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.").

Katz Has Only One Step: The Irrelevance of Subjective Expectations

Orin S. Kerr†

This Essay argues that the "subjective expectation of privacy" test from Katz v United States *is a phantom doctrine. The test exists on paper but has no impact on outcomes. An empirical study of cases decided in 2012 indicates that the majority of judicial opinions applying* Katz *do not even mention the subjective-expectations test; opinions that mention the test usually do not apply it; and even when courts apply it, the test makes no difference to the results.*

The subjective test acts as a phantom doctrine because of an overlooked doctrinal shift. A close reading of Justice John Marshall Harlan's Katz *concurrence suggests that the subjective test was originally intended to restate the holdings of the Supreme Court's cases on invited exposure. Under those cases, an individual waives his Fourth Amendment rights by inviting others to observe his protected Fourth Amendment spaces. After* Katz*, however, the Supreme Court misunderstood this original design and recast those holdings as part of the objective test instead of the subjective test. This doctrinal shift quietly eliminated the role of the subjective test. The Supreme Court should abolish the subjective-expectations test to clarify and simplify Fourth Amendment law.*

INTRODUCTION

Every student of criminal procedure knows that the *Katz* test for Fourth Amendment searches requires a two-part inquiry.[1] To establish a search under *Katz*, individuals must first demonstrate "an actual (subjective) expectation of privacy" and then show that "society is prepared to recognize [that expectation of privacy] as 'reasonable.'"[2] The first part of the test is subjective, and the second part is objective. Both the subjective and

† Fred C. Stevenson Research Professor of Law, George Washington University Law School. Thanks to Wayne LaFave and Joshua Dressler for comments on an earlier draft. Derek Woodman provided outstanding research assistance.

1 In this Essay, "the *Katz* test" refers to the two-part test for identifying whether a search has occurred that was introduced in Justice John Marshall Harlan's concurring opinion in *Katz v United States*, 389 US 347 (1967). See id at 361 (Harlan concurring). The test was later adopted by the full Court. See *Smith v Maryland*, 442 US 735, 740 (1979).

2 *Katz*, 389 US at 361 (Harlan concurring).

objective tests must be satisfied for a court to identify a Fourth Amendment search under *Katz*.[3]

Or so the courts say. But what if the courts are wrong?

This Essay argues that *Katz* is only a one-step test. Subjective expectations are irrelevant. A majority of courts that apply *Katz* do not even mention the subjective inquiry; when it is mentioned, it is usually not applied; and when it is applied, it makes no difference to outcomes. Further, this odd state of affairs is explained by a subtle and overlooked shift in Supreme Court doctrine in the 1970s and 1980s. The Court's decisions reclassified the subjective question as part of the objective test.[4] The change left the subjective test a phantom doctrine; it is an empty shell of words that has no function other than to confuse. The Court should formally abolish the subjective test to make Fourth Amendment law more simple and clear.

This Essay's descriptive conclusions are based on a study of every case published in 2012 available in Westlaw's ALLCASES database that applied *Katz*—540 cases in all.[5] In the study, only 43 percent of cases even mention the subjective-expectations test. Only 12 percent of cases apply the subjective test. And among the cases that apply the subjective test, there appear to be none in which the subjective inquiry controlled the outcome. No opinion held that the defendant satisfied the objective test but not the subjective test, which would have indicated that the subjective test changed the result. In a small number of cases—about 2 percent—the court held that the subjective test was not satisfied (and therefore no search occurred) without expressly reaching the objective test. But a review of those cases reveals that, in each case, the court used precedents and reasoning from the objective test and simply rephrased the inquiry as one of subjective expectations.

We are left with a puzzle: Why would the Supreme Court adopt a doctrine that has no impact on outcomes? The answer lies in a previously unrecognized shift in the Court's understanding of *Katz*. A close reading of Justice John Marshall Harlan's concurrence suggests that the subjective test originally

---

[3] Id. At least this is the case under the *Katz* test. A search can also be found under the trespass principles of *United States v Jones*, 132 S Ct 945, 951–52 (2012) ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

[4] See Part II.B.

[5] See Part I.

was meant to summarize precedents on exposure to third parties such as undercover agents and informants. The test did not actually measure subjective expectations. Instead, it reflected the notion that intentionally sharing information with someone relinquishes privacy in that information. Beginning in the 1970s, however, the Supreme Court recast this idea as an application of the reasonable-expectations prong, and specifically as the so-called third-party doctrine.[6] The concept that exposure waives rights jumped doctrinal boxes from the subjective prong of *Katz* to the objective prong.

This doctrinal shift left the subjective test an empty shell. Because an individual must satisfy both parts of the test to establish a Fourth Amendment search, the replication of work in the two prongs ensures that the subjective test cannot alter outcomes. In some opinions, the Supreme Court has reinterpreted the subjective test to instead assess actual subjective expectations—that is, whether the individual believed police access was likely. But the Court has also recognized that this interpretation is problematic and that reliance on true subjective expectations would be improper. The subjective test is irrelevant under either interpretation. Either it is irrelevant because it merely replicates the objective test, or it is irrelevant because the Supreme Court has suggested that courts should ignore it when it might actually alter outcomes.

Despite its irrelevance, the subjective element of *Katz* has lived on in the Supreme Court's cases. It is dutifully repeated but never closely analyzed. The Supreme Court should abolish the subjective-expectations test and make clear that the *Katz* test has only one step. Doing so would make the law less confusing. It would also help clarify that the scope of *Katz* is a normative question rather than a descriptive claim about what people actually expect.

This Essay proceeds in two parts. First, it introduces an empirical study of the *Katz* test to show that the subjective-expectations test is irrelevant in practice. Second, it traces the history of the *Katz* test to show how doctrinal evolution has rendered this test a phantom doctrine.

---

[6] See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich L Rev 561, 567–70 (2009).

I. A STUDY OF THE SUBJECTIVE-EXPECTATIONS TEST

To understand the subjective-expectations test, a study was conducted of every case that applied *Katz* in 2012 available in Westlaw's ALLCASES database.[7] The study began with case law that included the phrases "expectation of privacy" and "Fourth Amendment," which yielded 1,131 cases. Those cases were then read and reduced to a dataset of 540 cases that applied the *Katz* expectation-of-privacy test.

The study focused on three primary questions: First, when courts discuss the *Katz* test, how often do they mention both the subjective and objective tests? Second, when courts actually apply the *Katz* test, how often do they apply the subjective test? Third, when they apply the subjective test, how often is it outcome determinative?

A. Mentioning the Subjective and Objective Tests

Every case in the dataset was first coded for whether it mentioned the subjective test, the objective test, or both. The focus at this stage was on how the authoring judge articulated the *Katz* test. A case was deemed to have mentioned the subjective test if it used the word "subjective" at any point in describing or applying the expectation-of-privacy inquiry. A case was deemed to have mentioned the objective test if it used the words "objective," "reasonable," or "legitimate" in describing the applicable doctrine.

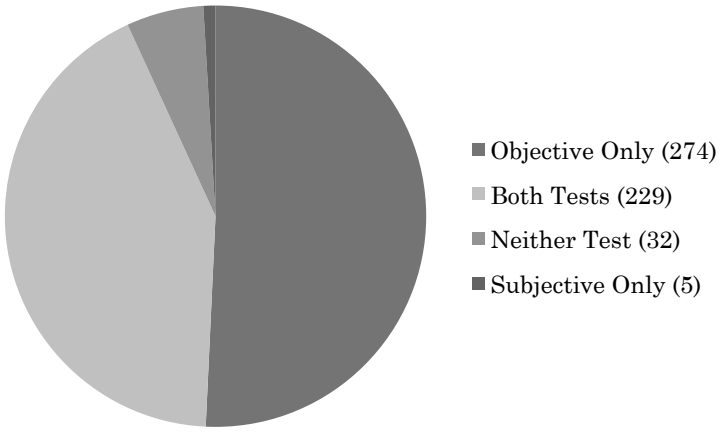
The results indicate that a slight majority of *Katz* applications, 57 percent (306/540), did not mention the subjective test. In contrast, the objective test was mentioned in 93 percent of cases (503/540). Six percent of *Katz* applications (32/540) mentioned neither the objective nor subjective tests; in most of these instances, the court merely referred to an "expectation of privacy" generally, without more detail.[8] In five cases, 1 percent of the total, the court mentioned the subjective test but not the objective test. Figure 1 summarizes the breakdown of cases mentioning or not mentioning the subjective and objective parts of the *Katz* test.

---

[7] The calendar year 2012 was selected because it was the last complete year in the database at the time that the study began.

[8] It generally appeared that these cases applied the objective test, although they did not use the labels associated with the objective test—"reasonable," "objective," or "legitimate."

FIGURE 1. MENTIONING THE SUBJECTIVE AND OBJECTIVE TESTS



B. Applying the Subjective and Objective Tests

The study next considered how opinions applied the subjective and objective tests. The focus here was the court's expression of a legal conclusion about whether a subjective or objective expectation of privacy had been established under *Katz*.[9]

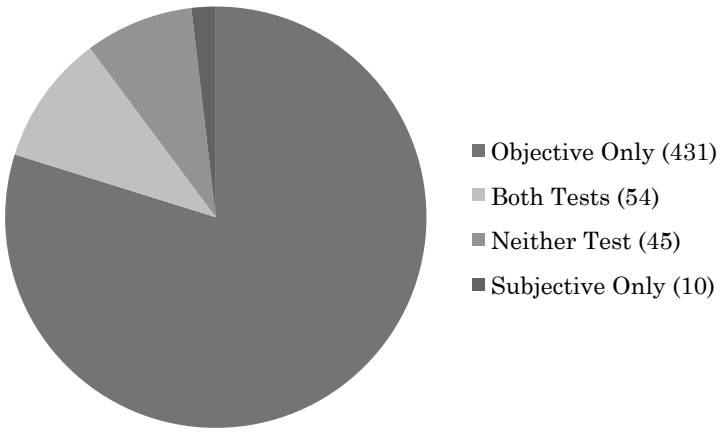
In 80 percent of the cases (431/540), the court applied only the objective test and did not apply the subjective test. In another 10 percent of the cases (54/540), the court applied both the subjective and objective tests. In 8 percent of the cases (45/540), the court applied neither test; in these instances, the court usually collapsed *Katz* into a generalized inquiry of privacy expectations. Finally, in 2 percent of the cases (10/540), the court applied only the subjective test and not the objective test. These results are summarized in Figure 2 below. The 45 cases that applied neither test did not specify either an objective or subjective test. Many simply described the test as whether the defendant had an "expectation of privacy."[10] As a practical matter, those

[9] The focus on conclusions rather than analysis made the coding simpler but also introduced the possibility of typographical errors altering the data. This problem is discussed below. See Part I.C.

[10] See, for example, *State v Grice*, 735 SE2d 354, 359 (NC App 2012); *State v Gardner*, 984 NE2d 1025, 1028 (Ohio 2012); *McMillan v Stoll*, 2012 WL 707117, *3 (ND Ill).

cases appear to have applied the objective test but not used the specific words "objective," "reasonable," or "legitimate."

FIGURE 2. APPLYING THE SUBJECTIVE AND OBJECTIVE TESTS



In short, courts applied the subjective-expectation-of-privacy test only rarely. In roughly nine out of ten cases, courts applied *Katz* without even considering whether the defendant had satisfied the subjective test.

C. Outcomes of Applying the Tests

The study's final inquiry considered how courts applied the subjective and objective tests in the subset of cases that ultimately ruled that a search had or had not occurred under the *Katz* test.[11] Here the dataset was limited to the cases that clearly applied either or both of the tests and reached a result as to whether a search had occurred.[12] Within that dataset, 103 cases ruled that a search had occurred and 392 ruled that no search had occurred.

Within the subset of the 103 cases ruling that a search had occurred, 83 percent (86/103) applied only the objective test, found that it was satisfied, and did not reach the subjective test. By contrast, 16 percent (16/103) applied both tests and found

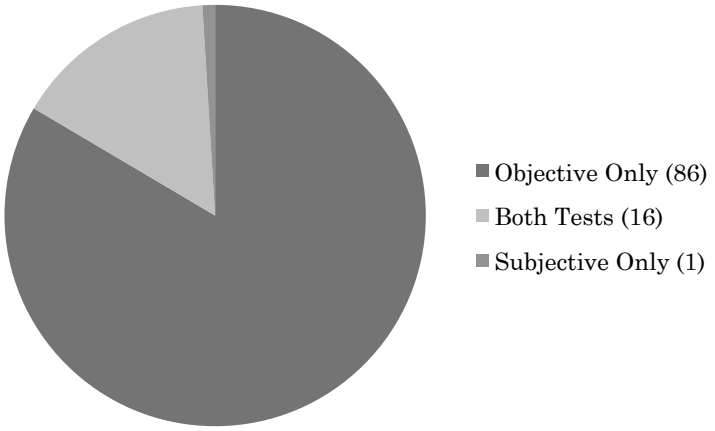
---

[11] Applications of the trespass test introduced during the study period in *Jones*, 132 S Ct at 950–51, were not included.

[12] This dataset thus excluded the forty-five cases that did not clearly apply either a subjective or objective test.

them both satisfied. Further, 1 percent (1/103) applied only the subjective test, found that it was satisfied, and did not reach the objective test. These results are summarized in Figure 3.

FIGURE 3. TESTS APPLIED WHEN A SEARCH OCCURRED



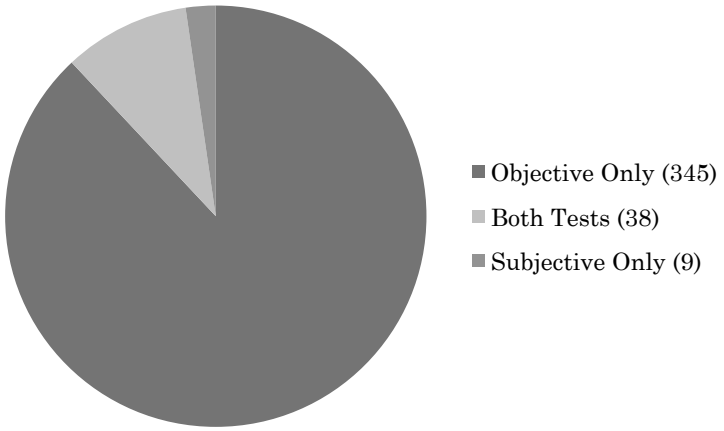
This is a striking result. The *Katz* test requires that the individual satisfy both the subjective and objective tests before a search will be found. When the objective test was satisfied, however, courts normally did not even consider the subjective test before announcing that a search had occurred. Further, the one case coded as applying only the subjective test before ruling that a search had occurred likely did so due only to a typographical error.[13]

In the subset of the 392 cases ruling that no search had occurred under *Katz*, 88 percent (345/392) applied only the objective test, found that it was not satisfied, and did not reach the subjective test. Ten percent (38/392) applied both tests. Further, in 2 percent of the cases (9/392), the court applied only the

[13] See *State v Hayes*, 809 NW2d 309, 314–15 (ND 2012) (considering whether the defendant had standing to challenge a home search). Under *Rakas v Illinois*, 439 US 128 (1978), the standing inquiry is answered by the *Katz* test. See id at 143 (relying on *Katz* to define the scope of the interest protected by the Fourth Amendment). *Hayes* concluded that, because the deed to the house was in the defendant's name, she paid the home's property taxes, and she used to live there, "she enjoyed a subjective expectation of privacy in [the house], and as a result, she has standing to contest the warrantless search." *Hayes*, 809 NW2d at 315. The court presumably meant to say that Hayes enjoyed an objective expectation of privacy, not a subjective expectation of privacy.

subjective test, found that it was not satisfied, and did not reach the objective test. These results are summarized in Figure 4.

FIGURE 4. TESTS APPLIED WHEN NO SEARCH OCCURRED



It is helpful to look more closely at two subsets of cases depicted in Figure 4. The first subset consists of the thirty-eight cases in which courts applied both tests and ruled that no search had occurred. Within this subset, twenty-eight cases held that there was neither a subjective nor an objective expectation of privacy. The subjective test did not change the outcome in these cases because the result for subjective and objective expectations was the same. In the remaining ten cases, the court held that there was a subjective expectation of privacy but not a reasonable expectation of privacy. Because the absence of a reasonable expectation of privacy doomed the effort to establish a search, subjective expectations played no role in the ultimate outcome. Finally, zero cases held that there was a reasonable expectation of privacy but no subjective expectation of privacy. These would have been cases in which the subjective test controlled outcomes. No such cases were found.

The final subset consists of the nine cases that applied the subjective test, ruled that no search had occurred, and did not reach the objective inquiry. Of the nine cases, four involved identical passages from pro se prisoner cases in one district that misquoted a controlling Supreme Court case to state its conclusion

as a subjective inquiry instead of an objective inquiry.[14] Two of the cases involved computers voluntarily shared with third parties; in those cases, the courts found that no Fourth Amendment rights had been violated after relying on a mix of subjective and objective arguments.[15] In one case, the court's phrasing of the test as subjective was likely an error; the court applied precedents and concepts of the objective test before stating the outcome as an application of the subjective test.[16] Finally, the last two cases held that an individual lacked a subjective expectation of privacy in factual contexts in which courts routinely hold that individuals lacked an objective expectation of privacy or consented to the search.[17]

---

[14] See *Strange v Kentucky*, 2012 WL 3637646, *4 (WD Ky); *Higgs v Easterling*, 2012 WL 692610, *10 (WD Ky); *Patton v Kentucky*, 2012 WL 3096618, *3 (WD Ky); *Tramber v Bolton*, 2012 WL 2912265, *2 (WD Ky). Each of these cases contains an identical passage relying on *Hudson v Palmer*, 468 US 517 (1984), for the view that an inmate lacks Fourth Amendment rights in his prison cell. The relevant passage in *Hudson* exclusively concerns the reasonable-expectation-of-privacy test. See id at 525–26 ("[W]e hold that society is not prepared to recognize as legitimate any subjective expectation of privacy that a prisoner might have in his prison cell and that, accordingly, the Fourth Amendment proscription against unreasonable searches does not apply within the confines of the prison cell."). The common passage in the four opinions misleadingly uses ellipses to create the impression that *Hudson* was based on the subjective-expectations test. See, for example, *Strange*, 2012 WL 3637646 at *4, quoting *Hudson*, 468 US at 526 (claiming that *Hudson* held that "a prisoner does not possess 'any subjective expectation of privacy . . . in his prison cell'"). The error was presumably inadvertent.

