permitted. Extended periods of delay should be permitted in this situation because extra delay imposes only an abstract additional infringement on the account holder's Fourth Amendment rights. The period of delay between preservation and the warrant matters only for when the warrantless seizure is subjected to a judicial determination of probable cause. *Mitchell* stressed that additional delay can interfere with a possessory interest in physical property for that reason: the longer property is seized before a warrant is obtained, the longer the infringement of Fourth Amendment interests will extend if a judge later concludes that no probable cause existed.[282]

The possessory interest is very slight, however, when a seizure has occurred only through electronic copying and the user retains access to his personal data. Because the test for probable cause would look to the time of preservation, the timing of judicial assessment of probable cause makes no obvious impact on the user's Fourth Amendment rights. The government has gained control of a preserved copy of the account but cannot access the copy without a warrant. Whether the judicial probable cause determination needed to obtain the warrant happens now or later has no obvious impact on the user's Fourth Amendment rights.

The reader may wonder: If the timing of the judicial determination of probable cause has little impact on the user's Fourth Amendment rights, then why require the government to have probable cause at the outset of preservation? At first blush, it might seem inconsistent to require cause at the inception of

279. United States v. Laist, 702 F.3d 608, 611 (11th Cir. 2012).

280. *Id.* at 616.

281. *See, e.g.*, United States v. Place, 462 U.S. 696, 709–10 (1983); *see also Laist*, 702 F.3d at 617.

282. *See* United States v. Mitchell, 565 F.3d 1347, 1351 (11th Cir. 2009) (per curiam).

preservation, but to then say that it makes little difference how much time elapses before a judge determines whether probable cause exists. But no inconsistency exists. The Fourth Amendment harm when preservation occurs without cause is that the government has taken control of constitutionally protected contents without cause. A cause requirement at the outset prevents limitless wholesale seizures on the off chance that probable cause will happen to someday emerge. In contrast, the post-preservation timing of a judicial determination of probable cause looks at a different question. It asks when a court will determine whether probable cause existed both at the inception of preservation.[283] Also, if new facts later emerged, the court will determine if probable cause also existed when the warrant was obtained.[284]

V. CONSEQUENCES AND REMEDIES

This Section offers two perspectives on the argument I have made in this article. First, it explains the proper role of Internet content preservation under the Fourth Amendment limits I have proposed. 18 U.S.C. § 2703(f) can continue to be an important part of the SCA. But it must be used much more sparingly than it has been used in the past. Preservation can give the government time to draft a proper warrant, and it can prevent destruction of evidence when exigent circumstances have been shown. But it cannot be used to preserve every suspect's account just in case probable cause emerges down the investigatory road.

The Section then turns to a practical litigation point. How might these issues come up in court? In particular, how might the Fourth Amendment limits of Internet content preservation be litigated in a criminal case? This Section focuses on two exceptions to the exclusionary rule that are likely to come up in litigation, the good-faith exception of *Illinois v. Krull*[285] and the inevitable discovery exception. These doctrines may make suppression a tricky road to travel, but they also leave open a path for a criminal defense challenge to current practices in the right circumstances.

283. In a case where there was an initial preservation based only on reasonable suspicion, the court would need to ask if there was reasonable suspicion at the outset of preservation and then probable cause by the time the reasonable-suspicion window elapsed and probable cause was required.

284. If probable cause existed at the moment of preservation, but new facts later emerged before a warrant was obtained that eliminated that probable cause, the government would be unable to compel disclosure of the preservation copy. *Cf.* United States v. Tenerelli, 614 F.3d 764, 770 (8th Cir. 2010) (discussing how a warrant can become stale if probable cause dissipates between the time the warrant is signed and the warranty is executed).

285. 480 U.S. 340, 360 (1987).

A. The Proper Role of Internet Content Preservation

This article suggests a dramatically narrowed role for Internet content preservation under the SCA. Investigators should no longer be allowed to issue preservation requests whenever they find out that a suspect has an Internet account just in case probable cause later emerges. Section 2703(f) cannot be used like a machine gun, letting officers spray preservation bullets at anything that moves, only to later see if they hit anything important. Instead, Internet content preservation must be targeted. In most cases it will require probable cause, and at the very least it will require reasonable suspicion for very brief periods of preservation.

