Saint Louis University Law Journal

Volume 66
Number 4 *Critical Race Theory and the Law (Summer 2022)*

Article 8

2022

Preservation Letters and Fourth Amendment Seizures: A Response to Professor Kerr

Michael L. Levy
University of Pennsylvania Carey Law School, mikel31556@gmail.com

PRESERVATION LETTERS AND FOURTH AMENDMENT SEIZURES: A RESPONSE TO PROFESSOR KERR

MICHAEL L. LEVY*

ABSTRACT

The Stored Communications Act (18 U.S.C. § 2701 et seq.) requires an Internet Service Provider to preserve the contents of a user account upon receiving a request from a government agency. The maximum period of preservation is 180 days. However, the government agency cannot get access to the copy, unless it presents proper legal process, usually a search warrant. During this time, the user has complete access to their account. In a recent article, Professor Orin Kerr has advanced a thesis that copying pursuant to the government's preservation requests under the Stored Communications Act is a Fourth Amendment seizure. This Article disputes Professor Kerr's argument. It does so on his terms, that digital copying is a meaningful interference with a possessory interest in property, but also advances a new theory of seizure in the digital world. This theory is premised on the idea that unlike physical seizures, which interfere with a possessor's access to the tangible objects seized, digital copying does not. The real concern with digital copying is the privacy of the data. Although privacy is usually the concern of the law of searches, this Article advances the idea that when we analyze the concept of seizure with respect to the copying of digital evidence, it is the owner's privacy interest in the data, and not their access to it, that we need to address. Viewed from a privacy perspective, preservation requests are not seizures.

* Mr. Levy is an adjunct Professor of Law at the University of Pennsylvania Carey Law School. He was an Assistant U.S. Attorney in the Eastern District of Pennsylvania for thirty-seven years and served as the Chief of Computer Crimes before retiring in 2019. He twice served as interim U.S. Attorney. The author thanks Assistant U.S. Attorneys Paul Shapiro, Albert Glenn, and Robert Livermore from the Eastern District of Pennsylvania, Josh Goldfoot and Nathan Judish from the Computer Crime and Intellectual Property Section of the U.S. Department of Justice, Professor David Rudovsky, University of Pennsylvania Carey Law School, and Professor Orin Kerr, University of California, Berkeley Law School for their helpful comments and suggestions during the drafting of this Article.

INTRODUCTION

In a recently published article,[1] Professor Orin Kerr expands upon his theory of Fourth Amendment seizure in the digital world that he advanced in *Fourth Amendment Seizures of Computer Data*.[2] In 2010, Professor Kerr examined cases involving the copying of data and concluded that they were seizures, even though in the physical world sense, the act of copying did not seem to result in a "meaningful interference with an individual's possessory interests in that property."[3] In his new article, Professor Kerr develops an idea that he advanced in 2010—the Stored Communications Act section that permits the government to require an Internet Service Provider to preserve a copy of a suspect's account is a seizure,[4] even though the government cannot get access to the contents of this copy.[5] In this Article, the author suggests that Professor Kerr is mistaken,[6] doing so by two methods. First, taking Professor Kerr's use of the traditional definition of seizure to cover digital copying, the author argues that a preservation letter does not act as a seizure. Second, the author suggests that Kerr's two articles are premised on a view of seizure of data that is wrong. Kerr's definition of seizure of data looks to the physical world cases.[7] However, the concerns about physical world seizures are about access to and control of objects.[8] This author suggests that the concerns about copying of data are not about access and control but are about privacy—the usual concern of search law, not seizure law. Once we acknowledge that, we can develop a more coherent view of digital seizures. Using such an analysis, a preservation letter is not a seizure.

This Article has several parts. Part I discusses Professor Kerr's theory of seizure. The second part will propose a different way of analyzing digital copying, based upon what the author suggests is the real concern—privacy and not possession. Part II further explains the thesis: our concern with digital copying is not with the deprivation of a possessory interest in the data, but in the privacy interest. The author suggests that this way of approaching the problem does a better job of explaining why photographing a scene is not a seizure and why copying by a government router on the Internet is not a seizure. Professor Kerr's 2010 article creates ad hoc exceptions for these two types of copying

1. Orin S. Kerr, *The Fourth Amendment Limits of Internet Content Preservation*, 65 ST. LOUIS L.J. 753 (2021) [hereinafter Kerr 2021].

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

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

4. 18 U.S.C. § 2703(f).

5. Kerr 2021, *supra* note 1.

6. As someone who has read Professor Kerr's writings frequently, and who uses his textbook to teach, this author writes this with much trepidation.