[15] The first decision, *United States v Coates*, 462 Fed Appx 199 (3d Cir 2012), was difficult to code. The defendant invited a police officer to look at his phone to see threatening texts that he had received. Id at 201. The officer testified that, while attempting to manipulate the cell phone and simultaneously keep his attention on the defendant, he inadvertently found child pornography on the phone. Id. The court held that the defendant waived his privacy rights by inviting the officer to look through his phone. Id at 203–04. The opinion does not make clear whether it was decided under the subjective test, the objective test, or consent doctrine. It arguably invokes all three. See id at 203 (describing in detail the defendant's conduct and concluding that his behavior was not characteristic of "an individual expecting to maintain privacy"). However, it was coded as resting primarily on the subjective test.

In *United States v Meister*, 2012 WL 252447 (MD Fla), the defendant left his computer at a shop to be repaired and approved a transfer of files from one computer to another. Id at *1. During the transfer, the computer-repair employee observed child pornography. Id. The court held that the defendant lacked a subjective expectation of privacy in the files and also suggested, without so holding, that there was no reasonable expectation of privacy. See id at *6–7.

[16] See *United States v Pittman-Wright*, 2012 WL 1815599, *11–12 (ND Cal).

[17] See *Bordley v State*, 46 A3d 1204, 1208, 1214–18 (Md App 2012) (holding that an individual locked out of his hotel room lacked a subjective expectation of privacy in the room, but relying on case law interpreting the reasonable-expectation-of-privacy test); *Evans v Skolnik*, 2012 WL 760902, *2–3 (D Nev) (holding that a defendant who was recorded on prison phones while speaking with his lawyer lacked a subjective expectation of privacy in the conversation). *Evans* is puzzling because the analysis is very brief and

D. *Katz* Is a One-Step Test

The results of the study suggest that the subjective prong of *Katz* is irrelevant. A majority of cases applying *Katz* did not mention subjective expectations. Only 12 percent of *Katz* cases purported to apply the subjective test.[18] Only 2 percent of *Katz* cases claimed to hinge their analysis on the subjective test.[19] And in each of those cases in the study, the court's reliance on subjective expectations appeared to be a mistake or at least a result that courts could otherwise express using the objective part of *Katz*. The hunt for a case that relied on the subjective test in an outcome-determinative way came up empty. Based on the cases analyzed in the study, subjective expectations appear to play no outcome-determinative role.

II. HOW THE OBJECTIVE TEST CAME TO DISPLACE THE SUBJECTIVE TEST

We are left with the puzzle of why the Supreme Court would adopt a doctrinal test that makes no difference in outcomes. Why bother? This Part argues that the answer lies in a post-*Katz* shift in Fourth Amendment doctrine. At the time of *Katz*, the subjective and objective tests each had a significant and independent purpose: the objective test addressed what spaces could receive Fourth Amendment protection, and the subjective test considered whether an individual had waived his privacy rights in an otherwise-covered space by inviting outsiders to observe him. To establish Fourth Amendment protection, the individual needed to show both that the government invaded a protected space under the objective test and that the space was not open to outsiders under the subjective test.

This original meaning of the two-part test was difficult to parse, however, and later decisions failed to appreciate it. Instead, later decisions addressed both of theses inquiries under the objective test. The expansion of the objective test displaced the subjective test. The subjective test is irrelevant today because the objective prong of the test now does the work originally

---

relies on a record not explained in the opinion. However, prison phones are ordinarily monitored, and the notice of monitoring establishes consent even for attorney-client communications. See *United States v Novak*, 531 F3d 99, 103 (1st Cir 2008) (O'Connor sitting by designation).

[18] See Figure 2.

[19] See Figure 2.

intended for the subjective test. The two inquiries collapsed into one. Understanding this shift requires a close study of Justice Harlan's concurrence in *Katz*, followed by a brief analysis of post-*Katz* doctrine.

A. The Original Understanding of the Subjective-Expectations Test

To understand the changing role of the subjective test, we need to start with a close reading of the concurring opinion in *Katz* that introduced it. The *Katz* majority ruled that using a microphone taped to a phone booth to listen in on a target's call was a Fourth Amendment search requiring a warrant.[20] The cryptic reasoning of the majority opinion inspired Harlan to add a brief concurrence.[21] Although Harlan wrote only for himself, his opinion deserves close scrutiny because a majority of the Court later adopted his formulation.[22]

Harlan began by summarizing his understanding of the majority's reasoning. First, he understood the majority opinion to hold "that an enclosed telephone booth is an area where, like a home, *Weeks v. United States*, 232 U.S. 383, and unlike a field, *Hester v. United States*, 265 U.S. 57, a person has a constitutionally protected reasonable expectation of privacy."[23] Harlan then addressed the broader question of how to know when a person has Fourth Amendment rights in a particular place. He explained his test in three sentences:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy

---

20 *Katz*, 389 US at 353.

21 See id at 361 (Harlan concurring).

22 See *Smith v Maryland*, 442 US 735, 740 (1979).

23 *Katz*, 389 US at 360 (Harlan concurring).

> under the circumstances would be unreasonable. Cf. *Hester v. United States*.[24]

Each sentence plays a specific role. The first articulates the two-part inquiry; the second explains the subjective test; and the third explains the objective test.

It is challenging to identify precisely what Harlan intended the subjective test to mean for two reasons. First, Harlan announced the test but cited no authority for it. Second, the language that Harlan used to express the subjective test can be interpreted in multiple ways. Focusing on the words "actual (subjective) expectation" and "intention" might suggest that the test requires a person to actually anticipate privacy. On the other hand, focusing on the words "exhibited" and "exposes" might suggest that the test requires a person to hide his private spaces from outsiders. The former interpretation focuses on thoughts, while the latter focuses on deeds.

We can solve this puzzle by starting with a critical clue: Harlan expressed the test as an "understanding of the rule that has emerged from prior decisions."[25] Taking Harlan at his word, he did not intend to create a new test from whole cloth. Instead, he was synthesizing case law existing at the time of *Katz*. The state of Fourth Amendment case law in 1967 can help fill in the missing context and explain the subjective test.

In 1967, there were two distinct lines of cases on what constituted a Fourth Amendment search. The first group consisted of the protected-area cases, which identified the spaces that could receive Fourth Amendment protection. Insides of homes could receive protection,[26] for example, while conversations in open fields could not.[27] *Katz* itself was a protected-area case. Harlan read the majority opinion as classifying a phone booth as a space that could receive Fourth Amendment protection like a home and unlike a field.[28]

The second set of cases involved voluntary exposure of protected spaces. In these cases, government agents observed areas

---

[24] Id at 361 (Harlan concurring).

[25] Id (Harlan concurring).

[26] See, for example, *Silverman v United States*, 365 US 505, 511–12 (1961) (holding that use of a "spike mike" touching the wall of a home violated the Fourth Amendment because "at the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion").

[27] See, for example, *Hester v United States*, 265 US 57, 59 (1924).

[28] See *Katz*, 389 US at 360 (Harlan concurring).

that normally would receive Fourth Amendment protection under the protected-area cases. However, the agents observed those areas either by invitation or in contexts in which the area was exposed to public view. The key question was whether the exposure relinquished Fourth Amendment protection.

Several of the voluntary-exposure cases had considered the use of "secret agents."[29] In those cases, criminals had admitted undercover agents or informants into their homes, offices, and hotel rooms and willingly shared information with them about their crimes on the assumption that the guests would not betray their trust.[30] The Court had uniformly held that no search occurred because a person who exposed his space to an agent had voluntarily relinquished Fourth Amendment protection.[31] Notably, the secret-agent cases were fresh at the time of *Katz*. The Court had decided three such cases in the immediately preceding Term,[32] and Harlan himself had authored a decision reaffirming the use of secret agents to record private conversations just a few years earlier.[33]

Although *Katz* was a protected-area case, the government's brief in *Katz* reminded the justices of the voluntary-exposure cases. A footnote in the brief explained that "not all observations of matters occurring in a 'constitutionally protected area' are prohibited by the Fourth Amendment."[34] The government cited two cases for support. First, in *United States v Lee*,[35] the Court had "found no illegal search where cases of liquor were observed in plain view on the open deck of a boat."[36] Second, in *McDonald v United States*,[37] the Court had "apparently found no illegal search in the observations made by police officers who peeked

---

29 See Note, *Judicial Control of Secret Agents*, 76 Yale L J 994, 995 (1967).

30 See, for example, *Hoffa v United States*, 385 US 293, 302 (1966); *Lewis v United States*, 385 US 206, 210–11 (1966); *Osborn v United States*, 385 US 323, 325–27 (1966); *Lopez v United States*, 373 US 427, 438–39 (1963); *On Lee v United States*, 343 US 747, 749 (1952).

31 See, for example, *Lewis*, 385 US at 211.

32 See generally *Hoffa*, 385 US 293; *Lewis*, 385 US 206; *Osborn*, 385 US 323.

33 See *Lopez*, 373 US at 439 ("[T]he risk that petitioner took in offering a bribe to [a secret agent] fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording.").

34 Brief for the Respondent, *Katz v United States*, Docket No 35, *14 n 6 (US filed Sept 22, 1967) (available on Westlaw at 1967 WL 113606) ("Government Brief").

35 274 US 559 (1927).

36 Government Brief at *14 n 6 (cited in note 34). See also *Lee*, 274 US at 563 ("[The] search, if any, of the motorboat at sea did not violate the Constitution . . . . But no search on the high seas is shown.").

37 335 US 451 (1948).

through an open transom" in a hotel room.[38] As described in the government's brief, these cases echo the basic principle of the secret-agent cases: the government does not commit a search when an agent observes matters inside a protected area that has been exposed to outside observation.[39]

The two lines of search cases explain Harlan's two-part test. The objective test summarized the protected-area cases, and the subjective test summarized the voluntary-exposure cases. As originally intended, the two parts of Harlan's test each did independent work. The objective test asked whether the nature of the space invaded by the government was one that society was willing to recognize as private. On the other hand, the subjective test asked whether the individual took steps to make objectively protected spaces open to outside observation and thus yielded privacy rights against that invited observation. For a Fourth Amendment search to occur, a government agent had to observe a space protected under the protected-area cases without exposure or invitation.

From this perspective, the subjective test from Harlan's concurrence simply restated the following passage from the *Katz* majority opinion:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. See *Lewis v. United States*, 385 U.S. 206, 210; *United States v. Lee*, 274 U.S. 559, 563. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[40]

This passage expresses the subjective inquiry as an exposure test. The *Katz* majority cited two cases as authority: *Lewis v United States*,[41] one of the secret-agent cases; and *Lee*, the case involving the plain view of contraband on a boat that the government cited in its brief.[42] Harlan's subjective test tracks the

---

[38] Government Brief at *14 n 6 (cited in note 34), citing *McDonald*, 335 US at 455, 458.

[39] See Government Brief at *14 n 6 (cited in note 34) (noting that the petitioner could not object to testimony based on what an agent "overheard by the 'naked ear' while lawfully in the hotel room immediately next door"). See also *Lewis*, 385 US at 211 ("But when, as here, the home is converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business, that business is entitled to no greater sanctity than if it were carried on in a store, a garage, a car, or on the street.").

[40] *Katz*, 389 US at 351–52.

[41] 385 US 206 (1966).

[42] See Government Brief at *14 n 6 (cited in note 34).

same concept. Harlan's opinion just lacks the citations to the exposure and secret-agent case law to make the reference clear.[43]

This perspective suggests that what we call the "subjective" part of *Katz* was not intended to be about actual subjective expectations. Contrary to the label, the test does not evaluate an individual's prediction of what will happen next.[44] Rather, the subjective test focuses on whether the individual took steps that "exhibited" an expectation of privacy—that is, whether the individual took objective measures to block the public or government from observing the information at issue.[45] In this way, the subjective test is akin to a consent doctrine. Whereas people normally have Fourth Amendment rights in their private spaces, they give up those rights when they consent to have others enter their private spaces and observe what occurs inside. Charlie Katz satisfied this part of the test because he entered the phone booth and closed the door behind him to place the call.[46] Closing the door blocked normal efforts to overhear the conversation, exhibiting a plan to keep the phone booth a private space for the duration of the call.[47]

B. Post-*Katz*: The Supreme Court Recasts the Subjective Inquiry as Part of the Objective Test

Although we can now appreciate the connection between the subjective test and the Court's exposure cases, that link is admittedly difficult to see absent a close study of the relevant history and context. Nor was it clear when *Katz* was freshly decided. Some contemporaneous interpretations of Harlan's subjective test suggested the connection, but others did not.[48]

---

43 That missing link may be found in Harlan's dissent in *United States v White*, 401 US 745 (1971). In *White*, Harlan announced a new approach that went beyond "the search for subjective expectations" and would overturn the secret-agent cases. Id at 786 (Harlan dissenting). Harlan rejected reliance on subjective expectations in *White* because he had concluded that a warrant was needed even when a person voluntarily exposed his conversations to an undercover agent. See id at 785–87 (Harlan dissenting). Harlan's *White* dissent thus directly links the subjective test and the secret-agent cases.

44 This is not a novel observation. See, for example, Wayne R. LaFave, 1 *Search and Seizure: A Treatise on the Fourth Amendment* § 2.1(c) at 583 n 95 (West 5th ed 2012), quoting Eric Dean Bender, Note, *The Fourth Amendment in the Age of Aerial Surveillance: Curtains for the Curtilage?*, 60 NYU L Rev 725, 743–44 (1985).

45 LaFave, 1 *Search and Seizure* at § 2.1(c) at 583 n 95 (cited in note 44).

46 See *Katz*, 389 US at 352.

47 See id. See also id at 361 (Harlan concurring).

48 Compare Note, *From Private Places to Personal Privacy: A Post-*Katz *Study of Fourth Amendment Protection*, 43 NYU L Rev 968, 982–83 & n 89 (1968) (suggesting the

And most importantly, when later Supreme Court majorities adopted Harlan's formulation, they did so without looking carefully at the nature of the subjective test. Those opinions simply assumed that the subjective test was genuinely subjective. They assumed that the subjective test asks whether the individual actually expected his information to remain private.[49]

The result was a subtle but important doctrinal shift. When the Court considered how the Fourth Amendment applied to secret agents and exposed spaces after *Katz*, opinions failed to recognize that such questions were supposed to be resolved under the subjective test. Instead, the Court analyzed these problems under the objective test. The switch appears inadvertent rather than deliberate. But its effect was to expand the objective test and displace the terrain that originally would have been covered by the subjective test.

Three cases show the evolution: *United States v White*,[50] *Smith v Maryland*,[51] and *Maryland v Macon*.[52] The shift began with *White*, a post-*Katz*, secret-agent case involving a criminal who divulged his crimes to an informant wearing a recording device.[53] In his controlling plurality opinion, Justice Byron White rearranged the roles of the subjective and objective tests. To Justice White, the subjective inquiry considered "actual expectations" of whether individuals "know [or] suspect that their colleagues have gone or will go to the police."[54] So construed, criminals must have an actual expectation of privacy in their conversations about their crimes: "Otherwise, conversation would cease and our problem with these encounters would be nonexistent or far different from those now before us."[55] Justice White instead construed the problem of secret agents as a question of "what expectations of privacy are constitutionally justifiable"[56]—that is, what was reasonable under the objective test. White concluded that an actual expectation that a person will

link), with *United States v Grogan*, 293 F Supp 45, 47 (MD Ala 1968) (not suggesting the link).

49 See notes 53–65, 67, and accompanying text.

50 401 US 745 (1971).

51 442 US 735 (1979).

52 472 US 463 (1985).

53 *White*, 401 US at 746–47 (White) (plurality). The Court had not yet adopted Harlan's two-part formulation at the time of *White*. The Court would not do so definitively until *Smith*, eight years later. See *Smith*, 442 US at 740.

54 *White*, 401 US at 751–52 (White) (plurality).

55 Id (White) (plurality).

56 Id at 752 (White) (plurality) (quotation marks omitted).

not be recorded is not constitutionally justifiable because a person always assumes the risk that he is speaking with someone who will report the conversation to the police.[57]

The Court echoed this new understanding of the subjective test in *Smith*, which considered whether installation of a pen register at the phone company in order to record numbers dialed from a suspect's home phone constituted a search.[58] The majority assumed that the subjective test measured what a person actually expected. "Although subjective expectations cannot be scientifically gauged," the *Smith* Court explained, "it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[59] Telephone users "typically know" that the numbers that they dial are conveyed to the phone company.[60] Despite these ruminations, the Court ultimately assumed that the defendant subjectively expected privacy and applied the objective test instead.[61] Relying on the secret-agent cases, including *White*, *Smith* held that a person had no legitimate expectation of privacy in information voluntarily turned over to third parties.[62] By disclosing information to the phone company, a telephone user assumed the risk that the phone company would disclose the information to the police.[63]

Macon completed the transition. An undercover agent entered a bookstore, browsed, and purchased two obscene magazines.[64] The question in the case was whether entering the store and observing the magazines constituted a search of the store.[65] Under the secret-agent cases, the answer would be "no" because the store had invited the public inside to browse. In the language of Harlan's *Katz* concurrence, the store had "expose[d]" its contents "to the 'plain view' of outsiders" and thus failed to exhibit an actual expectation of privacy.[66] *Macon* reached the same result by applying the objective test instead. Although the store owner might have actually expected that the authorities would

---

57 Id (White) (plurality).
58 *Smith*, 442 US at 736.
59 Id at 743.
60 Id.
61 See id at 743–44.
62 *Smith*, 442 US at 743–44.
63 See id at 744–45.
64 *Macon*, 472 US at 465.
65 Id at 467–69.
66 *Katz*, 389 US at 361 (Harlan concurring).

not learn about the obscene magazines for sale, the opinion reasoned, that expectation was not reasonable when "the public was invited to enter and to transact business."[67]

These cases reveal a dramatic shift in the Court's understanding of the subjective test. In Harlan's original formulation, a person who shared his information or space with others failed to exhibit an actual expectation of privacy. Observation by a government agent in these circumstances was not a search because the defendant failed the subjective test. In *White*, *Smith*, and *Macon*, however, the Court adopted a purely subjective understanding of the subjective test. The subjective inquiry came to rest on whether a person actually anticipated privacy, which can be answered only by going inside the person's mind. Whether government observation of shared information or space constitutes a search became an interpretation of the objective test, specifically the so-called third-party doctrine.[68]

To be clear, not every Supreme Court case applying *Katz* adopts the purely subjective interpretation of the subjective test. Some suggest a purely subjective approach,[69] while others seem more true to Harlan's original formulation.[70] Nonetheless, cases such as *White*, *Smith*, and *Macon* effectively merged the original focus of the subjective test with the objective test.