This does not mean that Internet content preservation must cease. Preservation can continue to play a significant role in many cases. Most importantly, preservation will remain important because writing up a warrant can take time. Determining the correct description of the evidence needed to satisfy the Fourth Amendment's particularity requirement can require considerable legal judgment. Explaining a complex digital crime investigation completely and accurately in an affidavit can require considerable time. As a matter of executive branch policy, warrant applications drafted by one agent or prosecutor may be reviewed by others first before a judge sees them.

Under my approach, preservation permits the government to order preservation of an account immediately, so agents can take their time to get the warrant details right. Agents can preserve, freezing the whole account, as soon as they have probable cause. They can then draft the warrant carefully later, making sure that the application they submit to a judge to compel disclosure has properly described the investigation, particularly described the property to be seized, and received the internal reviews that ensure the application is error-free. The preservation authority ensures that the warrant application process will not be rushed by fears that data will be deleted. This role should ring a bell, as it is the same role that the temporary seizure doctrine served for physical property in cases like *Mitchell*, *Smith*, and *Laist*.[286]

Preservation also can be used when exigent circumstances exist. If investigators learn that a suspect is likely to delete his account, or otherwise to delete incriminating records, the preservation authority can enable an immediate seizure to set aside the data and take it beyond the user's control. Again, this is a familiar role from caselaw on seizing physical computers. If an agent is speaking to a suspect about evidence of crime on his cell phone or laptop, and the suspect realizes the agent is coming back with a warrant to seize it, exigent circumstances may exist permitting the agent to seize the computer to prevent the suspect from destroying the hard drive or deleting incriminating files.[287] Preservation can serve the same role for Internet contents that it serves for

286. *See* Section IV, Part D.

287. *See, e.g.*, United States v. Bradley, 488 F. App'x 99, 103 (6th Cir. 2012).

physical devices. It just does so through the intermediary of the content provider rather than through direct action by an officer.

I don't mean to catalog the full set of circumstances in which preservation may be used. Fourth Amendment reasonableness can take many forms, making a universal answer impossible to provide. But the core lesson is that Internet content preservation needs to fit the same basic constitutional limits as other temporary seizures. For the last quarter century, § 2703(f) has been interpreted to allow the government to preserve everything with no cause. It has allowed investigators months to develop probable cause, and to simply not follow up in the majority of cases when no probable cause emerged. That practice must end.

B. Challenging Preservation in Court, and the Scope of Exclusionary Rule

The final question to consider is how challenges might be brought successfully in court. Civil actions are relatively unpromising. The absence of notice precludes civil suits when the government did not follow up with a warrant. When the government followed up with a warrant, but no charges were brought, the statute does not require notice to the user, either.[288] Even when notice has been provided, civil actions against providers will run into the broad statutory good faith exception[289]—or, in cases against the government, qualified immunity.

The more promising litigation context is a motion to suppress in a criminal case. Prosecutors usually will not, by default, disclose records of prior preservation. But defense counsel should press the issue. In every case where discovery reveals that a search warrant for Internet contents was obtained under 18 U.S.C. § 2703(a), defense counsel should assume that the warrant was preceded by preservation under § 2703(f). They should ask for any records on when a preservation request was made and how broadly it extended, including the contents of any preservation request letter that was sent to the provider. Defense counsel should also scrutinize any warrant materials for references to prior preservation. The goal should be nailing down the precise date on which preservation occurred—the point by which, if my arguments are correct, probable cause (or at least reasonable suspicion) must have been established.

Now assume a criminal defendant files a motion to suppress and can establish that preservation under § 2703(f) violated his Fourth Amendments rights. Can he actually win a motion to suppress? Here the picture is mixed. Suppression is always an uphill battle. That is particularly true when a defendant

288. *See* 18 U.S.C. § 2703(a). Notice may be provided under a provider's privacy policy, however, unless notice is forbidden under a gag order imposed by 18 U.S.C. § 2705(b).