7. Kerr 2021, *supra* note 1.

8. *Id*.

because under the traditional definition, they are seizures. The theory advanced here requires no special adjustments. Part III summarizes the workings of Section 2703 and the preservation section, subsection 2703(f). Part IV discusses Professor Kerr's position that a preservation letter is a seizure and shows that whether employing the traditional view or a privacy view of seizure, a preservation letter is not a seizure. Finally, Part V discusses the only type of data subject to suppression under Professor Kerr's theory—data that a user sought to delete after the provider copied the account pursuant to the preservation letter. This discussion applies both the physical seizure analysis employed by Professor Kerr and the privacy analysis advanced in Part II to argue that no seizure occurs. The idea implicit in Professor Kerr's argument is that there is a right to delete, and this author argues that there is no such right.[9]

I. PROFESSOR KERR'S POSITION THAT PRESERVATION IS A SEIZURE

The problem of conceptualizing digital seizures is best illustrated by the case of *United States v. Gorshkov*.[10] The FBI had identified Gorshkov as a Russian hacker who had gained access to American businesses, then set up an undercover business and invited Gorshkov to the United States under the pretext of retaining him for computer security.[11] Gorshkov flew to Seattle, where the FBI agents took him to the office of the undercover business and provided him with a computer so he could demonstrate his skills.[12] He used the computer to log into his account in Russia, downloaded some of his hacker tools, and demonstrated his skills.[13] As he left, the agents arrested him.[14] The agents had installed a keylogger on the computer they had given to him.[15] They obtained his password from the keylogger, logged into his Russian Internet account, and downloaded the contents.[16] The FBI did not obtain a warrant until after they had obtained the contents.[17] Gorshkov's motion to suppress was denied, in part because the court found that making a copy of his account

> [W]as not a seizure under the Fourth Amendment because it did not interfere with Defendant's or anyone else's possessory interest in the data. The data remained intact and unaltered. It remained accessible to Defendant and any co-

9. Kerr 2021, *supra* note 1.

10. United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

11. *Id*. at *1.

12. *Id*.

13. *Id*.

14. *Id*.

15. United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *1 (W.D. Wash. May 23, 2001).

16. *Id*.

17. *Id.* at *1–2.

> conspirators or partners with whom he had shared access. The copying of the data had absolutely no impact on his possessory rights.[18]

This definition of seizure comes from *United States v. Jacobsen.*[19] The result in *Gorshkov* was a straightforward application of *Jacobsen.* As such, it is correct. However, it feels intuitively wrong. How can a law enforcement agency obtain a copy of a person's data—that it did not have before—and not have seized it?

A more sophisticated effort to wrestle with the issue can be found in *United States v. Jefferson.*[20] There, FBI agents executing a search warrant viewed certain records that they chose not to seize.[21] The agents believed that they could take these documents under the plain view doctrine,[22] but following the directions of the Assistant U.S. Attorneys, opted to take high resolution photographs of thirteen documents or to make handwritten notes based upon their review.[23] At a hearing on a motion to suppress, the government conceded that two of the documents were not within the scope of the warrant and could not be seized.[24] The court ruled that the other documents could have been taken under the plain view doctrine.[25] To reach that conclusion, the court first had to decide if taking high resolution photographs or making notes constituted a seizure of the documents.[26] Making a deeper analysis of what it means to "seize" an intangible,[27] the court referenced *Hoffa v. United States,*[28] *Katz v. United States*,[29] and *United States v. New York Telephone Co.*[30] for the proposition that intangibles, such as words and electronic signals, could be "seized" within the meaning of the Fourth Amendment. Although *Arizona v. Hicks* held that copying of a serial number on a piece of equipment was not a seizure,[31] the court found that *Hoffa*, *Katz,* and *New York Telephone Co.* were more pertinent to the problem. Thus, the court held that photographing a document and taking notes about a document's contents were seizures,[32] and explained that these cases

> [R]ecognize that the Fourth Amendment privacy interest extends not just to the paper on which the information is written or the disc on which it is recorded but

18. *Id.* at *3.
19. 466 U.S. 109, 113 (1984) ("A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property.").
20. United States v. Jefferson, 571 F. Supp. 2d 696 (E.D. Va. 2008).
21. *Id.* at 699–700.
22. Horton v. California, 496 U.S. 128, 131 (1990).
23. *Jefferson,* 571 F. Supp. 2d at 700.
24. *Id.* at 711.
25. United States v. Jefferson, 571 F. Supp. 2d 696, 711 (E.D. Va. 2008).
26. *Id.* at 701.
27. *Id*.
28. 385 U.S. 293, 301 (1966).
29. 389 U.S. 347, 353 (1967).
30. 434 U.S. 159, 169 (1977).
31. 480 U.S. 321, 325 (1987).
32. United States v. Jefferson, 571 F. Supp. 2d 696, 704 (E.D. Va. 2008).

> also to the information on the paper or disc itself. It follows from this that recording the information by photograph or otherwise interferes with this possessory privacy interest even if the document or disc is not itself seized.[33]

The court expressed a critical insight—the central principle of this Article:

> In other words, while copying the contents of a person's documents by way of photographs or written notes does not interfere with a person's possession of those documents, it does interfere with the person's sole possession of the information contained in those documents: it diminishes the person's privacy value in that information.[34]

Judge Ellis had it right in *Jefferson*. When the drafters of the Fourth Amendment wrote about "papers and effects," they were not concerned about blank sheets of foolscap.[35] They were concerned about what they had written to one another on those sheets.[36] It was the privacy of the content that mattered to them.[37] In twentieth and twenty-first century terms, it is not the possessory interest in papers that is the concern, it is the privacy interest.