C. The Doctrinal Shift Makes the Subjective Test a Phantom Doctrine

The Court's doctrinal move rendered the subjective test irrelevant in two ways, which reflect the two prevailing understandings of the subjective test in the lower courts. Most lower courts recite the purely subjective version of the subjective test found in *White*, *Smith*, and *Macon*.[71] On the other hand, a minority of lower courts use Harlan's original formulation.[72] In the cases from 2012 discussed in Part I, courts applying the subjective test described it as requiring a person to "exhibit" or

---

67 *Macon*, 472 US at 469.

68 See Kerr, 107 Mich L Rev at 588–90 (cited in note 6). In that article, I argued that the Court should have viewed third-party disclosure as a question of consent. See id. I now see that the proper way to frame this consent principle within *Katz* is through the subjective prong of the test.

69 See, for example, *Safford Unified School District No 1 v Redding*, 557 US 364, 374–75 (2009); *California v Greenwood*, 486 US 35, 39–40 (1988).

70 See, for example, *Bond v United States*, 529 US 334, 338 (2000).

71 See Part II.B.

72 See Part II.B.

"manifest" an expectation of privacy in only 19 percent of the cases (12/64). In contrast, courts described the subjective test using the purely subjective standard in 81 percent of the cases (52/64).[73]

Under either understanding, however, the subjective test is irrelevant. When lower courts apply the subjective test using the original "exhibition" formulation, they end up repeating the same inquiry under both tests. Under precedents such as *White*, *Smith*, and *Macon*, the exhibition requirement is now part of the objective inquiry. A person who does not exhibit a subjective expectation of privacy necessarily has no reasonable expectation of privacy either. In that case, the subjective test cannot alter outcomes because the same analysis occurs under both tests.

When courts interpret the subjective test using the purely subjective understanding, the test becomes irrelevant in a different way. At first blush, it might seem that a test precluding Fourth Amendment protection when a search is anticipated would exert a powerful influence on outcomes. But such an understanding turns the subjective test into an absurdity. Professor Anthony Amsterdam pointed out this problem shortly after *White* was decided:

> An actual, subjective expectation of privacy obviously has no place . . . in a theory of what the fourth amendment protects. It can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection. If it could, the government could diminish each person's subjective expectation of privacy merely by announcing half-hourly on television that 1984 was being advanced by a decade and that we were all forthwith being placed under comprehensive electronic surveillance.[74]

---

[73] Identifying whether a court applied the subjective test using the original understanding of Harlan's formulation or using the *White-Smith* notion of actually expecting privacy is a difficult judgment call and often impossible to make with confidence. An application was coded as applying a subjective standard if it described the test as requiring a person to "have," "show," "demonstrate," "harbor," "profess," or "evince" a subjective expectation of privacy. An application was coded as applying the original Harlan formulation if the court described the test as requiring the individual to exhibit or manifest a subjective expectation of privacy.

[74] Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn L Rev 349, 384 (1974).

If the subjective test is truly subjective, then Amsterdam is surely right. A purely subjective standard would let the fox guard the constitutional henhouse.

The Supreme Court responded to this problem by indicating that the subjective inquiry should be suspended when it would produce such undesirable results. Recall that *Smith* adopted the purely subjective view of the subjective test.[75] In a footnote, *Smith* instructed that "of course" the subjective test should not be considered in some cases.[76] If the government announced that warrantless home searches would shortly commence, or refugees from totalitarian countries expected the government to tap their phones, individuals would not subjectively expect privacy but would still deserve Fourth Amendment protection:

> In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.[77]

Pause to appreciate the irony. After *Smith* misconstrues the subjective test to ask a purely subjective question, the footnote announces that the subjective test should be ignored in precisely those cases in which the misconstrued test would make a difference.[78]

The Court arguably went further in a footnote in *Hudson v Palmer*,[79] a subsequent case holding that inmates cannot establish Fourth Amendment rights in prison cells.[80] Citing the plurality and dissenting opinions in *White*, the Court noted in *Hudson* that it had "always emphasized" the objective test instead of the subjective test.[81] *Hudson* construed this emphasis as

---

75 See notes 58–63.

76 *Smith*, 442 US at 740 n 5.

77 Id.

78 The papers at the Library of Congress of *Smith*'s author, Justice Harry Blackmun, indicate that this footnote was added at the request of Justice John Paul Stevens. See Library of Congress Manuscript Division, *Harry A. Blackmun Papers, 1913–2001*, Supreme Court File, 1918–1999, Case File 1970–1994, Box 297, 78-5374 at 35–42.

79 468 US 517 (1984).

80 Id at 526.

81 Id at 525 n 7, citing *White*, 401 US at 751–52 (White) (plurality) and *White*, 401 US at 768, 786 (Harlan dissenting).

a "refusal to adopt a test of 'subjective expectation'"—a refusal that it described as "understandable" because "constitutional rights are generally not defined by the subjective intent of those asserting the rights."[82] "The problems inherent in such a standard are self-evident," the Court wrote, citing the footnote in *Smith* discussed above.[83]

The *Smith* and *Hudson* footnotes explain why lower courts ignore the subjective test in its purely subjective form. Because *Katz* requires an individual to satisfy both tests, the subjective test can impact outcomes only when an individual has established a reasonable expectation of privacy but the evidence shows that he subjectively did not expect privacy. But those are precisely the circumstances in which the *Smith* and *Hudson* footnotes direct courts to ignore the subjective test.

In sum, the evolution of Supreme Court doctrine has rendered the subjective test pointless under both the original and the purely subjective understandings. When courts use the original understanding of the subjective test, it becomes irrelevant because it merely repeats work now done by the objective test. And when courts use the purely subjective understanding, the test becomes irrelevant because the Supreme Court has directed courts to ignore the test when it would actually make a difference. Either way, the subjective test cannot alter outcomes. No wonder most lower courts ignore it.

CONCLUSION

Although the Supreme Court says that *Katz* is a two-part test, the subjective prong has become a phantom doctrine. Most opinions applying *Katz* do not mention it; opinions that mention the test usually do not apply it; and when courts apply it, the test makes no difference to outcomes. As a practical matter, the *Katz* test is only one step. The objective test is the only one that matters.

The Supreme Court's own case law has caused this strange result. As originally crafted by Justice Harlan, the subjective test did important and independent work. But later decisions of the Court misunderstood Harlan's test and merged the work of the subjective test into the objective test. That shift has left the subjective test with no work to do and no outcomes to change.

---

[82] *Hudson*, 468 US at 525 n 7 (citations omitted).

[83] Id, citing *Smith*, 442 US at 740–41 n 5.

The sensible resolution is for the Supreme Court to formally abolish the subjective test. Its existence on paper merely causes confusion. At first blush, the phrase "subjective expectations of privacy" sounds like it must hinge on the privacy that individuals actually anticipate. The phrase tricks the unwary into thinking that Fourth Amendment protection hinges on predictions. But it does not, and it should not. *Katz* instead rests solely on the scope of legitimate expectations of privacy. It is a normative inquiry that subjective expectations do not and should not answer.

The Questionable Objectivity of Fourth Amendment Law

Orin S. Kerr*

The Supreme Court often insists that Fourth Amendment rules must be objective. The doctrine should focus on what police officers do, not what they are thinking when they do it. Recently, however, Fourth Amendment law's objective façade has begun to crack. In a series of cases, the Supreme Court has introduced subjective tests. Fourth Amendment law is now best understood as a complex mix of subjective and objective tests. The Justices have not offered a clear explanation for why they use objective rules in some cases and subjective rules in others. But it should be clear that the Justices are making a choice, and that both subjective and objective approaches are in play.

This Article identifies the Supreme Court's recent turn to subjective rules and offers a normative framework for the choice between subjective and objective tests in Fourth Amendment law. It begins by reviewing existing caselaw and showing how it often hinges on an officer's subjective state of mind. The Article then offers a framework for choosing between objective and subjective tests. Subjective approaches can permit courts to craft narrower rules that better distinguish harmful from beneficial police practices. But the benefits of subjectivity depend on whether harms track subjectivity and whether states of mind can be determined reliably. To best achieve the aims of Fourth Amendment law, courts should consider in each context the civil liberties benefit of narrowing doctrine in light of the risk that a subjective test will be misapplied.

* Professor, University of California, Berkeley School of Law. The author thanks Daniel Epps, Richard Re, Eric Miller, and the faculty workshop at Loyola-L.A. law school for helpful comments on an earlier draft.

Introduction

The Supreme Court often insists that Fourth Amendment rules must be objective.[1] What an officer thinks is irrelevant.[2] Instead, the legality of government action depends on what the officer actually does.[3] The best-known example is the Court's blessing of pretextual traffic stops in *Whren v. United States*.[4] As long as an officer has probable cause that a traffic law was violated, *Whren* tells us, stopping the car is constitutionally reasonable. An

1. *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 404 (2006) ("An action is 'reasonable' under the Fourth Amendment, regardless of the individual officer's state of mind, 'as long as the circumstances, viewed *objectively*, justify [the] action.'" (emphasis in original) (quoting Scott v. United States, 436 U.S. 128, 138 (1978))).

2. *Id.* ("The officer's subjective motivation is irrelevant."); Bond v. United States, 529 U.S. 334, 338 n.2 (2000) ("The parties properly agree that the subjective intent of the law enforcement officer is irrelevant in determining whether that officer's actions violate the Fourth Amendment.").

3. *Bond*, 529 U.S. at 338 n.2 ("[T]he issue is not his state of mind, but the objective effect of his actions.").

4. 517 U.S. 806 (1996) (Scalia, J.).

officer's real reason for making the stop must "play no role" in the Fourth Amendment analysis.[5]

Whren's directive to ignore officer intent has been repeated in many Supreme Court Fourth Amendment cases.[6] Consider a few examples: To decide if an emergency justified an officer breaking into a house, courts must ask if the objective facts of the emergency justified the entry instead of whether the officer was actually trying to help stop it.[7] When considering whether an officer's inspection of a duffel bag violated the Fourth Amendment, it doesn't matter what the officer was trying to find.[8] With just two limited exceptions, the Court has explained, Fourth Amendment law should not consider an officer's subjective state of mind.[9]

That's what the Supreme Court says. But is it true?

This Article's first goal is to show that the objectivity of Fourth Amendment doctrine is weaker than the Court has acknowledged. Reliance on an officer's subjective thoughts is sprinkled throughout Fourth Amendment doctrine.[10] An officer's state of mind matters for what is a search, what is a seizure, state action, several standards for when a search or seizure is reasonable, and Fourth Amendment remedies.[11] Subjective tests have been adopted with particular frequency in the last decade, including in several cases by the author of *Whren*, the late Justice Antonin Scalia.[12] Fourth Amendment law retains its objective façade. The courts repeat it, and law students dutifully learn it. But viewed as a whole, Fourth Amendment law increasingly offers a mix of objective and subjective tests.

The Article's second goal is to offer a normative framework to assess the choice between subjective and objective approaches in Fourth Amendment law.[13] At its best, reliance on subjectivity can further the aims

5. *Id.* at 813, 819.

6. *See, e.g.*, Ashcroft v. Al-Kidd, 563 U.S. 731, 737 (2011); *Brigham City*, 547 U.S. at 404; United States v. Knights, 534 U.S. 112, 122 (2001); *Bond*, 529 U.S. at 338 n.2.

7. *Brigham City*, 547 U.S. at 405 ("It therefore does not matter here—even if their subjective motives could be so neatly unraveled—whether the officers [acted to] gather evidence against them or to assist the injured and prevent further violence.").

8. *Bond*, 529 U.S. at 338 n.2 ("The parties properly agree that the subjective intent of the law enforcement officer is irrelevant in determining whether that officer's actions violate the Fourth Amendment.").

9. *Al-Kidd*, 563 U.S. at 736 (Scalia, J.) (citing *Knights*, 534 U.S. at 122) (referring to "[t]wo limited 'exception[s]'"). The exceptions identified in *Al-Kidd* are the special needs and administrative search doctrines, "where actual motivations do matter." *Id.*

10. *See infra* Part I.

11. *See infra* Part I.

12. *See infra* Part I.

13. This is not a new question in Fourth Amendment scholarship. It has been discussed for decades in what amounts collectively to a significant body of literature. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 433–39 (1974) (introducing the pretext problem and discussing several possible solutions to it); Cynthia Barmore,

of Fourth Amendment law by enabling narrower rules that better distinguish harmful from helpful police conduct. What an officer is trying to do often correlates with the interests that the officer's conduct advances. Subjective rules can be useful if they prohibit acts when an officer's state of mind correlates with likely harm.[14] When the relevant government intent can be determined accurately, a test that considers the government's state of mind can avoid overly broad rules that would otherwise permit a great deal of harmful conduct or prohibit government acts that serve the public interest in enforcing the law.

The important caveat is that government states of mind can be difficult to measure.[15] Subjectivity is useful only if it can be measured relatively accurately in the setting of Fourth Amendment litigation. Judges' ability to accurately identify an officer's state of mind depends on the context. Some states of mind can be figured out better than others. But the practical challenges of identifying a government official's mental state can weaken or even subvert the benefits of subjectivity. Whether to use objective or subjective tests calls for a context-sensitive examination of both the benefits of narrower rules and the risks of measurement error for the particular subjective test being considered.[16]

A review of existing doctrine suggests a mixed bag on that score.[17] The Court's adoption of a subjective test for searches and seizures seems appropriate, as does its use of subjective tests for special needs and probation searches. The merits of the objective test in *Whren* are mixed, as the problem pairs particularly strong public interest in distinguishing stops based on intent

Authoritarian Pretext and the Fourth Amendment, 51 HARV. C.R. & C.L. L. REV. 273, 307 (2016) (arguing that Fourth Amendment doctrine should limit police enforcement undertaken "for reasons of power, money, or dogma"); Craig M. Bradley, *The Reasonable Policeman: Police Intent in Criminal Procedure*, 76 MISS. L.J. 339, 343 (2006) (rejecting the objective approach); John M. Burkoff, *Bad Faith Searches*, 57 N.Y.U. L. REV. 70, 111–16 (1982) (same); John M. Burkoff, *The Pretext Search Doctrine: Now You See It, Now You Don't*, 17 U. MICH. J.L. REF. 523, 528 (1984) (arguing for an inquiry into subjective intent to establish pretextual motives); Morgan Cloud, *Judges, "Testilying," and the Constitution*, 69 S. CAL. L. REV. 1341 (1996) (arguing for a two-part test to determine reasonableness with both subjective and objective components); George E. Dix, *Subjective "Intent" as a Component of Fourth Amendment Reasonableness*, 76 MISS. L.J. 373, 448–58 (2006) (considering different ways that subjective intent could be relevant to Fourth Amendment reasonableness); James B. Haddad, *Pretextual Fourth Amendment Activity: Another Viewpoint*, 18 U. MICH. J.L. REFORM 639, 640 (1985) (rejecting another scholar's contention that the Supreme Court "abandoned all efforts to curb pretextual fourth amendment activity"); Nirej Sekhon, *Purpose, Policing, and the Fourth Amendment*, 107 J. CRIM. L. & CRIMINOLOGY 65, 70–72 (2017) (advocating reliance on programmatic purpose); Eric F. Citron, Note, *Right and Responsibility in Fourth Amendment Jurisprudence: The Problem with Pretext*, 116 YALE L.J. 1072, 1077–78 (2007) (arguing that pretextual searches are problematic because they give the police too much power).

14. *See generally infra* subpart II(D).

15. *See generally infra* subpart II(E).

16. *See generally infra* Part II.

17. *See generally* Part III.

with a very high risk of measurement error. On the other hand, the Court's reliance on subjective concerns in the exclusionary rule setting is problematic.[18]

This Article proceeds in three parts. Part I surveys existing Fourth Amendment doctrines that rely on an officer's state of mind. Part II develops the normative framework. Part III reviews existing doctrines and offers tentative judgments on existing law's choices between objective and subjective tests.

I. Government Subjectivity in Existing Fourth Amendment Doctrine

This section is descriptive. It shows that an officer's subjective state of mind is often relevant to existing Fourth Amendment doctrine. Officer subjectivity plays a significant doctrinal role at each of the three stages of Fourth Amendment doctrine.[19] A subjective element is required at the first stage, on what is a search or seizure; it often arises at the second stage when courts figure out if a search or seizure was unreasonable and therefore unconstitutional; and it plays a major role in determining the scope of Fourth Amendment remedies.

Before I get started, let me clarify a definition. When I refer to doctrines that rely on "government subjectivity," I mean any legal test, rule, or standard that incorporates a government official's actual state of mind.[20] That would mean, in Model Penal Code terms, a test that looks to the intent, awareness, or conscious disregard of a risk of some fact or belief about the world.[21] Put in more colloquial terms, my focus is on legal tests that consider what government agents were thinking rather than focus exclusively on objective facts like what an officer was doing.