289. *See* 18 U.S.C. § 2707(e) ("A good faith reliance on– (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title)").

wins on a new Fourth Amendment claim.[290] At the same time, the prospect of suppression is less bleak than it may first seem. The good-faith exception of *Illinois v. Krull*[291] might apply, but there is a significant argument that it should not. While the inevitable discovery exception might apply, it would apply only to the warrant copy. The inevitable discovery exception would not apply to the contents found only in the preservation copy.

1. The Good-Faith Exception of *Illinois v. Krull*

The first exclusionary rule doctrine to consider is the good-faith exception of *Krull. Krull* directs that the exclusionary rule does not apply when officer conducts a search or seizure "in objectively reasonable reliance upon a statute."[292] When a statute permits an act that courts later determine violates the Fourth Amendment, the thinking runs, officers are entitled to rely on the implicit legislative judgment that the statute was constitutional and should not be punished when they do:

> Unless a statute is clearly unconstitutional, an officer cannot be expected to question the judgment of the legislature that passed the law. If the statute is subsequently declared unconstitutional, excluding evidence obtained pursuant to it prior to such a judicial declaration will not deter future Fourth Amendment violations by an officer who has simply fulfilled his responsibility to enforce the statute as written.[293]

At first blush, the case for relying on the good-faith exception when the government makes a § 2703(f) request seems straightforward. For a quarter century, since the law was enacted, the common understanding has been that § 2703(f) permits preservation requests at any time. After all, the law imposes no textual limits on when the government can request preservation. The Justice Department (including me, when I was there) and providers have understood that to mean that no limits exist. Preservation requests have been thought to be entirely at the government's discretion, with both agents and prosecutors having been trained accordingly. Absent contrary caselaw, it would be reasonable for an agent or prosecutor to assume that this shared understanding is correct.

But there's a problem with this argument. As Section I explained, the text of § 2703(f) is unclear about when the government can request preservation and what records preservation covers.[294] The prevailing practice has been to understand § 2703(f) as authorizing the government to order content

290. *See, e.g.*, Davis v. United States, 564 U.S. 229, 232 (2011) (holding that the exclusionary rule is not available if the government's conduct complied with then-existing precedents that have since been overturned).

291. 480 U.S. 340, 340 (1987).

292. *Id.* at 349.

293. *Id.* at 349–50.

294. *See supra* Section I, Parts B and D.

preservation whenever it wishes. But that interpretation may very well be wrong.[295] The uncertainty leaves unclear whether *Krull* applies. *Krull* is premised on the idea that investigators would reasonably decline to second-guess "the judgment of the legislature that passed the law" in authorizing what courts later conclude is a constitutional violation.[296] If the legislature made no such judgment, however, *Krull*'s reasoning may not apply.

If a court agrees that an unconstitutional act of preservation occurred, and that it was not authorized by the language of the statute, whether the good faith exception applies becomes quite murky. Courts might say that, with *Krull* out of the way, the exclusionary rule applies. Alternatively, they might say that the reasonable-mistake-of-law principle of *Heien v. North Carolina*[297] combines with *Krull* when the statute has been reasonably misinterpreted. On that thinking, perhaps the exclusionary rule does not apply when an officer reasonably misinterpreted a statute as authorizing preservation, and, if that misinterpretation had been correct, *Krull* would have then applied. I take no position on that question. Instead, I merely note that this application of the exclusionary rule is not clear.[298]

2. The Inevitable Discovery Exception

The second question is how the inevitable discovery exception might apply. Under the inevitable discovery exception, the exclusionary rule does not apply when "the prosecution can establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means."[299] The basic idea is a "but for" causation test. If the evidence would have been discovered anyway if the unconstitutional act never occurred, its discovery was not caused by the unconstitutional act and should not be suppressed.

Applying the inevitable discovery exception to preservation is surprisingly straightforward. As Section II explained, providers typically comply with a search warrant on a preserved account by working from two copies of the account—the preservation copy and the warrant copy.[300] The preservation copy is the set of responsive files made at the time of preservation, and the warrant

295. *Id.*

296. *Krull*, 580 U.S. at 350.