In his 2010 article, Professor Kerr proposed that such copying was a seizure under the Fourth Amendment, writing:

> In my view, the most consistent way to apply the Fourth Amendment seizure doctrine to computer data is to hold that electronic copying ordinarily seizes it under the Fourth Amendment. When the government makes an electronic copy of data, it obtains possession of the data that it can preserve for future use. To be sure, subsequently viewing the data in the copy and thus exposing its contents ordinarily amounts to a Fourth Amendment search. But obtaining the copy itself serves the traditional function regulated by the seizure power: it freezes whatever information is copied, preserving it for future access by government investigators. Generating an electronic copy of data freezes that data for future use just like taking physical property freezes it.[38]

Professor Kerr then had to deal with two anomalies created by his application of the traditional physical world definition to digital copying. The first was copying what the agents could already see. In *Hicks*, the agents looked at a stereo and copied down the serial number.[39] The Supreme Court held that

33. *Id*. at 702.

34. *Id.* at 703.

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

36. *See* Boyd v. United States, 116 U.S. 616, 625–39 (1886).

37. *Id.* at 630 ("Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony, or of his private papers to be used as evidence to convict him of crime, or to forfeit his goods, is within the condemnation of that judgment.").

38. Kerr 2010, *supra* note 2, at 711–12.

39. Arizona v. Hicks, 480 U.S. 321, 321 (1987).

writing down the serial number was not a seizure.[40] In *Bills v. Aseltine*,[41] the agents took photos of a search scene. The Sixth Circuit held that this was not a seizure.[42] These were common sense decisions, but if one said that copying information is a seizure, these cases would seem to be seizures. Professor Kerr's solution was to divide copying, which was an aid to the memory of the agent, recording what law enforcement had already seen as in *Hicks* and *Bills*, from copying without seeing the data, for the purpose of freezing it.[43] Digital copying is freezing and not an aid to memory.[44] Therefore, digital copying is a seizure; writing down or photographing what the agent had already seen is not.[45]

The other anomaly was the actions of government routers on the Internet. Routers on the Internet copy the data that they receive and send it on.[46] They retain it for short periods in case the routers downstream did not receive the communication.[47] Professor Kerr noted that such copying did not interrupt the usual course of transmission.[48] He compared the Internet router to detained packages, noting that when a package is detained in transit, the government's action interferes with the course of transmission, but the copying by the Internet router did not.[49]

The strict application of Professor Kerr's theory would prohibit law enforcement officers from taking photos of crime scenes, photos of their execution of search warrants, copying serial numbers, and the actions of government routers on the Internet. To avoid these untoward results, Professor Kerr created ad hoc distinctions for cases which either made no sense (*Hicks* and *Bills*), or which would effectively require rethinking having government routers on the Internet.[50] These are, however, "fudge factors"—ad hoc rules to render certain acts of copying not seizures—and do not arise from the definition of seizure. It was not that taking photos of a search scene or the use of government routers on the Internet did not fit the definition of seizure; it was that calling them seizures felt ludicrous. This solution is reminiscent of the efforts to preserve the geocentric view of the universe as evidence grew that the earth circled the sun and not vice versa. Scientists created concepts, such as

40. *Id.*
41. 958 F.2d 697, 700 (6th Cir. 1992).
42. *Id.* at 707.
43. Kerr 2010, *supra* note 2, at 717.
44. *Id*.
45. *Id*.
46. *Network Fundamentals—Switches, LANs, Routers, and Other Networking Devices,* UNIV. HOUS. (2022), https://www.uhcl.edu/information-security/tips-best-practices/routers [https://perma.cc/RA62-AU8X].
47. *Id*.
48. Kerr 2021*, supra* note 1, at 787–88.
49. Kerr 2010, *supra* note 2, at 720–24.
50. *Id.* at 714–15.

epicycles,[51] to explain the evidence, but it only made the system more complicated. Creating ad hoc exceptions—fudge factors—does not make for a consistent body of law.

II. A PRIVACY APPROACH TO SEIZURES OF DATA

A. The Theoretical Framework

A better solution to the problem of copying is to examine the underlying concerns about physical seizures versus data copying, because they are different. These differences should prompt a reexamination of what constitutes a seizure in the digital world. What troubles us about government copying of data is not the owner's possessory interest in the data. We are not concerned that the government will sell the data or otherwise make economic use it. That may be the concern of the copyright holder, but it is not the concern of the average person over the contents of their e-mail, Facebook messages, or Dropbox account. Nor are we concerned that the owner has lost access to the data. What concerns us is the privacy interest. If the government has a copy of the data, it can search it. While the government did not search Gorshkov's data until after it obtained a warrant, there was the potential for a warrantless search.[52] It is this privacy concern that makes *Gorshkov* feel wrong.[53] Similarly, we feel that the court got the concept right in *Jefferson* when it recognized that making a perfect copy of a document should be a seizure, even if the police leave the physical paper behind when they depart.[54] As the court in *Jefferson* said, the concern is not with the possession of the document, the concern with copying is that "it diminishes the person's privacy value in that information."[55]

The concern with physical world seizures is different. If the police seize one of your possessions, they have it; you do not. You are unable to make any use of the physical property.[56] When the police copy data, whether it is copying a computer hard drive or having an Internet Service Provider make a copy, there is no meaningful interference with the use of property. Our concern is with the police looking at it.

51. *See* Alexander Raymond Jones, *Ptolemaic System*, ENCYC. BRITANNICA (May 19, 2020), https://www.britannica.com/science/Ptolemaic-system [https://perma.cc/2CAK-DL7W].

52. United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026, at *1 (W.D. Wash. May 23, 2001).

53. *Id*. at *1–2.

54. United States v. Jefferson, 571 F. Supp. 2d 696, 703 (E.D. Va. 2008).

55. *Id.* at 702.