---

18. *See id.*

19. My doctrinal overview in this section has some similarities with prior efforts to assess the subjectivity of Fourth Amendment doctrine. *See* Sekhon, *supra* note 13, at 82–90 (summarizing cases that rely on subjective tests in Fourth Amendment law); *see also* Dix, *supra* note 13, at 377–78, 410–15, 418–20 (summarizing cases that rely on subjective tests in Fourth Amendment law, interspersed with discussion of cases that rely on objective tests).

20. Importantly, this Article concerns *government* subjectivity in Fourth Amendment doctrine. Although this may ring a bell with readers familiar with the subjective and objective expectation of privacy test under *Katz v. United States*, 389 U.S. 347 (1967), that test has no relevance here. The *Katz* test at most considers the expectations of privacy of individual suspects and society at large. It does not consider the *mens rea* of government agents, which is my focus here. For more on the role of a suspect's expectations in Fourth Amendment law, see generally Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015).

21. *See* MODEL PENAL CODE § 2.02 (AM. LAW. INST. 1985) (defining mental states of purposely, knowingly, and recklessly).

A. Government Searches and Seizures

Let's begin with the threshold question in Fourth Amendment law: What is a government search or seizure? Existing doctrine, much of it quite recent, imposes a subjective requirement at this stage. We'll run through the major cases to see this, starting with what is a search, next considering what is a seizure, and then concluding with the state action requirement.

1. Searches.—The Fourth Amendment search doctrine includes a government intent requirement that was first announced in 2012 in *United States v. Jones*,[22] an opinion by Justice Antonin Scalia. According to *Jones*, government action is only a Fourth Amendment search when conducted "to obtain information."[23] "[A]n attempt to find something or to obtain information" is required for a search to occur.[24]

A quick review of *Jones* explains how this requirement arose. Investigators installed a GPS device on a suspect's car and used it to track the suspect's location for 28 days.[25] The Court held that installation with intent to use the GPS device was a Fourth Amendment search.[26] The intent requirement was added in a footnote in response to Justice Alito's concurrence, which disagreed with the Court's conclusion that installing the device was a search.[27] Justice Alito reasoned that installing a device should not be a search because the Court's precedents indicated that no search likely would occur if the government had broken the installation into two stages.[28] Mere installation of the GPS device without its use would not be a search, Justice Alito argued, and mere use without its installation would not be a search either. Putting the pieces together, Justice Alito reasoned, installing the device and then using it should not be a search. [29]

The *Jones* majority introduced the intent requirement of Fourth Amendment searches in a footnote that responded to Justice Alito. Justice Scalia explained that "[a] trespass on 'houses' or 'effects,' or a *Katz* invasion of privacy, is not alone a search unless it is done to obtain information."[30] Combining installation and use triggered the search doctrine because it

22. 565 U.S. 400 (2012).

23. *Id.* at 408 n.5.

24. *Id.* Note that this test does not require an investigatory purpose, but merely a goal to obtain some kind of information. *Cf.* Jane Doe I v. Valencia Coll. Bd. of Trs., 838 F.3d 1207, 1212–13 (11th Cir. 2016) (holding that invasive ultrasounds conducted for instructional reasons are Fourth Amendment searches, and that no "investigative or administrative purpose" is required).

25. *Jones*, 565 U.S. at 402–03.

26. *See id.* at 413.

27. *See id.* at 408 n.5.

28. *See id.* at 420 (Alito, J., concurring in the judgment) ("If these two procedures are analyzed separately, it is not at all clear from the Court's opinion why either should be regarded as a search.").

29. *Id.*

30. *Id.* at 408 n.5 (majority opinion).

combined the act of installation with the appropriate future intent to use it: "Trespass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information."[31] To trigger the Fourth Amendment search doctrine, the government must act with an intent to obtain information.

2. Implied Licenses.—The Court also adopted a subjective intent test in its 2012 decision in *Florida v. Jardines*,[32] another opinion by Justice Scalia. *Jardines* was an implied license search case used to interpret the trespass test of *Jones*.[33] *Jardines* considered whether a Fourth Amendment search occurs when an officer walks up to the front door of a private home with a drug-sniffing dog to see if the dog will alert to the smell of drugs inside.[34] *Jardines* made two rulings that are relevant here. First, it ruled that an officer's approach to the front door of the home could be a search because it entered the curtilage of the home, an outside space around the home that is treated as the home for Fourth Amendment purposes.[35] Second, the Court ruled that approaching the door with a drug-sniffing dog was outside the implied license to enter the curtilage that homeowners extended to home visitors.[36]

According to Justice Scalia, the scope of the implied license was determined by the officer's subjective intent when he approached the front door.[37] Residents implicitly permitted anyone "to approach the home by the front path, knock promptly, wait briefly to be received, and then (absent invitation to linger longer) leave."[38] But the same license did not extend to an officer who approached the home with a "specific purpose" to conduct a search.[39] According to Justice Scalia, officers approaching the door with the intent to gather evidence from inside are outside the license: "to spot that same visitor exploring the front path with a metal detector, or marching his bloodhound into the garden before saying hello and asking permission, would inspire most of us to—well, call the police."[40]

Jardines explicitly rejected the state's contention its subjective approach was inconsistent with objective cases like *Whren*. According to the Court, the objective cases stood "merely" for a narrow point that improper

31. *Id.*
32. 569 U.S. 1 (2013).
33. *See id.* at 11 (discussing the *Jones* test).
34. *Id.* at 3–5.
35. *Id.* at 6–7.
36. *Id.* at 9.
37. *Id.* at 10.
38. *Id.* at 8.
39. *Id.* at 9 ("The scope of a license—express or implied—is limited not only to a particular area but also to a specific purpose.").
40. *Id.*

motive did not normally render an otherwise-lawful search or seizure in violation of the Fourth Amendment.[41] It was proper to rest the implied license on officer intent, in contrast, because the question before the Court was identifying "whether the officer's conduct was an objectively reasonable search" in the first place.[42]

3. Seizures.—The doctrine of seizures also includes a subjective element that was introduced by *Brower v. County of Inyo*,[43] yet another opinion by Justice Scalia. *Brower* held that a seizure requires "an intentional acquisition of physical control."[44] "[G]overnmental termination of freedom of movement" is a seizure, the Court held, only "through means intentionally applied."[45]

Brower involved a fatal crash following a high-speed chase by an escaping driver who crashed his car into a police roadblock.[46] The driver's heirs brought a Fourth Amendment civil suit against the officers who set up the roadblock alleging excessive force. In their view, the roadblock had "seized" the driver unreasonably when he crashed into it.[47] The Court of Appeals held that the escaping driver was not seized because he was trying to evade the police, not be stopped by them.[48]

The Supreme Court disagreed in another opinion by Justice Scalia.[49] The government had seized the driver when he crashed into the roadblock, the Court held, because he was stopped "by the very instrumentality set in motion or put in place in order to achieve that result."[50] Intent to stop was crucial, as a Fourth Amendment seizure "requires an intentional acquisition of physical control." The case would be different, Justice Scalia reasoned, if the stopping were an accident: "if a parked and unoccupied police car slips its brake and pins a passerby against a wall," no Fourth Amendment seizure has occurred.[51] Because the driver "was meant to be stopped by the physical obstacle of the roadblock," and was so stopped, the officers had seized him.[52]

Brower's subjective requirement for seizures resembles *Jones*'s subjective requirement for searches. In both cases, officers need an intent to

41. *Id.* at 10.

42. *Id.*

43. 489 U.S. 593 (1989).

44. *Id.* at 596.

45. *Id.* at 597.

46. *Id.* at 594.

47. *See id.* (claiming the respondents used unreasonable force in establishing the roadblock, thus effecting an unreasonable seizure of Brower).

48. Brower v. Cty. of Inyo, 817 F.2d 540, 546 (9th Cir. 1987).

49. *Brower*, 489 U.S. at 599.

50. *Id.*

51. *Id.* at 596.

52. *Id.* at 599.

achieve the natural result of their acts. To conduct a search, an officer needs intent to obtain information. And to conduct a seizure, an officer needs intent to take possessory control of property.

4. Government Action.—Government subjectivity also plays a role in the doctrine of Fourth Amendment state action. When a private party conducts a search or seizure, the Fourth Amendment applies "if the private party act[s] as an instrument or agent of the Government"[53] by acting "at their direction."[54] Under the cases, the government officials' intent about the private party action is important to whether the private party is deemed a Fourth Amendment state actor.

Coolidge v. New Hampshire[55] provides an example. The police suspected that Mr. Coolidge committed a brutal murder, and they went to the Coolidge home and spoke to Mrs. Coolidge when Mr. Coolidge was away.[56] The police asked Mrs. Coolidge if her husband owned any guns, and she volunteered to bring them to the police.[57] Two officers accompanied Mrs. Coolidge to the bedroom where the guns were located. "If you would like them," she told the police, "you may take them."[58] The officers took the guns away, one of which the prosecution believed was the murder weapon.[59] Mr. Coolidge argued that his wife had been acting as a state actor when she went to the bedroom and that, therefore, a warrant was required to enter their home.[60]

The Supreme Court disagreed. According to the Court, whether Mrs. Coolidge was acting as a state actor under the Fourth Amendment depended on whether the officers were attempting to control or direct her conduct.[61] In this case, the impetus for entering the home to obtain guns and clothes was Mrs. Coolidge, not the police: she was acting on her own accord in an effort to prove her husband innocent.[62] "There is not the slightest implication of an attempt on [the officers'] part to coerce or dominate her," the Court wrote, "or, for that matter, to direct her actions by the more subtle

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

54. *Id.*

55. 403 U.S. 443 (1971).

56. *Id.* at 446.

57. *Id.* at 486.

58. *Id.*

59. *See id.* at 448 (stating the prosecution's claim that one of the guns taken from the Coolidge home by the police was the murder weapon).

60. *See id.* at 487 (articulating the petitioner's argument that he was the victim of a search and seizure because Mrs. Coolidge was acting as an instrument of the officials by complying with a demand made by them).

61. *See id.* at 487–89 (stating and applying the test as a question of whether an actor is acting as an "instrument" of the state through the coercion or dominance of the police).

62. *Id.* at 489.

techniques of suggestion that are available to officials in circumstances like these."[63] A subjective government effort to control the private party was needed to make that private party a government actor.

B. Fourth Amendment Reasonableness

After identifying a government search or seizure, courts next ask whether the search or seizure is constitutionally reasonable and therefore lawful.[64] The reasonableness of a search or seizure generally hinges on its justification. In general, a search or seizure is permitted when conducted to satisfy a significant government interest that outweighs the invasion of privacy or security.[65] Once again, the government's subjective intent plays an important role in making that assessment.

This section surveys the reasonableness doctrines that rely on government subjectivity. It starts with the special needs doctrine, turns to the inventory search doctrine, covers the scope of *Terry* frisks, and concludes with probation and parolee searches.[66] At each stage, the doctrine looks to an officer's subjective state of mind.

1. The Special Needs Doctrine.—The starting point for understanding the role of officer subjectivity in reasonableness doctrine is the so-called "special needs" doctrine.[67] Under the special needs doctrine, government searches or seizures can be permitted without a warrant or probable cause when they are conducted in a reasonable way to advance important government interests

63. *Id.*

64. *See, e.g.*, United States v. Jones, 565 U.S. 400, 413 (2012) (addressing the government's argument of reasonableness after determining that the government's actions constituted a search under the Fourth Amendment).

65. *See* Orin S. Kerr, *An Economic Understanding of Search and Seizure Law*, 164 U. PA. L. REV. 591, 618–24 (2016) (characterizing the reasonableness standard under the Fourth Amendment as a form of cost–benefit analysis that balances the intrusion upon an individual's privacy against the degree in which the search is necessary to further a legitimate governmental interest).

66. There are additional individual cases from the circuits that have applied subjective tests but that have not been reviewed by the Supreme Court. *See, e.g.*, Perez Cruz v. Barr, 926 F.3d 1128, 1140–43 (9th Cir. 2019) (adopting a subjective test for the application of the rule of *Michigan v. Summers*); United States v. Mohamud, 843 F.3d 420, 441–44 (9th Cir. 2016) (appearing to adopt a subjective test to Fourth Amendment analysis of who is targeted in a communication between an individual who lacks Fourth Amendment rights and an individual who has Fourth Amendment rights); United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (adopting a subjective test for applying the plain-view doctrine to digital evidence). I have opted not to discuss them as examples of the subjective approach because they are individual lower court decisions and are not firmly established in the caselaw.

67. *See generally* WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 10 (6th ed. 2020) (analyzing the application of the special needs doctrine by the courts in different contexts).

other than ordinary law enforcement.[68] The doctrine exists because modern governments wear many hats. In addition to enforcing criminal laws, government officials are tasked with administering government workplaces, running public schools, protecting the public from drunk drivers, and performing countless other nonlaw-enforcement tasks. The special needs doctrine provides a doctrinal framework for balancing these government interests with privacy rights outside traditional law enforcement.[69]

Applying the special needs doctrine often requires considering government intent.[70] In particular, courts often examine the governmental purpose of the search or seizure to determine if it was undertaken for a special need outside ordinary law enforcement.[71] Importantly, this question is typically posed at a programmatic level rather than an individual one. Courts scrutinize the purpose of the program, not what a particular officer was thinking.[72] But the legality of the search nonetheless hinges on government intent.

We can helpfully frame the dynamic by contrasting two cases: *Michigan Department of State Police v. Sitz*[73] and *City of Indianapolis v. Edmond*.[74] In *Sitz*, the Court held that a drunk driving checkpoint was constitutional. The checkpoint program was "aimed at reducing the immediate hazard posed by the presence of drunk drivers on the highways."[75] This nonlaw-enforcement public safety purpose permitted the government to stop the cars so long as the stop was generally reasonable: The usual requirement of probable cause or reasonable suspicion did not apply. The seizures in *Sitz* were reasonable, the Court concluded, because "the State's interest in preventing drunken driving" and "the extent to which this system can reasonably be said to advance that interest" outweighed "the degree of intrusion upon individual motorists who are briefly stopped."[76]

In contrast, the Supreme Court invalidated a narcotics checkpoint in *Edmond*. The city of Indianapolis set up a checkpoint on a highway entering the city to search cars for drugs.[77] The "primary purpose" of the checkpoint was "the discovery and interdiction of illegal narcotics," the Court noted,

68. *See generally id.* (describing the way in which the courts have characterized the special needs doctrine).

69. *See* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254, 276 (2011) (describing the characteristics of the special needs test as laid out by the Supreme Court).

70. *See infra* notes 73–82.

71. *See id.*

72. *See id.*

73. 496 U.S. 444 (1990).

74. 531 U.S. 32 (2000).

75. *Edmond*, 531 U.S. at 39 (describing the checkpoint in *Sitz*).

76. *Sitz*, 496 U.S. at 455.

77. *Edmond*, 531 U.S. at 34–36.

which was a traditional law enforcement goal.[78] This purpose meant that the special needs doctrine from *Sitz* could not apply. "Because the primary purpose of the Indianapolis narcotics checkpoint program is to uncover evidence of ordinary criminal wrongdoing," the Court held, "the program contravenes the Fourth Amendment."[79] A purpose to enforce criminal law requires satisfying traditional cause-based legal standards as in *Edmond*, while a purpose to advance other governmental goals, such as public safety, permits the program if it satisfies a general balance of interests as in *Sitz*.

Edmond stressed that it was the "programmatic purpose," not the individual officer's intent, that mattered.[80] Although the *Whren* line of cases rejected reliance on a particular officer's intent, "programmatic purposes may be relevant to the validity of Fourth Amendment intrusions undertaken pursuant to a general scheme without individualized suspicion."[81] The basic idea appears to be that special needs searches and seizures reflect a broader nonlaw-enforcement interest and are permitted when reasonable to advance that interest. Courts measure whether a search or seizure reflects and advances that interest by first determining whether its motivation matches its legal justification.[82]

2. The Inventory Search Exception.—The Supreme Court has also considered subjective intent in applying the inventory search exception. The inventory search exception permits the police to search property taken into police custody to create a record of its contents in the event that claims are later made that property was not returned or was damaged.[83] The Court has suggested that the inventory search exception applies only if the impounding of property is not a pretext for general law-enforcement concerns. As the Court stated in *Florida v. Wells*,[84] "an inventory search must not be a ruse for a general rummaging in order to discover incriminating evidence."[85] Under the doctrine, "[t]he individual police officer must not be allowed so much latitude that inventory searches are turned into a 'purposeful and general means of discovering evidence of crime.'"[86] As applied in the lower courts,

78. *See id.* at 34, 40–41 (agreeing with lower courts that the city's proximate goal was to apprehend drug offenders).

79. *Id.* at 41–42.

80. *Id.* at 46.

81. *Id.* at 45–46.

82. *See id.* at 37–40 (examining law-enforcement motivations in cases where suspicionless searches have been upheld or overturned).

83. *See generally* LAFAVE, *supra* note 67, at § 7.4(a) (discussing inventory search doctrine).

84. 495 U.S. 1 (1990).

85. *Id.* at 4.

86. *Id.* See also South Dakota v. Opperman, 428 U.S. 364, 376 (1976), allowing an inventory search and stressing that "there is no suggestion whatever" that the inventory search "was a pretext concealing an investigatory police motive."

this means that courts routinely scrutinize inventory searches to determine if they were conducted "as a pretext for criminal investigation."[87]

The Supreme Court reconciled the role of subjective intent for inventory searches with its usual opposition to such a role in *Whren*. According to *Whren*, the inventory search cases did not "endors[e] the principle that ulterior motives can invalidate police conduct that is justifiable on the basis of probable cause to believe that a violation of law has occurred."[88] The key was that searches "for the purpose of inventory or administrative regulation" did not require probable cause.[89] Only when probable cause was not required did subjective intent matter. Thus, "outside the context of inventory search or administrative inspection," an officer's motive could not invalidate "objectively justifiable behavior under the Fourth Amendment."[90]

3. The Scope of Terry *Frisks.*—The Supreme Court has also relied on subjective intent, albeit less than fully explicitly, in determining the permitted scope of frisks for weapons. *Terry v. Ohio*[91] permits officers to pat down a suspect for guns, knives, or other threats to the officer when the officer has reasonable suspicion that the suspect is armed and dangerous.[92] In *Minnesota v. Dickerson*,[93] the Court imposed an important limit on the type of frisk that appears to hinge on the officer's state of mind.