297. 135 S.Ct. 530, 540 (2014).

298. This issue was anticipated, but expressly not answered, in *Krull*. *See Krull*, 480 U.S. at 361–62 n. 17 (declining to address whether the exclusionary rule would apply if an officer acted outside a statute that authorized searches and seizures later deemed unconstitutional, and noting that the application of the exclusionary rule "might well be different when police officers act outside the scope of a statute, albeit in good faith" because "the relevant actors are not legislators or magistrates, but police officers").

299. Nix v. Williams, 467 U.S. 431, 444 (1984).

300. *See supra* notes 101 to 103, and accompanying text.

copy is the set of responsive files created from the account as it existed when the warrant was served.[301] Providers sometimes comply with a warrant by handing over both copies separately, and other times do so by combining the two copies into a single production.[302]

Applying the inevitable discovery exception leads to a simple outcome: the exclusionary rule applies to the preservation copy but not to the warrant copy. If the preservation copy is the fruit of an unconstitutional seizure, then it should not have existed and it cannot be used. But the warrant copy exists independently of preservation, and therefore it exists independently of the constitutional violation. The government can ensure that it is only using "information [that] ultimately or inevitably would have been discovered by lawful means,"[303] by using only the warrant copy.[304]

The simplicity of this answer gives some reason for law enforcement to ask for compliance with warrants on preserved accounts, in the form of distinct preservation and warrant copies instead of one combined production. If the government receives the two copies separately, it can respond to a successful suppression motion—or, ex ante, avoid a possible Fourth Amendment challenge—by using only the warrant copy. Receiving a combined production, without a distinct warrant copy, creates a more difficult situation for the government because it bears the burden of establishing inevitable discovery.[305] The government would have to put the toothpaste back in the tube by showing that each incriminating message was in the account when the warrant was served. Although not an impossible task, it is far easier to simply work from the warrant copy.[306]

CONCLUSION

Applying the Fourth Amendment to new technologies often leads to calls for change. Digital is different, the argument runs, and old rules must be adapted

301. *Id.*

302. *See supra* Section II, Part D.

303. *Nix*, 467 U.S. at 444.

304. *Cf.* United States v. Perez, 798 F. App'x. 124, 126 (9th Cir. 2020) (declining to address how the Fourth Amendment applies to § 2703(f) because it was not clear error for the district court to have found that the evidence compelled was from the warrant copy and not the preservation copy).

305. *See* United States v. Lazar, 604 F.3d 230, 239–41 (6th Cir. 2010).

306. If the provider has not saved records of what contents were in the warrant copy, one government strategy might be to obtain a second warrant in anticipation of (or in response to) the suppression litigation. If specific incriminating contents are still in the account when the second warrant is served, then those contents are admissible. But this is an imperfect strategy, as there may be account contents that existed at the time of the first warrant that were deleted by the time of the second warrant.

to modern facts.[307] But that is *not* the claim I am making here. My argument is about similarity, not difference. Internet content preservation should be subject to the same basic Fourth Amendment restrictions that courts have applied to the temporary seizures of packages, mail, and physical computers. Current practices are unconstitutional not because the legal rules must be changed, but because the current practices have never been subject to constitutional scrutiny at all.

Historically speaking, that is understandable. 18 U.S.C. § 2703(f) was enacted in 1996, long before courts began to consider the Fourth Amendment limits on disclosure of stored Internet records. At a time when the government could simply subpoena most of a suspect's e-mails, the idea of requiring probable cause for mere preservation would have seemed fanciful. But our understanding of how the Fourth Amendment applies to the Internet has changed. We now see Internet contents as akin to mail and packages. Our understanding of Internet preservation must be similarly brought up to date. The government has enjoyed a windfall of unlimited preservation for long enough.

307. I have made this argument often myself. *See, e.g.*, Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 407 (2013) ("The computer will be to the 21st century Fourth Amendment what the automobile was to the 20th century Fourth Amendment. In both cases, transformative technologies justify technology-specific rules.").