56. When the police seize a container (i.e., suitcase, backpack, cell phone, computer) the concern is both with the possessory interest in the property and the privacy interest in what is in it. Thus, the Supreme Court ruled that the seizure of Riley's telephone was proper because it was taken incident to arrest. It was the privacy concerns that led the Court to require a warrant to copy and search the data inside it. Riley v. California, 573 U.S. 373, 403 (2014).

Kerr argues for the traditional definition of seizure, but with digital data, he focuses on exclusivity of possession when stating: "The question is, should the law focus on when a person loses exclusive rights to the device, or when a person loses exclusive rights to the data? The law should focus on when the person loses exclusive rights to the data."[57] However, the concern about someone else having a copy of our data is not like that of a copyright holder, concerned that the wrongful possessor will make money from it. Our concern about exclusivity of possession is, at its heart, a concern about our privacy in the data. We alone should determine who gets to see our data. Absent some good reason (for example, probable cause), we should determine whether the government can get to see it.

For this reason, we need to recast what is a seizure of data. This author proposes the following:

> A digital seizure occurs when the government copies data (whether it exists in electronic or physical format) for the purpose of letting a law enforcement officer view the data, which the law enforcement officer has not previously been able to view, if the law enforcement officer has ready access to the data as a result of the copying.[58]

When the officer has already been able to view the data, the privacy interest was lost before the copying. Thus, copying the serial number, in *Hicks*,[59] or taking a photo of a search scene, in *Bills*,[60] were not seizures because the police had invaded the privacy interest before they made the copy. The same definition takes care of the government router on the Internet. The router does not copy the data for any human to see. For that reason, the copying by the router is not a seizure.[61]

For the most part, the definition proposed here and Professor Kerr's reach similar results. The copying of Gorshkov's account would be a seizure under either test. Those documents that the agents perused in *Jefferson* and then photographed or described in notes would not have been seized because they had already reviewed them. If the warrant covered those items, or if they could be properly seized under the plain view doctrine, any seizure (physically or digitally) would be proper. On the other hand, if the agents in *Jefferson* had photographed documents without reading them, their actions would have been a seizure.

57. Kerr 2010, *supra* note 2, at 712.

58. Viewing includes any form of human perception—sight, hearing, etc. Taste, smell, and touch are not yet realities on the Internet, but who knows what will be available in twenty years.

59. Arizona v. Hicks, 480 U.S. 321, 325 (1987).

60. Bills v. Aseltine, 958 F.2d 697, 700 (6th Cir. 1992).

61. This is the old conundrum whether a tree falling in the forest makes a sound if no one hears it. In this case, the author suggests that the answer is that if no one hears it, or will hear it, nothing has been seized.

The *Jefferson* case does raise a problem that was not involved in its facts. Suppose the agents had looked at a document, concluded it was not within the scope of the warrant or the plain view exception, but photographed it anyway. Did the agents' review of the document remove the privacy right, and does that mean that the photographing is not a seizure? Although the answer is not clear, this author suggests that such copying would not be proper because the original, permissible invasion of the privacy right was very limited. In searching for paper (or digital) files, the law only permits a cursory review to determine if the document is within the scope of the warrant.[62] Although this causes some loss of privacy, the loss is only sufficient to determine if the document is within the scope of the warrant. If a quick scan shows that it is not, the agent must stop reading and move on. Making a copy under these circumstances is a much larger invasion of privacy than permitted by the search authority. The agents should be permitted to make notes that are consistent with what they permissibly saw. For example, during a home office search in the investigation of a fraud case, the agent could note that she came across a copy of the subject's will. The preservation here would match the permissible invasion of privacy and no more. A detailed description of what the subject had bequeathed and to whom would not be proper, unless the agent could seize the will under the warrant. That copying would be a greater invasion of privacy than the law permitted.

Both Kerr's rule and this one also resolve the question of what part of the Fourth Amendment was implicated when the Supreme Court wrote in *Katz*, "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[63] The Court never said whether it was a search or a seizure.[64] Using either test, copying the words spoken by Katz inside the telephone booth was done to hear words the government had not heard before.[65] Under Professor Kerr's test, this was to freeze Katz's words.[66] Under the test proposed above, it is a seizure because the government had no access to Katz's words before the event in question. Using the traditional concept of seizure as Professor Kerr does, the recording of Katz's voice might also have been a seizure because the government had an unauthorized exemplar of Katz's voice—an asset it did not have before. However, we all know that it was not the

62. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."); United States v. Williams, 592 F.3d 511, 519–20 (4th Cir. 2010) (applying the principle to computer searches); United States v. Stabile, 633 F.3d 219, 234 (3d Cir. 2011) (same).

63. Katz v. United States, 389 U.S. 347, 353 (1967).

64. *See id*.

65. *Id*. at 354.

66. Kerr 2010, *supra* note 2, at 708.

sound of Katz's voice, but the content of his words that mattered. That was a privacy concern, not a property concern.

Similarly, under both tests, the making of a consensual recording of a conversation is not a seizure. To Professor Kerr, the recording is an aid to memory.[67] Under the proposed test, the government was entitled to perceive and did perceive the conversation as it was happening.