The officer in *Dickerson* patted down a suspect for weapons and felt "a small lump"[94] sticking out from the suspect's jacket pocket. With his hands outside the jacket, the officer manipulated the lump, "examin[ing] it with [his] fingers."[95] The officer's manipulation of the lump led it to slide around, causing the officer to conclude that it was likely a lump of crack cocaine wrapped in cellophane. At that point the officer reached into the pocket and pulled out the item, confirming his suspicion and leading to charges.[96] Among the issues before the Supreme Court was whether the officer could use his hands to examine the lump from the outside of the pocket to determine what was inside.

87. *See* People v. Toohey, 475 N.W.2d 16, 19, 24–25, 27 (Mich. 1991) (presenting an overview of Supreme Court exceptions to the need for a warrant and holding that the search was constitutional because there was no showing that it was a pretext for a criminal investigation).

88. Whren v. United States, 517 U.S. 806, 811 (1996).

89. *Id.* at 811–l2.

90. *Id.* at 812.

91. 392 U.S. 1 (1968).

92. *Id.* at 30.

93. 508 U.S. 366 (1993).

94. *Id.* at 369.

95. *Id.*

96. *Id.*

The Court answered no.[97] The core problem was the officer's subjective state of mind at the time of his act. *Terry* permitted officers to conduct a pat-down for weapons. But the officer in *Dickerson* already had "concluded that it contained no weapon" when he examined the lump.[98] Because the officer believed that there was no weapon in the suspect's pocket, his act of "squeezing, sliding and otherwise manipulating the contents of the defendant's pocket"[99] "was unrelated to '[t]he sole justification'" of *Terry* frisks[100] and "overstepped the bounds of the 'strictly circumscribed' search for weapons allowed under *Terry*."[101]

Although the Court did not dwell on the point in *Dickerson*, its analysis appears to rest the scope of *Terry* frisks on the officer's subjective intent. Whether squeezing the lump complied with the Fourth Amendment depended on whether the officer was looking for a weapon or looking for evidence. The officer could squeeze the lump while trying to find a weapon because that goal was related to the officer-safety justification for *Terry* frisks. On the other hand, squeezing while subjectively searching for drugs was unlawful because it was unrelated to that justification.

4. Probation and Parolee Searches.—Subjective approaches have also been applied in the lower courts to Fourth Amendment rules on searches of probationers and parolees. The Supreme Court has explained that those on probation and parole can have limited Fourth Amendment rights if courts impose search provisions on their conditions of release.[102] This raises an intriguing question: Does an officer need to know the person's status to rely on the Court's deferential Fourth Amendment search rules?

To see this, imagine an officer searches a person or his property as part of a criminal investigation. The officer only later determines that the person was on probation or parole and had a decreased expectation of privacy. In such a case, how much Fourth Amendment protection does the person receive? Is the level of protection set by the officer's subjective but incorrect belief that the person had full Fourth Amendment rights? Or are protections lowered by the person's status as a probationer or parolee that the officer did not know?

---

97. *Id.* at 377, 379.

98. *Id.* at 378.

99. *Id.* (quoting Dickerson v. State, 481 N.W.2d 840, 844 (1992)).

100. *Id.*

101. *Id.*

102. *See* United States v. Knights, 534 U.S. 112, 122 (2001) (upholding a limited right to privacy under the Fourth Amendment for those on probation). *See also* Samson v. California, 547 U.S. 843, 852 (2006) (stating that those on parole have a limited but not fully diminished right to privacy under the Fourth Amendment).

Although the Supreme Court has not directly addressed this question, lower courts are uniform that the officer's subjective understanding controls. As one court summarized: "[T]here is a knowledge component to a valid parole search, that is, the officers conducting the search must have knowledge of the elements that validate the search."[103] For the special rules on probation and parole searches to apply, officers must know that the person was on parole or probation, that the person's parole or probation agreement included a search provision, and that the place searched was subject to the provision.[104]

This approach has been justified on the ground that the reasonableness of a search should be measured "based on the circumstances *known to the officer* when the search is conducted."[105] Facts that become known only after a search occurred should not impact its reasonableness.[106] As a practical matter, this makes the reasonableness of the search hinge on the officer's subjective state of mind. If the officer correctly thinks he is searching a person on probation or parole, the lower standards apply. If the officer incorrectly thinks he is searching a person with no prior convictions, they do not.[107]

C. Fourth Amendment Remedies

Officer subjectivity plays a particularly significant role in the application of the exclusionary rule. Under the exclusionary rule, the fruits of unlawful searches may be subject to suppression in a criminal case. The

103. United States v. Williams, 702 F.Supp.2d 1021, 1030 (N.D.Ill. 2010).

104. *See id.* (laying out the specific factors an office must have knowledge of before being allowed to execute a valid parole search); *see also* United States v. Caseres, 533 F.3d 1064, 1075–76 (9th Cir. 2008) (holding that officer must be aware of search condition to justify search under parole search rules); Moreno v. Baca, 431 F.3d 633, 641 (9th Cir. 2005) (holding that officer must be aware of parole status to rely on parole search rules); State v. Brusuelas, 219 P.3d 1, 5 (N.M. Ct. App. 2009) (holding that officer must be aware of probation condition for probation search rules to apply).

105. *In re* Jaime P., 146 P.3d 965, 972 (Cal. 2006).

106. *Id.*

107. It could also be argued that the probable cause and reasonable suspicion tests themselves are examples of subjective government *mens rea* tests in Fourth Amendment doctrine because they look to what an officer knew in order to determine if the government had sufficient cause. *See, e.g.*, Craig M. Bradley, *The Reasonable Policeman: Police Intent in Criminal Procedure*, 76 MISS. L.J. 339, 372 (2006) ("[T]here is no such thing as a purely objective Fourth Amendment inquiry. Once one concedes, as the Court does in *Devenpeck*, that what the police know is part of the probable cause equation, the genie of police intent is out of the bottle."). Although this could be included as an example of government subjectivity, I think the picture is somewhat more mixed. First, the Supreme Court has formally rejected an intent-based standard for probable cause. *See* Devenpeck v. Alford, 543 U.S. 146, 153 (2004) (noting that "an arresting officer's state of mind . . . is irrelevant to the existence of probable cause"). Second, the so-called "collective knowledge doctrine," which allows courts to consider the knowledge among different officers, suggests that the knowledge component in cause thresholds is more about what an officer was objectively told than what an officer subjectively knew. *See generally* WAYNE R. LAFAVE, SEARCH AND SEIZURE § 3.5(a)–(b), § 9.5(j) (5th ed. 2018) (discussing the collective knowledge doctrine).

complex doctrines that govern the exclusionary rule include frequent consideration of the government's subjective intent. There are four doctrines to consider: the role of *mens rea* in *Herring v. United States*,[108] the fruit of the poisonous tree doctrine, *Franks* challenges,[109] and lower court rules on flagrant disregard of a warrant.

1. The Role of Mens Rea in Herring v. United States*.*—The starting point for considering officer subjectivity in exclusionary rule case law is the Court's 2009 ruling in *Herring v. United States*.[110] Under *Herring*, only "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence," is sufficiently deliberate and culpable to trigger the exclusionary rule.[111]

Here are the facts. Officers found drugs and guns on Herring when they searched him after arresting him based on a report that a warrant had been issued for his arrest.[112] It turned out, however, that the report was wrong. The warrant had been recalled months earlier, but the nearby county that reported that a warrant existed had failed to update its database.[113] The county quickly realized its error, but its correction came too late: The officers had already arrested Herring and found the drugs and guns.[114] The question before the Supreme Court was whether the exclusionary rule required the suppression of the fruits of Herring's wrongful arrest.

The answer, the Court reasoned, depended on the officers' culpability in making the unlawful seizure. According to Chief Justice Roberts, suppression is only appropriate when it results in appreciable deterrence that outweighs the social costs of letting the guilty escape punishment.[115] And, critically, the prospects of deterrence hinge largely on the officer's state of mind: "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system."[116]

The exclusionary rule should not be applied to Herring's arrest, the Court ruled, because the "police mistakes [we]re the result of negligence . . . rather than systemic error or reckless disregard of constitutional requirements."[117] The officers who relied on the report that there was a

108. 555 U.S. 135 (2009).
109. Franks v. Delaware, 438 U.S. 154 (1978).
110. 555 U.S. 135 (2009).
111. *Id.* at 144.
112. *Id.* at 137.
113. *Id.* at 137–38.
114. *Id.* at 138.
115. *Id.* at 141.
116. *Id.* at 144.
117. *Id.* at 147.

warrant out for Herring's arrest had no reason to doubt the accuracy of that claim. None of the officers involved had heard of a similar error occurring.[118] Absent a showing of reckless or intentional misconduct—such as evidence that the officers "knowingly made false entries to lay the groundwork for future false arrests"—the degree of fault was mere negligence and not the higher degree of culpability required to trigger the exclusionary rule.[119]

An important caution in treating *Herring* as a case about officer subjectivity is that the Court insisted its test was objective and not subjective. "The pertinent analysis of deterrence and culpability is objective, not an 'inquiry into the subjective awareness of arresting officers,'" the Court wrote.[120] The test relies on "a particular officer's knowledge and experience, . . . but not his subjective intent," citing *Whren*.[121] While that may be true for distinguishing mere negligence from gross negligence, it seems hard to see how that applies to "deliberate" wrongful conduct. The dictionary definition of "deliberate" is "intended, not done by chance or accident."[122] This suggests that intent or awareness of violating the Fourth Amendment can itself reflect the culpability that triggers the exclusionary rule, which to my mind brings the *Herring* inquiry into a more subjective frame despite the Court's statement to the contrary.

2. The Fruit of the Poisonous Tree Doctrine.—An officer's subjective awareness of illegality is also relevant to the so-called fruit of the poisonous tree doctrine. This doctrine asks whether the discovery of particular evidence was so closely connected to an earlier constitutional violation that the evidence must be suppressed as a result of it.[123] In 2016, in *Utah v. Strieff*,[124] the Court interpreted the doctrine to rely in part on whether the violation was "a purposeful or flagrant violation" of the defendant's Fourth Amendment rights.[125]

The officer in *Strieff* stopped a man who had just walked out of a house under surveillance for narcotics activity.[126] The officer asked the man for identification, the man produced a state identification card identifying himself as Edward Strieff, and a call to the police dispatcher revealed that

118. *Id.*

119. *Id.* at 144.

120. *Id.* at 145 (quoting Reply Brief for Petitioner at 4–5, Herring v. United States, 555 U.S. 135 (No. 07-513)).

121. *Id.* at 145–46.

122. *Deliberate*, MACMILLAN DICTIONARY, https://www.macmillandictionary.com/us/dictionary/american/deliberate_1 [https://perma.cc/24FD-FF87].

123. *See generally* LAFAVE, *supra* note 67, at § 11.4 (discussing the fruit of the poisonous tree doctrine).

124. 136 S. Ct. 2056 (2016).

125. *Id.* at 2063.

126. *Id.* at 2059–60.

there as a warrant out for his arrest.[127] The officer searched Strieff and found drugs, leading to drug charges.[128] The initial stop violated the Fourth Amendment because the officer lacked the reasonable suspicion to justify the stop.[129] The question in *Strieff* was whether the drugs discovered in the search incident to arrest were fruits of the unlawful stop and therefore should have been suppressed.[130]

In a nod to *Herring*, Justice Thomas reasoned in *Strieff* that the exclusionary rule was proper "only when the police misconduct is most in need of deterrence—that is, when it is purposeful or flagrant."[131] The officer's violation "was at most negligent," Justice Thomas concluded, based on "good-faith mistakes" about how the law applied to his acts.[132] The conclusion that the officer's "errors in judgment hardly r[o]se to a purposeful or flagrant violation of Strieff's Fourth Amendment rights" counseled against suppression.[133]

3. Franks *Challenges.*—The test for challenging false statements in search warrants also has a subjective element. Under *Franks v. Delaware*,[134] the fruits of a search warrant can be suppressed if the defense can make a showing that the warrant was issued based on false statements of probable cause made "knowingly and intentionally, or with reckless disregard for the truth."[135]

The problem addressed in *Franks* is that a search warrant can establish probable cause based on erroneous facts. Consider three different kinds of errors. In some cases, the officer might assert evidence honestly believed that turns out to be wrong.[136] For example, an affidavit might correctly report an informant's claim that he saw the defendant commit the crime, but it may turn out that the informant was mistaken.[137] In other cases, the officer marshalling the evidence in the affidavit might make an innocent mistake.

127. *Id.* at 2060.

128. *Id.*

129. *See id.* at 2062 (noting the Court's assumption that the initial stop was unconstitutional for lack of reasonable suspicion).

130. *See id.* at 2059 (framing the case around the question of whether the Fourth Amendment violation justified suppressing the seized evidence).

131. *Id.* at 2063.

132. *Id.*

133. *Id.*

134. 438 U.S. 154 (1978).

135. *Id.* at 155–56.

136. *See id.* at 165 ("This does not mean 'truthful' in the sense that every fact recited in the warrant affidavit is necessarily correct, for probable cause may be founded upon hearsay and upon information received from informants, as well as upon information within the affiant's own knowledge that sometimes must be garnered hastily.").

137. *See id.* (acknowledging that information received from informants may include incorrect material).

For example, the officer might accidentally misstate the evidence by reading a police report incorrectly in a way that makes the evidence seem stronger than it is.[138] Finally, the officer might deliberately or recklessly falsify the evidence, such as when a corrupt officer simply lies in the affidavit to intentionally create an impression of probable cause that did not exist.

Franks holds that evidence obtained from a warrant search should be suppressed when a defendant can show by a preponderance of the evidence that assertions in the warrant affidavit fit into the third category: the statements are "deliberate falsehood[s]" or false statements made with "reckless disregard for the truth," without which no probable cause would have been found and the warrant should not have issued.[139] Justice Blackmun's opinion for the Court does not delve into why the test treats false statements based on an affiant's "negligence or innocent mistake" one way but those based on "deliberate falsity or reckless disregard"[140] another. But it suggests that the reason was the seriousness of the harm. The "specter of intentional falsification"[141] threatened to reduce the warrant requirement "to a nullity."[142] The Fourth Amendment would have little meaning, Justice Blackmun reasoned, "if a police officer was able to use deliberately falsified allegations to demonstrate probable cause, and, having misled the magistrate, then was able to remain confident that the ploy was worthwhile."[143]

4. Flagrant Disregard of Warrant Limitation.—A final exclusionary rule doctrine that relies on subjective intent is the "flagrant disregard" standard for executing warrants that has been widely adopted by the federal courts of appeals.[144] When a warrant is executed in flagrant disregard of its terms, the entirety of the fruits of the warrant search can be suppressed. Courts applying this test consider whether the officers so grossly exceeded the scope of the warrant that the officers appeared to be subjectively on a "fishing expedition" seeking other information.[145] When this occurs, the remedy is blanket

138. *See id.* at 170 (recognizing "instances where police have been merely negligent in checking or recording the facts relevant to a probable-cause determination").

139. *Id.* at 171–72.

140. *Id.*

141. *Id.* at 168.

142. *Id.*

143. *Id.*

144. *See, e.g.*, United States v. Khanani, 502 F.3d 1281, 1289 (11th Cir. 2007) (applying the standard of flagrant disregard to test a Fourth Amendment violation); United States v. Le, 173 F.3d 1258, 1269–70 (10th Cir. 1999) (describing the test for transforming a valid warrant into a general warrant as a test of "'flagrant disregard' for the terms of the warrant"); United States v. Matias, 836 F.2d 744, 747–48 (2d Cir. 1988) (citing cases). The test has not yet been addressed by the United States Supreme Court, however.

145. *See, e.g.*, United States v. Liu, 239 F.3d 138, 140 (2d Cir. 2000) (describing circumstances in which government agents "flagrantly disregard" sthe terms of a warrant in ways that justify "wholesale suppression" of the evidence); United States v. Young, 877 F.2d 1099, 1105–06 (1st

suppression of all of the evidence—even that evidence described in the warrant that was properly found and seized.

United States v. Foster[146] provides an example. Officers executed a search warrant at Foster's home for marijuana and several guns.[147] When the officers found that evidence, Foster was arrested and transported to the county jail. The officers continued the search for additional evidence, however. During the continued search, officers watched home movies that Foster had apparently recorded that included sexual acts between Foster and his stepdaughter. Federal agents ended up seizing the videos and state agents seized anything of value they could find in the home, including a lawn mower and three vehicles.[148]

The Tenth Circuit held that everything found in Foster's home should be suppressed because the officers had executed the warrant in flagrant disregard of its terms. Once in the house, the officers had ignored the warrant and simply looked for any evidence of any crime and had looked for "anything of value"[149] to seize. The officers had viewed the warrant "as a general warrant," and they "executed the warrant in accord with those views."[150] The district judge's factual finding that the officers had gone on a "fishing expedition" was supported by the record: "the officers' disregard for the terms of the warrant was a deliberate and flagrant action taken in an effort to uncover evidence of additional wrongdoing"[151] unrelated to the warrant's terms. Thus, the entire fruits of the search were suppressed.[152]

II. The Normative Case for Objective Versus Subjective Fourth Amendment Rules

Part I showed that Fourth Amendment doctrine relies increasingly on a mix of objective and subjective tests. This section turns to the normative question: When are subjective approaches appropriate? This section makes two related arguments and then puts them together.

First, reliance on subjectivity can advance Fourth Amendment goals because it allows courts to enact narrower rules that more accurately identify harmful police practices. What an officer was thinking tells us what the officer was trying to do. What an officer was trying to do sheds light on what

Cir. 1989) (citing cases to support suppression only when the lawful parts of a search seem to be a pretext for the unlawful parts).