The proposed test has a parallel to the test in *United States v. Jones,* where the Court held that there was a search when the government "physically occupied private property for the purpose of obtaining information."[68] Here, under the proposed test, we can say that there is a seizure when the government makes a copy for the purpose of obtaining information. If it already has the information, the copying is not a seizure because the government has already obtained the information. If the purpose of the copying is not to obtain information for human perception, as is true for the government router on the Internet, it is not a seizure. This is a consequence of focusing on the privacy interest that this author suggests is at the heart of the digital copying problem.

This focus on human acquisition to learn something new has a statutory parallel in the Wiretap Act. Section 2510(4) defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication."[69] The Wiretap Act has a venue provision that only allows a judge to approve an interception "within the territorial jurisdiction of the court in which the judge is sitting."[70] The cases conclude that, even if the connection to the telephone line occurs in one jurisdiction, the relevant jurisdiction for determining the location of the interception is the listening post, the place at which humans perceive the content of the communication.[71] From a physical perspective, the communication was "seized" at the point of insertion of the wiretap into the stream of communication. However, the law is concerned with the acquisition of the content by humans. The location of human perception determines where the seizure took place.[72]

Applying Wiretap Act ideas here means that we do not care about the Internet router, not because it does not change the path of the packets of data, but because no human looks at it. Similarly, we are not upset about the police photographing or writing down the things that they see, because they have already seen them.

67. *Id.* at 715.

68. United States v. Jones, 565 U.S. 400, 404 (2012).

69. 18 U.S.C. § 2510(4).

70. *Id*. § 2518(3).

71. *See e.g.*, Dahda v. United States, 138 S. Ct. 1491, 1495 (2018); United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992); United States v. Denman, 100 F.3d 399, 402–03 (5th Cir. 1996); United States v. Jackson, 207 F.3d 910, 914 (7th Cir. 2000).

72. *See id.*

III. PRESERVATION UNDER THE STORED COMMUNICATIONS ACT

The Stored Communications Act ("SCA")[73] regulates government access to data that customers store with cloud providers. Google, Microsoft, Yahoo!, Apple, Twitter, Facebook, and Dropbox are examples of such providers. The SCA and recent court decisions require the government to obtain a search warrant whenever it wants to obtain user content in an account.[74] Because so many criminal cases today involve electronic evidence, good investigators think about cloud accounts, such as e-mail and social media, at the start of any investigation. However, at the start of an investigation, law enforcement officers usually do not have probable cause to obtain a search warrant for an account. Cloud accounts and their contents are readily deleted. The SCA provides a solution that prevents destruction of the contents of the account for a limited time, while simultaneously preserving the privacy of the contents.[75]

Section 2703(f) provides that upon receiving governmental entity requests, a provider must "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."[76] In short, the provider must make a copy of the contents of the account.[77] The law requires the provider to keep this copy for ninety days and allows the government a single ninety-day extension.[78] Thus, the law gives the government six months to acquire sufficient evidence for a search warrant.[79] During that time, the provider holds the copy and is not allowed to give it to the government without a search warrant.[80] This action has no impact on the customer's ability to use the account or to have access to the data it contains. However, preservation does thwart a customer's efforts to delete contents, which might be evidence of the crime under investigation. While the customer can make deletions, the preserved copy is the record of the account as of the date of preservation.[81] If the government returns with a search warrant within 180 days, the provider will have the preserved copy to disclose.

Consider an all too real-world example of this preservation power and the need for it. During the insurrectionist attack on Congress on January 6, 2021, many of those who invaded the Capitol carried their cell phones and took

73. The Stored Communications Act is found at 18 U.S.C. § 2701 *et seq.* The portion that regulates how the government can obtain data from providers is found at Section 2703.

74. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting).

75. 18 U.S.C. § 2703(f).

76. *Id*. § 2703(f)(1).

77. *Id*.

78. *Id*.

79. *Id*.

80. 18 U.S.C. §§ 2702(a), (b)(2).

81. *See* Part V *infra* for the issues that this may raise.

photographs and videos.[82] Many participants posted these to online sites, and the work began immediately to identify the perpetrators.

As someone who conducted investigations in which cloud data was evidence, this author suggests the logical steps any investigator would take. After seeing a social media post containing of one of these videos or photographs, investigators would send a preservation letter to the specific social media provider to preserve the posting account. That would have happened hundreds of times in the days following the assault. Investigators would then work to develop probable cause to search the contents of that account. If a provider offered electronic communication services (e.g., Facebook messenger), an investigator would try to find facts to support a warrant to gain access to communications that related to any planning for the attack, as well as any communications during or after. The investigator would also look for evidence of other accounts belonging to this person to develop a full picture of their role and plans.[83] Communications with others about the assault would provide leads to follow up, likely resulting in preservation letters for the accounts of those persons and efforts to search them as well. However, in this author's experience, it takes weeks to get a response to a search warrant.[84] Thus, preservation for an extended period is essential.

IV. IS PRESERVATION UNDER THE STORED COMMUNICATIONS ACT A SEIZURE?

In the 2010 article, Professor Kerr suggested that the use of preservation letters under § 2703(f) is a seizure.[85] He has now expanded on it in his new article, devoted exclusively to this topic.[86] He suggests that when the government makes the request of the provider, the copying is government action, and that it is a seizure.[87] Applying his 2010 idea of seizure (copying as freezing) to the traditional rules about when a private search constitutes government

82. Kat Lonsdor et al., *A Timeline of How the Jan. 6 Attack Unfolded—Including Who Said What and When*, NPR (Jan. 5, 2022), https://www.npr.org/2022/01/05/1069977469/a-timeline-of-how-the-jan-6-attack-unfolded-including-who-said-what-and-when [https://perma.cc/8Y2R-54TM].

83. The author has not discussed these cases with any prosecutor involved, but an examination of those charged confirms that social media provided very useful evidence for the government's case. *See* U.S. DEP'T JUST., U.S. ATT'YS OFF. D.C., CAPITOL BREACH CASES, https://www.justice.gov/usao-dc/capitol-breach-cases (last visited Apr. 4, 2022). As examples, the case against Jared Hunter Adams relied upon data from Instagram and Google, No. 1:21-CR-212; the case against Alvear Gonzalez used data from Snapchat, No. 1:21-CR-115; the case against Gina Bisignano used data from Twitter, No. 1:21-CR-36; and the case against James Bonet used data from Facebook, No. 1:21-CR-121.

84. Google often took two months or longer to provide a response to a search warrant.

85. Kerr 2010, *supra* note 2, at 723–24.

86. Kerr 2021, *supra* note 1.

87. *Id*. at 702.

action, he concludes that the copying is a seizure.[88] He then concludes that to allow a brief seizure (a few hours) the government needs reasonable suspicion, citing physical world cases involving the detention of objects.[89] When the government has probable cause, he would permit warrantless copying for twenty to thirty days. Again, he cites physical world seizure cases for this point.[90]

Professor Kerr first proposed this argument in 2010. He has spoken to organizations of criminal defense attorneys suggesting that they raise this question,[91] and he has posted a short summary of this argument on the Volokh Conspiracy.[92] Yet, there are almost no cases on the subject.[93] Defense attorneys have not taken up his challenge. Prosecutors and providers continue to use the preservation process. That suggests that most people believe that when the provider makes a copy, but the government cannot see it until it provides a search warrant, there is no seizure. According to Professor Kerr, however, this is a seizure because an agent of the government (the Internet Service Provider ("ISP") acting on a government request) has made a copy, and the government has not seen it before.[94] This author suggests that the preservation letter is like the *Gorshkov* case, only on the other side of the looking glass. We do not feel this is a seizure because the subscriber has not lost access to anything, but unlike in *Gorshkov*, the government has not gotten access to anything. Calling this a seizure seems just as odd as saying that what happened in *Gorshkov* was not a seizure.

A. Even Under a Traditional Definition of Seizure, Preservation Under § 2703(f) is not a Seizure

In his new article, Professor Kerr takes his new concept of seizure—copying to freeze data—and applies standard physical world law to it.[95] Because the ISP acts at the request of the government, and because the statute requires the ISP to preserve a copy, this would be considered government action.[96] Thus, he determines it is a seizure. In the physical world, a warrantless seizure can only last for a brief time. No cases permit a warrantless seizure of a physical object for 180 days, so Professor Kerr argues that the preservation process violates the

88. *Id*. at 711.

89. *Id*. at 754–55.

90. *Id.* at 755–57.

91. Kerr 2021, *supra* note 1, at 705.

92. *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/437G-B82T].

93. Kerr 2021, *supra* note 1, at 758.

94. *Id.* at 783.

95. *Id.* at 757.

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

Fourth Amendment.[97] The new article does not make it clear why we should be open to a new concept of seizure for digital evidence (one that defines seizure as copying for freezing, but not copying for memory), but at the same time, not re-examine the collateral issues, such as the time limits for warrantless copying of items, that should go with such a rethinking.

This Section first suggests that even using physical world thinking, the preservation is not a seizure even though the acts of the ISP are done at the government's request. Further, even using the physical world thinking, the time periods offered by Professor Kerr do not make sense. Finally, in examining the preservation letter under the light of the privacy analysis, this author concludes there is no seizure.

1. Caselaw Suggests That Preservation is Not a Seizure Under Physical World Standards

Before turning to the new proposed approach, the author believes that Professor Kerr is wrong in his assertion that preservation is a seizure, even under physical world standards. Kerr cites two cases, *United States v. Place*[98] and *United States v. LaFrance*,[99] for the proposition that seizures based upon reasonable suspicion must be quite brief. In *Place*, agents stopped Place as he landed at LaGuardia airport.[100] When he would not consent to the search of his luggage, they detained it and took it to Kennedy Airport where it was subject to a dog sniff.[101] It took ninety minutes from the seizure until the dog alerted to the luggage. Because it was Friday afternoon, the agents held the luggage and obtained a search warrant on the following Monday. The Court held that ninety minutes was too long of a seizure.[102] What influenced the Court was not just that the seizure deprived Place of his possessory interest in his bags, but also holding his baggage effectively detained him.[103] With the preservation of an account, the account holder neither loses access to the data nor their freedom of movement.

LaFrance makes an even stronger case for preservation not being a seizure. *LaFrance* involved the shipment of drugs by FedEx.[104] The FedEx contract obligated it to deliver the package to the recipient by noon on the day of seizure.[105] At 9:03 AM, the police asked FedEx to hold the package; somewhere

97. Kerr 2021, *supra* note 1, at 754–55.

98. 462 U.S. 696, 715 (1983).

99. 879 F.2d 1, 10 (1st Cir. 1989).