146. 100 F.3d 846 (10th Cir. 1996).

147. *Id.* at 848.

148. *See id.* at 848, 848 n.1 (discussing the items seized during the process of the warrant's execution).

149. *Id.* at 848.

150. *Id.* at 850.

151. *Id.* at 850–51.

152. *Id.* at 853.

interests the officer's conduct furthers. If courts can know an officer's state of mind, doctrinal reliance on states of mind can allow courts to more accurately distinguish acts likely to advance important government interests from those unlikely to advance them. More tailored and specific Fourth Amendment rules can allow those rules to achieve a greater public enforcement benefit at a lower civil liberties cost.[153]

The second argument is that the benefit of subjectivity depends on the error rates of determining it. Subjectivity is useful when it can be measured relatively accurately. But when courts can't identify states of mind accurately, subjective tests that aim to maximize the public benefit of enforcement can inadvertently have the opposite effect.[154] Importantly, subjective approaches are not monolithic. Some states of mind can be reliably determined while others cannot be. But whether subjectivity can advance Fourth Amendment interests depends in large part on whether that particular subjective inquiry can be accurately measured.

Combining these two points suggests a framework for choosing between objective and subjective rules in Fourth Amendment doctrine. In each context, courts should consider the potential benefit of a narrower subjective rule in light of the likelihood courts can identify the government's state of mind accurately.

A. The Existing Debate on Objective Versus Subjective Rules

It's useful to begin with the existing scholarly debates on objective versus subjective Fourth Amendment rules. That debate has been plentiful but also relatively narrow. It has focused primarily on the reasonableness of Fourth Amendment searches and seizures, especially in the context of *Whren* and pretextual stops. Here's a quick overview.

On one hand, the Supreme Court has defended objective rules for the reasonableness of searches and seizures primarily on the ground that "the Fourth Amendment regulates conduct rather than thoughts" and objectivity "promotes evenhanded, uniform enforcement of the law."[155] When Fourth Amendment law relies on individualized suspicion to justify a search or seizure, that objective suspicion provides the objective and reliable justification.[156] The alternative of relying on what an officer was subjectively thinking is comparatively arbitrary, as two similarly situated officers might do exactly the same things but have two different sets of thoughts.[157] The best

153. *See generally infra* subpart II(C).

154. *See generally infra* subparts II(D)–(E).

155. Ashcroft v. Al-Kidd, 563 U.S. 731, 736 (2011).

156. *See generall*y Whren v. United States, 517 U.S. 806 (1996).

157. *See* Devenpeck v. Alford, 543 U.S. 146, 153–55 (2004) (articulating that Fourth Amendment reasonableness analysis relies on objective standards of conduct, rather than the officer's subjective state of mind).

way to have consistent rules is for the reasonableness balance to look to the factual basis for the officer's conduct rather than the thoughts in his head.

Scholars have generally doubted these claims. Much of the literature has focused on the debate over *Whren*, and especially the concern that allowing pretextual law enforcement gives the police so much discretion that *Whren* effectively blesses racially discriminatory police practices.[158] Scholars have explained that racially discriminatory enforcement inflicts grievous harms, and they argue that these harms should be considered as part of the reasonableness of the government's action.[159] The harms of racially discriminatory enforcement are so severe that the "objective" measure of reasonableness provided by probable cause is no longer accurate: The subjective must be considered.[160] While *Whren* itself suggested that the Fourteenth Amendment might be a better source for addressing this concern, the critics (including Justice Ginsburg, in a recent concurrence)[161] forcefully argue that it is a Fourth Amendment concern that justifies a Fourth Amendment response.[162]

These arguments are tremendously important, especially in light of the recent and long-overdue renewal of public interest in racially discriminatory

158. The literature here is vast and impressive. Prominent examples include: Albert W. Alschuler, *Racial Profiling and the Constitution*, 2002 U. CHI. LEGAL F. 163, 192–96; Gabriel J. Chin & Charles J. Vernon, *Reasonable but Unconstitutional: Racial Profiling and the Radical Objectivity of* Whren v. United States, 83 GEO. WASH. L. REV. 882, 894, 898–99, 919, 941 (2015); David A. Harris, *"Driving While Black" and All Other Traffic Offenses: The Supreme Court and Pretextual Traffic Stops*, 87 J. CRIM. L. & CRIMINOLOGY 544, 582 (1997); Kevin R. Johnson, *How Racial Profiling in America Became the Law of the Land:* United States v. Brignoni-Ponce *and* Whren v. United States *and the Need for Truly Rebellious Lawyering*, 98 GEO. L.J. 1005, 1065–75 (2010); Pamela S. Karlan, *Race, Rights, and Remedies in Criminal Adjudication*, 96 MICH. L. REV. 2001, 2010–11 (1998); Tracey Maclin*, Race and the Fourth Amendment*, 51 VAND. L. REV. 333, 376–78 (1998); Wesley MacNeil Oliver, *With an Evil Eye and an Unequal Hand: Pretextual Stops and Doctrinal Remedies to Racial Profilin*g, 74 TUL. L. REV. 1409, 1413–14 (2000); David Rudovsky, *Law Enforcement by Stereotypes and Serendipity: Racial Profiling and Stops and Searches Without Cause*, 3 U. PA. J. CONST. L. 296, 320–22 (2001); David A. Sklansky, *Traffic Stops, Minority Motorists, and the Future of the Fourth Amendment*, 1997 SUP. CT. REV. 271, 312–316 (1997). *Cf.* Anthony C. Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 74 N.Y.U. L. REV. 956, 978–83 (1999).

159. *See, e.g.*, Chin & Vernon, *supra* note 158, at 917–22, 924–26 (arguing that *Whren* is in tension with the Fourteenth Amendment's nondiscrimination principles and that nondiscrimination should be incorporated into reasonableness calculations).

160. *Cf.* Jonathan Witmer-Rich, *Arbitrary Law Enforcement Is Unreasonable:* Whren*'s Failure to Hold Police Accountable for Traffic Enforcement Policies*, 66 CASE W. RES. L. REV. 1059, 1080 (2016) (suggesting that addressing arbitrariness, which can be described objectively, is insufficient to address discrimination in law enforcement, which is subjective).

161. *See* District of Columbia v. Wesby, 138 S. Ct. 577, 594 (2018) (Ginsburg, J., concurring in the judgment) ("I would leave open, for reexamination in a future case, whether a police officer's reason for acting, in at least some circumstances, should factor into the Fourth Amendment inquiry.").

162. *See, e.g.*, Bradley, *supra* note 15, at 343 (rejecting the objective approach); Burkoff, *supra* note 15, at 111 (1982) (same); Dix, *supra* note 15, at 377 (same).

police enforcement.[163] But it seems to me that both sides of this existing debate are only part of a broader dynamic. The choice between subjective and objective doctrines in Fourth Amendment law raises broader stakes that have been underdiscussed and underdeveloped. The remainder of this section tries to develop that broader perspective, which will then be applied in Part III to evaluate existing doctrine.

B. Costs and Benefits in Fourth Amendment Law

In my view, the debate over officer subjectivity in Fourth Amendment law is best framed in terms of the expected costs and benefits of government action. Officer subjectivity matters because an officer's subjective thoughts are often relevant to those costs and benefits. Subjectivity can bring promise or peril, however, making officer subjectivity both appealing and risky as a doctrinal mechanism to weigh competing interests in Fourth Amendment law. Understanding this point requires starting with first principles about the functional role of search and seizure law. With that foundation explored, we can then see how it plays out with officer subjectivity.

Here's the big picture. Fourth Amendment law can be understood as an effort to internalize the civil liberties harms of government investigations.[164] Investigators try to collect evidence to solve cases and enforce the law. Ideally, this can further the public benefits of criminal enforcement such as protecting public safety and punishing wrongdoers. But there's a catch: Typically, government officials undervalue the civil liberties harms that their investigations cause.[165] They are less attuned than they should be to the harms to privacy, property, and collective community well-being that their investigations can trigger.[166]

Fourth Amendment law can be understood as a way to internalize investigative harms by imposing a rough cost–benefit framework on policework.[167] In a world without the Fourth Amendment, we would expect officers to engage in societally harmful searches and seizures because they

163. *See, e.g.*, Giovanni Russonello, *Why Most Americans Support the Protests*, N.Y. TIMES (June 5, 2020), https://www.nytimes.com/2020/06/05/us/politics/polling-george-floyd-protests-racism.html [https://perma.cc/ZJ74-NM8F] (describing recent shifts in public opinion about racism and policing, noting that "[n]ever before in the history of modern polling have Americans expressed such widespread agreement that racial discrimination plays a role in policing — and in society at large.").

164. For an economic model of search and seizure protections explaining these harms as "externalities" that can be addressed through a cost–benefit analysis, see Kerr, *supra* note 65, especially subparts I(A)–(D).

165. *Id.* at 603–05.

166. *See id.* at 600.

167. *See id.* at 605–06.

would fail to account fully for those societal costs.[168] Fourth Amendment law pushes the police to account for the externalities of their investigations by prohibiting steps when their civil liberties costs can be expected to outweigh the public benefits to the enforcement of the law.[169]

When judges implement Fourth Amendment law, they intuitively try to account for this dynamic. They will consider both how much a government action furthers legitimate government interests in enforcing the law and public safety and how much it infringes on privacy and civil liberties. And they will channel those instincts through the basic framework of Fourth Amendment doctrine, regulating those steps that impose high civil liberties costs as "searches" or "seizures" and subjecting searches or seizures to a rough cost–benefit analysis of reasonableness.[170] The outcome, at least ideally, is more efficient investigations that achieve greater public safety benefits at lower costs to civil liberties.[171]

C. The Scope Problem in Weighing Costs and Benefits

Now, let's focus on the role of government subjectivity. The subjectivity debate relates to a particular problem of measuring costs and benefits that I will call the scope problem. In an ideal world, courts could measure the costs and benefits of every single law enforcement step in isolation. They could determine if a particular officer's act in a particular case on a particular day advanced public interests more than its civil liberties costs.

But this isn't realistic. In the real world, the need for *ex ante* clarity and the impossibility of measuring costs and benefits in any one case requires courts to generalize.[172] Instead of looking at each case in isolation, courts devise rules that generalize from groups of facts. They analyze the costs and benefits of government-investigative steps by measuring the typical costs and benefits of that step over the range of facts governed by the rule.

The scope problem is that the costs and benefits of any step depend on the level of generality used to describe it. Because Fourth Amendment doctrine can use broad or narrow rules, courts have significant flexibility in selecting a scope that determines how costs and benefits will be

168. *See id.* (stating that "[a]bsent legal restriction, the police will discount external costs and take steps that seem desirable to officers but are welfare-reducing to society as a whole[,]" and presenting an example of these calculations).

169. *Id.*

170. *Id.*

171. *See id.* (arguing that Fourth Amendment rules tend to serve this function).

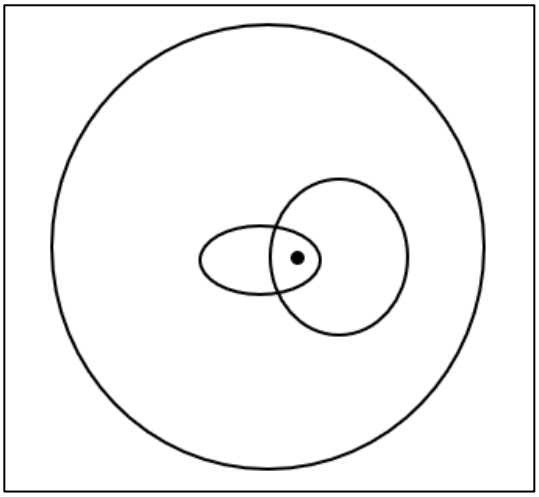
172. *See id.* at 608–10 (discussing the difficulties of predicting and measuring costs and benefits in individual cases).

categorized.[173] This has major implications for the role of officer subjectivity in search and seizure law.[174] Relying on an officer's state of mind allows courts to craft narrower rules, making it an important tool to generate more accurate rules if intent can be known.

It's important to understand why the scope problem exists and the role it plays in crafting Fourth Amendment doctrine. The problem exists because any factual scenario can be described as being inside an infinite number of different sets of broader facts that can be harnesses for a legal rule. Any one state of affairs in the world can be seen as an example of a range of possible sets, some larger and some smaller, which focus on different variables.

Figure 1 helps illustrate the point. The single dot represents the facts of any one case. The different shapes, all of which include the dot, are groupings of facts that represent the coverage of different possible rules. Note that some of the groupings are broad while others are narrow, representing broad or narrow rules. But the single dot—representing the specific facts of one case—is within all of these sets.

Figure 1



The scope problem is important because a judicial assessment of how much a step typically advances government interests and imposes costs largely depends on the scope courts select. Implementing the cost–benefit framework of Fourth Amendment law requires assessing costs and benefits

173. *Cf.* Mark Kelman, *Interpretive Construction in the Substantive Criminal Law*, 33 STAN. L. REV. 591, 593–94 (1981) (discussing how the reasonableness of a person's action in criminal law varies based on the timeframe over which that action is analyzed).

174. *See supra* notes 164–72 and accompanying text (exploring how the existence of the Fourth Amendment helps police departments internalize civil-liberties-based harms through a cost–benefit analysis framework).

over a presumed set of cases. Courts generalize about what is typical for that set based on their plausible intuitions about how facts in that grouping tend to work.[175]

But here's the key point: Because the scope defines the set, the scope also determines how much the costs and benefits of that step will be assessed. When judges are picking the set, they are picking the groupings of facts (such as those represented in Figure 1) over which the balance will be made. Picking the set picks the group of facts, and picking the group of facts can determine how a generalization over those facts will inform the cost–benefit balance.[176]

This likely sounds hopelessly abstract, so let me use a stylized example to render it more concrete. Imagine a traffic stop. Specifically, let's say that an officer pulls over a car with a broken taillight. He does so, let's assume, because he has some suspicion that the driver is a murderer. The officer has no interest in enforcing the traffic laws. Instead, he wants to question the driver to see if he can gather evidence of the murder.

Now imagine you are a judge tasked with deciding if the officer violated the Fourth Amendment. To make things interesting, assume that Fourth Amendment law is largely undeveloped. Imagine prior law has established that pulling the car over was a seizure,[177] but that it does not resolve when a traffic stop is a reasonable seizure. Your job, as a judge, is to craft the legal doctrine that answers whether the act of pulling over the car is a "reasonable" seizure.

As part of that task, you must create a legal test that analyzes how much the stop helped advance public interests in enforcement of the law. But as we will see below, the measurement of benefit depends on the scope you choose. We can see how by describing the stop in four different ways. We'll start at the broadest level of generality and move to a more specific description, focusing on how the measurement of government benefit may change.

Start at the broadest scope, what I will call Description 1. If we had to describe the stop in the most general terms, we might say that the officer's act was *detaining a person*. The driver is a person, after all, and pulling over the car is an example of detaining a person.[178] Using Description 1 requires us to answer a very broad question: On average, how much does detaining a person advance government interests?

---

175. *See* Kerr, *supra* note 164, at 610–11.

176. *Cf.* Kelman, *supra* note 173, at 594–95 (highlighting that, in the criminal context, factual settings can be regarded either as disjointed events or as one unified incident depending upon which outlook the viewer chooses).

177. *See* Brendlin v. California, 551 U.S 249, 251 (2007) (holding that pulling over a car seizes all of its occupants).

178. *See id.* at 255–56 (acknowledging that the police's stopping of a vehicle and detention of its occupants, no matter how brief, is sufficient to constitute a seizure).

At that level of generality, the answer seems to be "not much." Government officials can detain individuals in an incredibly wide range of hypothetical cases. On one hand, the cases include moments when an officer has good reasons to detain the person. But they would also include times when an officer has terrible reasons to detain the person, such as to harass or intimidate him. Those cases would also include when an officer detains someone for no real reason at all, such as for entertainment value. Generalizing across all of these cases, the act of detaining a person is not associated with a reliable amount of government benefit.

Next let's be more specific. For Description 2, describe the act as *a police officer pulling over a driver who has violated the traffic code*. Detaining the person now advances a more direct public interest. Unsafe driving leads to thousands of deaths and countless injuries every year.[179] Pulling over a driver who has violated the traffic code is an important way to identify traffic violations and ensure that he is driving in compliance with safety-oriented laws. Of course, we can't know at this level of generality if any particular act of pulling over a driver who has violated the traffic code actually advances safety. But generalizing across all of the hypothetical cases, pulling over a driver who has violated the traffic code likely advances a significant public safety benefit.

Next get more specific again. For Description 3, let's describe the act as *pulling over a driver who has violated the traffic code when the traffic violation is a pretext for the stop*. Adding information about the officer's state of mind changes the picture. We are now dealing with the subset of cases in which the officer has no interest in furthering the public safety benefit that the stop earlier seemed to benefit. We would expect that pretextual stops do not advance the traffic benefit and instead raise concerns about racial discrimination and profiling. Generalizing across all of these cases, it doesn't seem like pretextual stops benefit enforcement of the law at all.

One last example. For Description 4, let's offer every detail we know and return to the original statement of the hypothetical: *The officer pulls over a car with a broken taillight because he has some suspicion that the driver is a murderer. The officer has no interest in enforcing the traffic laws, but he wants to question the driver to see if he can gather evidence of the murder.* This last example fills in the true reason for the stop. Our assessment of how much the stop advances public safety goes up again, at least somewhat, because the stop will enable the officer to question a murder suspect. The

179. As the Supreme Court has recognized, the number of driving-related fatalities is "staggering." Birchfield v. North Dakota, 136 S. Ct. 2160, 2178 (2016) (citing NHTSA, TRAFFIC SAFETY FACTS, 2014 DATA, SUMMARY OF MOTOR VEHICLE CRASHES 2 (No. 812263, May 2016) (Table 1), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812263 [https://perma.cc/S57U-FHZQ]) (showing 29,989 fatalities and 1,648,000 injuries in 2014).

pretextual stop was not racial profiling or a personal vendetta, we learn. Instead, the officer was trying to solve an important case.