100. *Place*, 462 U.S. at 698.

101. *Id*. at 699.

102. *Id.* at 709–10.

103. United States v. Place, 462 U.S. 696, 708–09 (1983) ("Nevertheless, such a seizure can effectively restrain the person since he is subjected to the possible disruption of his travel plans in order to remain with his luggage or to arrange for its return.").

104. United States v. LaFrance, 879 F.2d 1, 2 (1st Cir. 1989).

105. *Id*. at 3.

around 9:20 AM, the police requested that FedEx deliver the package to the police station.[106] It arrived at 12:45 PM; the dog sniff test began at 1:15 PM and ended by 2:15 PM.[107] The court measured the time of detention from noon, when the package should have been delivered.[108] In other words, there was no interference with the defendant's possessory interest in the package until he was contractually due to receive it. The time of deprivation was measured from that point, even though the police had exercised dominion and control over the package earlier. If this scenario had taken place with an ISP account, the owner would have access to the account before 9:03 AM, after 9:03 AM, and so on until such time as the account holder or the provider decided to shut the account down. With preservation, the ISP meets its contractual obligation to deliver the data whenever and wherever the user wants it. It is difficult to see how this is a meaningful interference with the possessory interest in the property.

Changing the facts of *LaFrance* only slightly makes the result even more clear. If the police had called FedEx and asked them to hold a package, then they went to FedEx the same day, wrote down information from the package label, and told FedEx to continue with the delivery of the package, whether there has been a seizure depends on whether the delivery of the package was delayed. If the actions of the agents did not slow the delivery (e.g., it was put on the same outgoing truck it had been scheduled to be put on and FedEx had delivered the package at noon), the actions would not be a seizure under the Fourth Amendment.

In *United States v. Va Lerie*,[109] the police pulled the luggage from the luggage compartment of a Greyhound bus on which Va Lerie was a passenger. In rejecting his claim that removing the luggage from the bus constituted a seizure, the court gave as one of its reasons the fact that there was no basis to believe that the luggage would not have been put back on the bus in time for its departure.[110] The court dealt with the three major concerns of seizure, writing,

> [R]eversing the district court's seizure decision, we hold such conduct did not constitute a seizure, because the removal of the luggage did not (1) delay Va Lerie's travel or significantly impact Va Lerie's freedom of movement, (2) delay the timely delivery of the checked luggage, or (3) deprive Greyhound of its custody of the checked luggage.[111]

On the second point—delaying delivery—the court noted that Va Lerie consented to the search of the luggage after it had been removed from the bus.[112]

106. *Id*.

107. *Id.* at 3.

108. *Id.* at 7.

109. United States v. Va Lerie, 424 F.3d 694, 696 (8th Cir. 2005) (en banc) (the defendant's luggage was taken off of a Greyhound bus on which he was traveling).

110. *See id.* at 707.

111. *Id.* at 696.

112. *Id.* at 709–10.

In rejecting the idea that the police action was a seizure before his consent, the court wrote, "the NSP's removal of Va Lerie's checked luggage from the bus did not affect the timely delivery of the luggage. No evidence suggests the luggage would not have been placed back on the bus for transport to its destination had it not been for the discovery of illegal drugs."[113]

When the ISP makes a copy after receiving a preservation letter, following the paradigm of *Place*, *LaFrance*, and *Va Lerie*, nothing interferes with the subscriber's personal freedom, there is not even a second's delay in the user's access to her data, and the data never leaves the custody of the ISP. If this would not be a seizure in the physical world, it is difficult to find a rationale that makes it a seizure in the digital world. Moreover, in the physical world examples, the government agents had their hands on the luggage and packages. With a preservation letter, the government does not obtain a copy of the data and cannot see the data until it produces the necessary legal process, usually a search warrant. The ISP is forbidden to turn it over without such process.[114]

Owner access to the data was also one of the facts that influenced the court in *United States v. Laist*.[115] Laist allowed FBI agents to take his computers and drives and consented to a search.[116] Before the agents took away the devices, Laist asked if he could copy the files he needed for school.[117] The agents allowed him to "download whatever he wanted to download," and Laist "did take off what he thought he needed at that time."[118] A few days later, Laist revoked his consent, but the FBI waited twenty-five days before preparing a search warrant.[119] The issue was whether the delay in obtaining the warrant violated the Fourth Amendment.[120] In deciding not to suppress the evidence, the court gave weight to the fact that Laist had been permitted to copy whatever "he thought he needed at the time."[121] The fact that Laist had the data he wanted, even though he no longer had possession of his device, was an important fact for the court.[122]

In *Laist*, what happened was clearly a seizure—the defendant did not have the use of his computers at all. But access to the data was an important factor in the decision on the question of delay in obtaining the warrant.[123] Consider, however, that although he was allowed to copy whatever he thought he needed,

113. *Id.* at 708.
114. 18 U.S.C. §§ 2702, 2703(a).
115. 702 F.3d 608, 616 (11th Cir. 2012).
116. *Id.* at 610–11.
117. *Id*. at 611.
118. *Id.*
119. *Id.* at 611–12.
120. United States v. Laist, 702 F.3d 608, 612 (11th Cir. 2012).
121. *Id.* at 611.
122. *Id.* at 616.
123. *Id*.