I hope this example explains the scope problem. The public benefit associated with a government step depends on how we group it. The description conjures up a range of facts, and that range of facts will lead to an assessment of the typical benefit of the step. When courts craft Fourth Amendment doctrine, they necessarily pick a rule that determines the relevant grouping. What benefit the law estimates for a particular step depends on the group produced by the chosen specificity of the rule.

D. Officer Subjectivity as a Tool to Narrow the Scope of Rules

Why does all of this matter for officer subjectivity in Fourth Amendment law? It matters, I think, because considering an officer's subjective state of mind can let us narrow the scope of Fourth Amendment rules. Subjectivity allows the courts to distinguish the subset of cases with a particular state of mind from the subset of cases without it. Subjectivity can act as a scalpel, dividing up the general set of cases into the narrower subsets with different states of mind.

This can be useful because states of mind will often correlate with the public benefits and civil liberties costs of government action. What an officer was thinking tells us what he was trying to do. That, in turn, tells us what interest he was hoping to advance. And because we are more likely to hit what we aim for,[180] the interest that an officer was trying to advance viewed *ex ante* likely correlates with the interest the act actually did advance viewed *ex post.*

From this perspective, reliance on officer subjectivity lets courts craft narrower rules that can lead to more accurate cost–benefit balancing. It lets courts pick smaller sets in the Venn diagram of Fig. 1. Narrower rules mean less generalization of costs and benefits. And that in turn can more specifically regulate police practices to better identify harmful practices and achieve higher public benefits at lower civil liberties costs by channeling law enforcement conduct away from acts with low public benefits and higher civil liberties costs.

Let's go back to the traffic stop hypothetical above to see the dynamic. Description 1 was extremely general. It covered any detention for any reason or no reason at all, requiring one estimate of benefit for an incredibly wide range of facts. Description 2 was somewhat more specific, carving out a subset of detentions (traffic stops) in a category of circumstances (traffic violations). But it's still a very broad category.

180. *Cf.* HENRY D. THOREAU, WALDEN 27 (J. Lyndon Shanley ed., Princeton Univ. Press 1971) (1854) ("In the long run men hit only what they aim at.").

The primary narrowing then came in Descriptions 3 and 4, both of which used officer subjectivity. Description 3 narrowed the category to cases in which the officer was acting pretextually. The subjectivity was still broad in that it ruled out one intent (a wish to enforce traffic laws) while permitting all others. Description 4 then provided the final narrowing. It carved out what we would hope is a very small category of stops when the officer is making a pretextual stop to find and question a suspected murderer. Relying on the officer's state of mind enabled a more finely grained doctrine with the potential for more accurate cost–benefit assessments.

This in turn can lead to police practices that better advance the public interest. The objective rule groups together government acts with bad intents and good intents: It allows both, even though the acts with bad intent are harmful. If states of mind can be accurately determined, the subjective rule will deter officers from the harmful acts associated with bad intents. Relying on subjectivity can permit narrow rules that distinguish good from bad practices with a scalpel instead of a sledgehammer. The subjective rule can minimize how often the harmful, bad-intent acts occur, resulting in law enforcement investigations with more public benefit at lower civil liberties cost.

E. The Difficulty of Determining Government States of Mind

The potential benefit of officer subjectivity is tempered by the widely recognized problem of measurement error.[181] It can be difficult for a court to determine an officer's state of mind.[182] As Justice White complained over a half century ago, "sending state and federal courts on an expedition into the minds of police officers would produce a grave and fruitless misallocation of judicial resources."[183]

The problem derives in part from how courts resolve disputed facts in Fourth Amendment cases. Facts typically will be found after hearings on motions to suppress. The officer will take the stand weeks or months after a search or seizure occurred. A prosecutor will conduct a direct examination followed by a defense counsel's cross-examination. In an adversarial hearing, far removed in time and place from the relevant events, only the officer may know what he had been thinking. If the lawfulness of a government investigation hinges on officer subjectivity, the officer is likely to be keenly aware of which states of mind will lead to victory (a ruling for the

181. *See, e.g.*, Brigham City v. Stuart, 547 U.S. 398, 405 (2006) (concluding that an officer's subjective intent in conducting an exigent circumstances search does not matter, "even if their subjective motives could be so neatly unraveled").

182. *See id.* at 405 (expressing the difficulty in accurately ascertaining an officer's subjective intent in conducting an exigent circumstances search).

183. Massachusetts v. Painten, 389 U.S. 560, 565 (1968) (White, J., dissenting).

government) and which ones may lead to defeat (a ruling for the defendant). This is not an environment particularly conducive to revealing the truth.

Nor is the problem just that some officers will simply lie, although some will. Like everyone else, government officials on the job may act for an inchoate mix of reasons. An officer who pulls over a car with a broken taillight might do so in part to enforce the traffic laws or to question the driver as a suspect in another crime. He might do so in part for an illegitimate reason, such as to engage in racial profiling or harassment.[184] But he might do so in part because he has been instructed to by his boss, because he is expected to make a certain number of stops per day, or because he just thinks it is part of his job.

And he might not know exactly why he did it. As Anthony Amsterdam has pointed out, "[m]otivation is, in any event, a self-generating phenomenon: if a purpose to search for heroin can legally be accomplished only when accompanied by a purpose to search for a weapon, knowledgeable officers will seldom experience the first desire without a simultaneous onrush of the second."[185] Trying to reconstruct a specific state of mind may be trying to create a clarity that never existed.[186]

This doesn't mean that courts can never figure out an officer's mental state. Instead, the challenge typically will vary depending on how specific the subjective inquiry might be. A very narrow subjective test may be difficult to apply while a more general test may be easier. Go back to the traffic stop example. Imagine the subjective test is specific: Did the officer pull over the car with at least in part a genuine wish to enforce the traffic code? That will often be hard to tell, as the stop will objectively look the same with or without that wish. But the picture changes if the subjective inquiry is more inclusive. Say the test asks whether the officer pulled over the car with an intent to obtain information. Answering *that* question will be easy. All of the plausible narratives for an ordinary traffic stop will include that intent.

In general, however, the difficulty of reconstructing officers' states of mind provides a critical cautionary note on the role of subjectivity in Fourth Amendment doctrine. When states of mind can be accurately identified, subjectivity allows courts to use narrower and more specific rules that can impose more precise cost–benefit weighing and thereby achieve more benefits at lower costs. At the same time, inability to determine states of mind

184. This, of course, was the concern of the petitioners in *Whren*. *See* Whren v. United States, 517 U.S. 806, 810 (1996) ("Petitioners, who are both black, further contend that police officers might decide which motorists to stop based on decidedly impermissible factors, such as the race of the car's occupants.").

185. Amsterdam, *supra* note 13, at 437.

186. *See* Stuart, 547 U.S. at 405 (concluding that an officer's subjective intent in conducting an exigent circumstances search does not matter "even if their subjective motives could be so neatly unraveled").

accurately can thwart or even reverse this benefit. A rule that carves out a specific set of cases based on officer intent cannot achieve the needed benefit assessment if the officer's intent can't be accurately identified.

It may be helpful to break down why this is true. The first reason is deterrence. The goal of a subjective rule is to deter officers from engaging in wrongful-intent acts that have low governmental benefit and high civil liberties cost. If courts can identify subjectivity accurately, the officer will know that his bad intent will be sussed out in a suppression hearing. The threat of suppression can discourage the wrongful thought and encourage more beneficial and less harmful police practices. But the prospect of measurement error weakens the deterrent benefits of a subjective rule. It is difficult for courts to deter what they can't identify. The less a court can accurately tell *ex post* whether an officer had a wrongful thought, the less an officer will link the wrongful thought to a risk of suppression *ex ante*.

Second, the remedies of Fourth Amendment law further upset the cost–benefit balance if subjectivity cannot be measured accurately. Consider the effect of the exclusionary rule. If suppression results from a finding of improper intent, but intent cannot be determined accurately, a subjective rule will mean that evidence often will be suppressed when the benefits are likely high (a proper-intent act misinterpreted as an improper one) but can be used when the benefits are likely low (an improper-intent act misinterpreted as a proper one). The result will be less usable evidence and less public benefit of enforcement of the law.

The remedies following from an improper finding of wrongful intent could also over-deter investigations. The prospect of losing evidence even when officers do everything correctly may push law enforcement resources into other enforcement techniques.[187] The prospect of civil liability when an officer is wrongly deemed to have violated the law because of his wrongful state of mind might similarly over-deter officers from investigative steps that rely on a subjective intent rule.[188]

F. An Example

This is all very abstract, so let me show how it works with a stylized example. Let's stick with the *Whren* question of when the police can pull over a car based on a traffic violation. Imagine the Supreme Court is trying to choose among three rules. The first rule is the *Whren* objective rule: probable cause always allows the stop. The second rule is a narrower

187. Investigators generally have multiple ways to collect evidence of different crimes, and they can allocate resources depending on what methods are easy and reliable and which are not. *See, e.g.*, William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1267, 1275–76 (1999).

188. *Cf. id.* (concluding that when the law taxes some kinds of policing more than others, the police will shift time and energy away from more expensive tactics and towards cheaper ones).

subjective rule: probable cause plus an actual intent to enforce the traffic laws allows the stop. And the third rule is a flat ban: probable cause of a traffic violation never allows the stop. Which is the best rule?

Let's fill in some numbers. Assume officers stop cars to enforce the traffic laws (what we can label the "good" reason) 80% of the time. They stop cars to engage in a fishing expedition or for reasons other than enforcing the traffic laws (bad reasons) 20% of the time. Assume that a good stop causes on average 10 utils of public benefit while a bad stop causes on average zero utils of public benefit. Further assume that a good stop causes on average 2 utils of civil liberties harm while a bad stop causes on average 10 utils of civil liberties harm.

Let's start by comparing the objective rule with the ban. Under *Whren*'s objective rule, a court would not distinguish between good and bad reasons for the stop. The average stop will be expected to cause 8 utils of public benefit (10 utils per stop 80% of the time) and 3.6 utils of harm (2 utils 80% of the time and 10 utils 20% of the time) for a net benefit of 4.4 utils. Allowing stops under the *Whren* objective rule leads to more public benefit from enforcement than harm. Under these assumptions, *Whren*'s objective rule is better than the ban.

Now introduce the subjective rule. Assume, for now, that courts can distinguish good intent and bad intent with perfect accuracy. The narrower subjective rule lets courts see two different kinds of stops: Good-intent stops and bad-intent stops. With their perfect ability to distinguish the two, courts can allow stops based on good intent because their benefits (10 utils) far exceed their harms (2 utils). On the other hand, courts can prohibit stops based on bad intent because their harms (10 utils) far exceed their benefits (zero).

Among the three options, the subjective rule is superior. Because courts can distinguish good intent from bad, suppressing the latter, officers will have a strong incentive to only make stops with an appropriate intent. As that number approaches zero, the overall benefit of traffic stops would approach the average of 8 utils from the stops with the lawful intent. The average benefit of a stop would go up (from 8 utils under the objective rule to 10 utils under the subjective rule) while the average harm of a stop would go down (from 3.6 utils under the objective rule to 2 utils under the subjective rule). With bad-intent stops now out of the picture, the net benefit of a stop would jump from 4.4 utils under the objective rule to 8 utils under the subjective rule.

Next remove the assumption that courts can accurately determine an officer's state of mind. Let's assume the worst case, that courts have zero ability to distinguish good from bad intent. The judicial judgment is now a coin flip. Under the subjective legal rule, the officer now faces a 50% chance of a finding of illegality regardless of his intent. Half of the stops with good

intent would be wrongly judged unlawful, and half of the stops with bad intent would be wrongly judged lawful.

Under this assumption, the objective test is superior. The 20% error rate of the objective rule will zoom up to 50% under the subjective rule. And if the benefit of a stop depends on evidence being admissible, and the exclusionary rule applies when a court finds bad intent, the net expected benefit of a stop will decline. When the officer has a good intent, the net benefit will be 8 utils if the court correctly identified the intent but minus 2 utils if the court incorrectly does so. The average benefit of a stop will be 3 for a good-intent stop or minus 10 for a bad intent stop. This would greatly reduce if not eliminate the public value of traffic stops. If 80% of the stops are good intent stops, the average benefit of a stop under a subjective rule is just 0.4 as compared to the flat ban—far below the net benefit of the objective rule.

This example is entirely artificial, of course, with made-up numbers and stylized assumptions. But it's the proof of concept, not the details, that I care about. If courts can accurately identify an officer's state of mind, subjective tests can enable narrow doctrines that accurately select out and discourage harmful practices and improve the net benefits of police practices. On the other hand, when courts cannot identify states of mind accurately, subjective tests can aim for that task but fail, reducing or even eliminating those benefits. Subjective tests may be best if subjectivity can be measured, but objective tests may be better otherwise.

III. Existing Doctrine and the Normative Role of Subjectivity

Part I of this Article described the role of subjectivity in existing doctrine, and Part II offered a normative framework for its use. This Part now puts the two Parts together. Specifically, it asks whether existing doctrine from Part I is plausibly justifiable under the normative standard of Part II. Does existing law make sense? Should the Supreme Court rely on subjectivity more? Or does it use subjectivity too much already?

This section will offer tentative thoughts on several but not all of the doctrines addressed in Part I. My analysis suggests that the choices the courts have made on past doctrine are a mixed bag. The Court's use of a subjective test for searches and seizures seems appropriate, as does its use of subjective tests for special needs and probation searches. The objective test in *Whren* is more difficult to assess, as a subjective test in this context pairs particularly high potential benefit with particularly high risk of measurement error. On the other hand, the Court's reliance on subjective concerns in the exclusionary rule setting is problematic.

A. Searches and Seizures

As Part I showed, existing law on the threshold question of searches and seizures has a modest subjectivity requirement. Government action must include an "attempt to find something or to obtain information" to constitute a Fourth Amendment search.[189] A seizure must be "through means intentionally applied," taking control of property "by the very instrumentality set in motion or put in place in order to achieve that result."[190] It could be argued in both instances that these subjective limits are textually or historically required. (Most obviously, the word "search" may linguistically imply an attempt to obtain information.)[191] But our question is different: Does the subjective requirement of searches and seizures plausibly aid in the cost–benefit function of existing doctrine?

For the most part, I think it does. The intent requirement excludes acts that fail to trigger the balancing of interests Fourth Amendment law contemplates. When the government acts without any intent to control others or collect information, it is not acting in its role as law enforcer or sovereign. An officer who accidentally touches a person while walking through a crowded public event has not taken a step that needs justification from a cost–benefit perspective. Adopting definitions of searches and seizures that exclude accidents allows courts to focus on acts that need justification within the balancing of interests that the law elsewhere presumes.

Further, the nature of the subjective test for searches and seizures makes it relatively straightforward to apply. Searches and seizures typically are distinctive acts, and an officer is likely to lack the intent of obtaining information or taking control through means intentionally applied only in rare accidents or other very unusual circumstances. Take the facts of *United States v. Jones*.[192] It's hard to imagine an officer attaching a GPS device to the underbody of a suspect's car for a reason other than to obtain information. There is similar certainty in *Brower v. County of Inyo*,[193] the roadblock case.

---

189. United States v. Jones, 565 U.S. 400, 408 n.5 (2012). For more in-depth analysis, see subpart I(A).

190. Brower v. County of Inyo, 489 U.S. 593, 597, 599 (1989) (emphasis omitted). For more in-depth analysis, see subpart I(A).

191. As Justice Scalia noted in *Kyllo v. United States*, 533 U.S. 27, 32 n.1 (2001):

> When the Fourth Amendment was adopted, as now, to "search" meant "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to search the house for a book; to search the wood for a thief." N. Webster, An American Dictionary of the English Language 66 (1828) (reprint 6th ed. 1989) (emphasis omitted).

Id. But see Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 70 (2013) ("The word 'search' has several possible meanings. . . . The ambiguity of the word ensures that a wide range of concepts might plausibly define the meaning of searches.").

192. 565 U.S. 400 (2012).

193. 489 U.S. 593 (1989).

A roadblock is a distinctive event. The facts identify its purpose. It's hard to imagine officers creating a roadblock without an intent to stop a car driving on the road. There can be difficult cases, of course.[194] But on the whole, the intent requirement in searches and seizures seems like a plausible aid to the cost–benefit assessment: It narrows the category and the intent usually will be clear.

One oddity amidst the Court's otherwise sensible use of subjective intent in defining searches and seizures is *Florida v. Jardines*.[195] Recall that *Jardines* adopted what looks like a subjective test for the scope of implied license. *Jardines* concludes that a person at home gives implied license to officers to conduct a knock-and-talk, but that the implied license does not extend to officers who have an intent to gather evidence against that person. The person's implied license depends on the officer's intent, with people giving implied license to some intents but not others.

The subjective test in *Jardines* seems difficult to justify under my framework. In narrowing the category, *Jardines* does not draw a plausible line between acts that seem different based on the government interests they advance. An officer seeking eyewitness testimony about a burglar in the neighborhood has the same kind of intent to collect evidence as an officer seeking to gather evidence of a homeowner's crimes. And it's typically hard to know whether an officer approaching a home had an intent that a homeowner might approve. An officer with a trained drug-sniffing dog may have intent to use the dog there. But who knows whether an officer conducting a knock-and-talk is treating the person who answers the door as a suspect? Under my framework, a subjective test in *Jardines* seems problematic.

A possible catch is that the role of intent in *Jardines* may be only a legal fiction. The Court may have been boxed in by doctrine to express an objective test in a subjective way. Here's the context. In *Kentucky v. King*,[196] the Court had blessed the knock-and-talk procedure generally. *Jardines* then concluded that bringing the dogs to sniff went too far. In explaining the line between those two outcomes, the claim that the two scenarios differed based on the officer's subjective intent may have been a useful fiction. It's a fiction

194. Two recent examples are illuminating. First, when a parking enforcement employee "chalks" a tire, is that done to obtain information? In the short term, no, but in the long term, yes: Which perspective controls? *See* Taylor v. City of Saginaw, 922 F.3d 328, 333 (6th Cir. 2019) (concluding that chalking was done to obtain information). Similarly, when an officer places a seized cell phone into airplane mode, is that done to obtain information? *Cf.* United States v. Evans, 780 F. App'x 340, 344–45 (6th Cir. 2019) (finding that an officer's action in placing a seized cell phone into airplane mode would seem to require reasonableness review and remanding to district court for further development of the record). Again, a long-term perspective suggests it is, while a short-term perspective may suggest to the contrary.

195. 569 U.S. 1 (2013).

196. 563 U.S. 452 (2011).

because the Court has never subjected standard knock-and-talks to the same subjective test. It has simply assumed that a homeowner would welcome a knock-and-talk as friendly, when often that will be untrue.[197]

The idea that the intent test is a fiction in *Jardines* is bolstered by the last line of the Court's analysis: bringing the dog was unlawful, the Court says, because it "objectively reveals a purpose to conduct a search, which is not what anyone would think he had license to do."[198] This reading of *Jardines* suggests the test may not be subjective at all. Perhaps the distinction is whether the objective facts can only be explained as "snooping" about[199] or look inconsistent with speaking to the person at home in a way a homeowner might want. It is objective behavior, not subjective intent, that counts.

B. Reasonableness

Now turn to the role of subjectivity in reasonableness doctrine. Here existing doctrine strikes me as a mixed bag. In some instances, its use is readily justifiable by the cost–benefit framework advanced in this Article. In other cases, its use is questionable or dubious. In particular, reliance on subjectivity seems appropriate in the special-needs cases and in probation and parole cases. The benefits of subjectivity in these contexts are clear and the risk of error low. On the other hand, *Whren* is a harder case. The theoretical payoff of a subjective approach in *Whren* is extremely high, but the risks of measurement error are also great.

Start with the Court's use of modified subjectivity in the context of roadblock programs such as those in *Indianapolis v. Edmond* and *Sitz*.[200] Recall that, in those cases, the Court relied on the "programmatic purpose" of the roadblock programs to see if they were enacted for a special need.[201] This seems appropriate, in my view. Reliance on programmatic purpose allows the Court to adopt narrower rules that distinguish roadblocks designed to advance special needs from ordinary law enforcement programs. Absent reliance on subjectivity, the Court would have to treat roadblocks as all-or-nothing: It would have to group together genuinely safety-related programs and standard-issue law enforcement. Reliance on programmatic purpose allows the Court to adopt a more finely grained rule that allows reasonable safety-related programs while prohibiting the rest.

---

197. *Cf.* Illinois v. Wardlow, 528 U.S. 119, 132–35 (2000) (Stevens, J., dissenting) (noting the distrust among many of the police, "particularly [among] minorities and those residing in high crime areas").

198. *Jardines*, 569 U.S. at 10.

199. *Id.* at 9 n.3.

200. *See supra* subpart I(B).

201. *See id.*

Further, accurately identifying whether the programmatic purpose of a roadblock falls within a special need seems achievable. When the government has a special program that focuses resources in a particular way at a particular time and place, someone must have directed that program. Managerial decisions will have been made, and records likely kept, that should make it possible to reconstruct the programmatic purpose in most cases through discovery and affidavits. In this context, relying on the modified subjectivity of the "programmatic purpose" doctrine allows a narrow rule that seems relatively reliable to apply correctly.

A subjective test also seems proper in the context of probation and parole searches. As Part I showed, lower courts have required officers to have prior knowledge of a person's special status as a parolee or probationer, as well as knowledge of the search terms of a person's parole or probation agreement, to trigger the more deferential Fourth Amendment rules for probationers and parolees.[202] This is an appropriate knowledge test that correlates with intent. It allows courts to limit the deferential rules for probation and parole searches to cases genuinely advancing those interests, and it does so using a subjective test that is likely to be measured accurately.

Consider the two parts of the framework. First, knowledge limits the deference trigger to contexts when the search is most likely to advance the interests that justify deference. Think about the flip side. An officer who doesn't even realize that a search target has a special status as parolee or probationer obviously isn't trying to advance the government's interest in monitoring parolees or probationers by conducting the search. To that officer, the later realization of the target's special status merely raises the prospect of a windfall.

A knowledge requirement for parole and probation searches is also likely to be applied accurately. In most cases, it should be possible to tell whether an officer knew a suspect's probation or parole status and the terms of their agreement. Obtaining that knowledge usually requires checking a file. In most cases, it will be easy to tell whether an officer checked the file and knew its contents before the search or only learned that information afterwards. The ability to identify knowledge in most cases makes a knowledge test relatively reliable, justifying a subjective test to trigger the probation and parole rules.

But what about *Whren*? Should courts consider an officer's pretextual purpose as part of the reasonableness of a traffic stop? I have mixed views.

---

202. *See* United States v. Caseres, 533 F.3d 1064, 1075–76 (9th Cir. 2008) (holding that an officer must be aware of search condition to justify search under parole search rules); Moreno v. Baca, 431 F.3d 633, 639 (9th Cir. 2005) (holding that officer must be aware of parole status to rely on parole search rules); State v. Brusuelas, 219 P.3d 1, 5 (N.M. Ct. App. 2009) (emphasizing the importance of officer knowledge of probation condition in analyzing whether probation search rules apply).

On one hand, it would be extremely helpful for courts to be able to distinguish good-faith from pretextual traffic stops. An officer's motive in making a traffic stop likely correlates strongly with the interests that the stop advances. A stop motivated by an officer's genuine wish to enforce the traffic laws is likely to advance the public interest in enforcing the traffic laws. A stop motivated by other reasons is not.

The public interest in identifying pretextual traffic stops is particularly great in the context of racially discriminatory enforcement. Our country's continuing failures to come to grips with racially discriminatory policing and the great harms that policing has caused make a rule that distinguishes stops motivated by good-faith government interests from those motivated by discrimination very appealing. If courts could accurately identify an officer's discriminatory intent during a stop, then courts could invalidate stops made with harmful intent and permit stops made without it.

The problem is that it is particularly difficult to know an officer's state of mind in making a traffic stop. Traffic stops are routine police actions, not special programs, which makes it unlikely that there would be a reliable programmatic purpose to invoke. And no one but the officer who had probable cause to make the stop is likely to know with any reliability whether it was made for traffic or non-traffic reasons. To an outside observer, traffic stops made for pretextual and non-pretextual reasons will look mostly identical. Reliably distinguishing stops based on officer purpose seems particularly difficult.

The difficulty is particularly great in the context of discriminatory enforcement. An officer who pulls over a car to harass a motorist is extremely unlikely to admit that goal on the witness stand. Statistical evidence could be used to show a general trend of officers pulling over more minority motorists than facts justify.[203] Data could even be produced about the racial composition of the drivers that a particular officer stopped.[204] But generalized statistical evidence is an awkward fit for a doctrine based on an officer's state of mind at a particular time: It will be difficult to know based on general statistics to what extent any particular stop was racially motivated.[205]

---

203. *See, e.g.*, WILLIAM R. SMITH, DONALD TOMASKOVIC-DEVEY, MATTHEW T. ZINGRAFF, H. MARCINDA MASON, PATRICIA Y. WARREN & CYNTHIA P. WRIGHT, THE NORTH CAROLINA HIGHWAY TRAFFIC STUDY 345–46 (2003), https://www.ncjrs.gov/pdffiles1/nij/grants/204021.pdf [https://perma.cc/75BR-FKQR] ("Adjusting for response bias . . . , the data suggests that African Americans are actually 1.65 times as likely [as whites] to have been stopped in the last year.").

204. For example, in *United States v. Buford*, No. 1:20CR54RLW(SPM), 2020 WL 5413528 (E.D. Mo. Aug. 19, 2020), the government produced data about the racial composition of the individuals stopped by the detaining officer during both the year and the week preceding the stop in question. According to that data, 32.4% of the officer's stops in the prior year were of black motorists, while 55% of the officer's stops in the prior week were of black motorists. *Id.* at *5.

205. For example, in *Buford*, the magistrate judge was reluctant to conclude that this data showed that the stop of Buford was done on the basis of his race: In rejecting reliance on the

It's possible that technology might help courts identify a discriminatory intent. Today's traffic stops are often recorded by police cameras.[206] The presence of audio or video recording the stop may make it easier to discern some kinds of intent. For example, an officer who makes a speeding stop and quickly launches into a series of questions about an unrelated crime is likely to have made a pretextual stop. Is it possible that, *ex post*, a judge could tell from listening to the audio of the officer's questions whether the officer had a different goal in making the stop? Perhaps—although the same inquiry could be easily gamed or explained away by an officer.

A more promising approach might be an objective rule designed to capture the subjective concern with discriminatory enforcement. For example, Professor Amsterdam once proposed dealing with the harms of pretextual *Terry* frisks with a suppression rule: *Terry* frisks should be permitted, but the fruits of such searches—other than weapons—should be suppressed.[207] Courts could adapt this approach for traffic stops. For example, perhaps stops could be allowed under *Whren*, but only evidence of the traffic violation could be admitted. The rule would be objective, but its goal would be discouraging stops made for improper subjective reasons.

C. Remedies

The use of subjective standards for the exclusionary rule seems particularly problematic. As Part I showed, recent doctrine has focused on officers' states of mind toward the legality of their acts.[208] If the officer deliberately violated Fourth Amendment law, the act is culpable and the exclusionary rule is likely to apply.[209] On the other hand, if the officer had a good-faith belief that his act was legal, or the violation was merely part of a garden variety and non-systemic negligence, the act is less culpable, and suppression is less likely.[210]

In my view, this approach is dubious. The aim of relying on an officer's mental state is commendable. But it is particularly difficult for courts to identify an officer's state of mind (and the broader practices of law

---

numbers, the court noted that "there was no expert testimony or other information provided to the Court to explain or otherwise contextualize the information." *Id.*

206. *See generally* BARRY J. POLLACK, GERALD B. LEFCOURT, E.G. "GERRY" MORRIS, NORMAN L. REIMER, KYLE O'DOWD & JUMANA MUSA, POLICING BODY CAMERAS: POLICIES AND PROCEDURES TO SAFEGUARD THE RIGHTS OF THE ACCUSED (2017), https://www.bja.gov/bwc/pdfs/BWC-NACDL-March2017.pdf [https://perma.cc/AB6L-W3R5] (summarizing the criminal defense bar's findings on the effectiveness of body cameras and offering recommendations to increase police accountability and protect the rights of the accused).

207. *See* Amsterdam, *supra* note 13, at 437–38 (explaining how an exclusionary rule would reduce undesirable incentives for police officers to conduct unconstitutional searches and seizures).

208. *See supra* subpart I(C).

209. *See supra* subpart I(C).

210. *See supra* subpart I(C).

enforcement) toward legal violations. Relying on officer intent in the exclusionary rule setting triggers many of the same difficulties as it does in the *Whren* setting. And the exclusionary rule context also brings additional challenges, owing to the specific problem of trying to assess culpability in a multimember law enforcement structure using tools generally designed to determine a single officer's state of mind.

At the outset, we can appreciate the goal of relying on officer *mens rea* in the exclusionary rule setting. The Court has defended its focus on officer subjectivity based on notions of culpability and deterrence. An officer who has intentionally violated the law can be easily deterred, the thinking runs. In contrast, it is difficult to deter mere negligence or even an entirely innocent legal violation.[211] We can reframe the Court's thinking using this Article's approach by recognizing that a subjective test can allow a narrower and more focused remedy.

To see this, imagine you think that suppression for intentional violations would have major deterrent payoff while suppression for merely negligent violations would have little or no deterrent payoff. If that is true, a test that hinges on officer *mens rea* helpfully allows courts to distinguish the two. Courts don't have to lump all violations together, either adopting a suppression remedy for all of the violations or for none of them. Instead, they can apply the exclusionary rule when the payoff is highest while rejecting suppression when the payoff is lower, zero, or even a net negative. Assuming that the costs and benefits actually play out that way—which is hardly clear, but an assumption beyond the scope of this Article—a subjective approach permits a narrower rule that produces greater public benefit at lower cost.

This salutary goal is unfortunately very likely to go unmet, however, owing to the difficulty of determining the relevant mental states accurately. The first problem is the same one that makes a subjective intent test for racial discrimination in *Whren* cases so difficult. An officer who suspects or knows that he is violating the law is unlikely to admit it, and there is normally no way to tell other than through his own testimony. Imagine an officer who decides to make an arrest knowing he lacks probable cause because he wants to remove a person from the scene and doesn't care if evidence found in a search incident to arrest is later suppressed. The officer will not announce his legal conclusion, or otherwise act in an outward way any differently. Instead, the officer will follow the usual arrest procedure and keep his state of mind to himself. In that setting, a subjective test is as difficult to apply accurately as it is in the traffic-stop context of *Whren*.

Determining mental states in the exclusionary rule setting is even more challenging because law enforcement is a "they," not an "it." An individual officer who conducts a search or seizure may not be fully or even partially

211. *See supra* subpart I(C).

responsible for the decision to do so. Perhaps he was advised to search by another officer. Perhaps a judgment to make an arrest was made by a team of lawyers or other advisors. When decisionmaking power to search or seize is divided among different actors, the notion of mental states with respect to legality is tricky. It forces courts to adopt one of two approaches, both of which are plagued with measurement difficulties.

The first approach is the macro perspective, which looks at law enforcement as a whole and determines its culpability. The Supreme Court suggested this approach in *Herring v. United States*,[212] the case of an arrest based on an erroneous entry in a police county database. According to the Court, suppression could be appropriate if a defendant showed that error involved "recurring or systemic negligence," rather than merely "isolated negligence," depending on whether "errors in [the] County's system [we]re routine or widespread."[213]

This is a test that is particularly difficult to apply. The defendant has the burden of proof.[214] But how can a defendant establish that a broader law enforcement "system" as a whole had widespread errors? The defendant likely will have neither the legal nor financial means to conduct a broad review of the relevant law enforcement system. A defendant can place an officer on the stand, and that officer presumably will testify (as did the officers in *Herring*[215]) that the system is quite reliable. But it's hard to see how that claim can be tested, and the broader system evaluated, in the context of a suppression motion.

Equivalent problems also arise under a micro approach, in which we look at the culpability only of the officers who conducted the search or seizure. An officer may have been advised to conduct the search by others who are aware of the possible or likely illegality of the search but who deem the risk acceptable. In that case, the officer who actually conducts the search may lack a culpable mental state even if others in the system did have a culpable mental state.

We saw this dynamic in recent litigation over the Playpen warrant.[216] The Playpen warrant authorized installation of software on the computers of visitors to a child pornography site on the dark web.[217] In colloquial terms, the software hacked into the computers of visitors, searching thousands of different machines in places unknown. We know from the extensive litigation

212. 555 U.S. 135 (2009).

213. *Id.* at 137, 144, 146–47.

214. *See* LAFAVE, *supra* note 67, at § 3.1.

215. *Herring*, 555 U.S. at 147.

216. *See* Transcript of Motion hearing at 44–46, United States v. Anzalone, 221 F. Supp. 3d 189 (D. Mass. 2016) (No. 15-10347-PBS) (discussing how an FBI agent was directed to execute a search warrant by multiple levels of management in the FBI and Department of Justice).

217. *Id.* at 46, 62.

over the warrant that it was authorized by a team of high-level lawyers within the executive branch who carefully considered the legal risks of going forward with the warrant application.[218] And indeed, courts later held that the warrant violated the Fourth Amendment.[219] But at least some of the courts that have applied the good-faith exception have assumed the application was made only by the line attorney and FBI-agent affiant and considered their culpability in isolation.[220] The risks and deliberative process of the actual decisionmakers were not even considered.

Conclusion

In a recent concurrence in *District of Columbia v. Wesby*,[221] Justice Ginsburg called on her colleagues to rethink the persistent objectivity of Fourth Amendment law. Fearing that the objective approach "sets the balance too heavily in favor of police unaccountability to the detriment of Fourth Amendment protection," Justice Ginsburg called for the introduction of some subjective standards to restore the balance.[222] "I would leave open, for reexamination in a future case," she explained, "whether a police officer's reason for acting, in at least some circumstances, should factor into the Fourth Amendment inquiry."[223]

The good news for Justice Ginsburg is that the government's reason for acting already factors into the Fourth Amendment inquiry in a wide variety of circumstances. Although the Supreme Court talks a good game about the objective standards of Fourth Amendment law, the cases, especially recent ones, often embrace officer subjectivity. An officer's thoughts and goals are relevant to what counts as a search or seizure, to constitutional reasonableness, and to the scope of remedies. Although the Court has not articulated a consistent theory of why it sometimes chooses objective tests and why it sometimes picks subjective tests, it's important to see that the Justices are making a choice. Fourth Amendment law is not unquestionably objective. It is a mix, and the Justices choose in each case whether a particular doctrine is appropriately objective or subjective.

---

218. *See id.* at 43–46 (discussing the interagency deliberative process that led to the approval of the Playpen warrant).

219. *See, e.g.*, United States v. Taylor, 935 F.3d 1279, 1284 (11th Cir. 2019) (noting that lower court decisions for this case held that the warrant violated the Fourth Amendment).

220. *See, e.g.*, *id.* at 1291, 1292 n.14 (focusing on the awareness of the agent and prosecutor who applied for the warrant).

221. 138 S. Ct. 577 (2018).

222. *Id.* at 594 (Ginsburg, J., concurring in the judgment in part).

223. *Id.*

The framework offered in this paper can help courts choose between the two approaches. A subjective approach is useful when it allows courts to adopt narrower rules that can distinguish more harmful police practices from less harmful ones. In that setting, relying on subjectivity can ensure a greater public benefit in enforcement at a lower civil liberties cost. At the same time, the benefits of subjectivity have to be weighed against the challenge of making reliable mental state determinations. Mental states are not monolithic. A subjective approach is preferable only if mental states can reliably distinguish more harmful practices from less harmful ones. The best path forward is for courts to make context-sensitive decisions based on the potential benefits of narrower subjective rules and the ease of determining intent in suppression hearings.