his choice of what to copy was obviously made under stress. It is not unusual to think of something one wants that is stored on a computer and to search for it. This could be the contact information for an old friend, an e-mail one received three years ago, a document one wrote, or a purchase one made. Which of us could remember those things when being rushed to copy whatever we needed? Nevertheless, the court held that having access to what he designated at the time of the seizure mitigated its impact. Contrast that with the preservation letter. The customer does not have to make a snap decision—or any decision. All data remains available during the entire preservation period. Looking for the place you bought those comfortable shoes four years ago? If it is in your cloud account, even if it has been preserved at the request of the government, you can find it. All of this suggests that preservation is not a seizure.[124]

2. Kerr's Application of Physical World Time Limits is not Justified

As noted above, Professor Kerr adopts physical world time limits to preservation letters, allowing for a few hours' detention when based upon reasonable suspicion and for longer periods (using cases, such as *Laist*, in which the government delayed applying for a search warrant as the standard) when based upon probable cause.[125]

Consider the impossibility of meeting these time deadlines in the Capitol assault cases discussed above. Even a single person incident would result in a search for multiple online sources, and it may take the review of the contents of one (provided only weeks after the execution of a search warrant) to get probable cause to search another. Although inconvenience to the government is not a basis for disregarding the Fourth Amendment, when one contemplates what seizures are "reasonable," practical considerations play an important role.

When turning to the reasons justifying time limits on warrantless seizures of physical objects, it is clear that none of the concerns creating those limitations are involved with digital copying. All of the cases express a concern that a physical world detention deprives the user of the use of the object. When the object is a digital device, detention deprives them of access to the data. In luggage cases, such as *Place*, the seizure also limits the owner's freedom of

124. As this Article was about to be sent to the printer, the Ninth Circuit rejected the argument that a preservation letter is a seizure. The court focused upon the two factors emphasized in this Article, writing: "Here, the preservation requests themselves, which applied only retrospectively, did not meaningfully interfere with Rosenow's possessory interests in his digital data because they did not prevent Rosenow from accessing his account. Nor did they provide the government with access to any of Rosenow's digital information without further legal process." United States v. Rosenow, No. 20-50052, 2022 WL 1233236, at *12 (9th Cir. Apr. 27, 2022) (noting additionally that by agreeing to the terms of service, Rosenow consented to the provider honoring preservation requests).

125. *Id.* at 799–800, 804–05.

movement.[126] If we are going to rethink the doctrine of seizure and apply it to copying as Professor Kerr does, we must also examine the reasons for the time limits for warrantless detention.[127] Losing access to a physical object, and in some cases to the data it contains, has a significant impact on the owner. Thus, courts have allowed only short periods of warrantless detention.

Even assuming that the preservation of data is a seizure, there is no reason to port in the time limits of the physical world. The preservation letter has none of the impacts on the owner that the physical world seizures do. The question then is whether a 180-day preservation is unreasonable. As discussed above, the preservation has no impact on the user's access to the data and does not give the government access to it either. The status quo is preserved for all parties. Under such circumstances, the idea of what is reasonable needs reexamination. Investigations take time. A diligent investigator will pursue many leads: interviewing witnesses, subpoenaing records, etc. Some businesses are quick to respond to subpoenas; others—banks, and Google, in this author's experience—are much slower. The congressional decision to allow a maximum of six months for the government to gather enough facts to justify a search warrant is a reasonable solution, particularly when the impact on the user is negligible.

B. Applying a Privacy Analysis, a Preservation Letter is not a Seizure

Turning to the privacy interest, which is the real concern, the copying has no impact on the user's privacy interest. Although the ISP makes a copy of the data, the ISP already has the data. The user has entrusted the ISP to hold the data, and the ISP has access to the content.[128] Making an extra copy has no impact on the user's privacy interest. No one has been added to the list of those who can see the data. Preservation has no impact on the real concern with data copying—privacy. The lack of any impact on privacy suggests that preservation

126. United States v. Place, 462 U.S. 696, 708–09 (1983).

127. Kerr 2021, *supra* note 1, at 757.

128. For example, Google's terms of service make clear that they can look at a user's content. *See Terms of Service*, GOOGLE (Jan. 5, 2022), https://policies.google.com/terms?hl=en-US [https://perma.cc/K6EP-WTKA] (after making clear that a user keeps any intellectual property rights in data stored with Google, the terms of service say, "This license doesn't affect your privacy rights—it's only about your intellectual property rights[.]"). Facebook's terms of service are similar. See Terms of Service, FACEBOOK (Jan. 4, 2022), https://www.facebook.com/terms.php [https://perma.cc/S2PV-CWLC] ("Specifically, when you share, post, or upload content that is covered by intellectual property rights on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings)."). Dropbox encrypts stored data, but it controls the encryption keys. *See How Dropbox Keeps Your Files Secure*, DROPBOX, https://help.dropbox.com/accounts-billing/security/how-security-works (last visited on Mar. 31, 2022).

is not a seizure. The fact that the copy was made at the request of the government does not change anything. The provider always makes backup copies of its data, which will include the customer's account. Moreover, unlike the case in which a government agent copies a hard drive, the government has no access to the copy. There is no impairment of the privacy interest until the government produces a warrant. Without a warrant, this tree falling in the forest makes no sound.[129]

V. THE PROBLEM OF DELETED DATA

The only problem that remains is the impact of preservation of data, which the customer deletes after the preservation but before the execution of the search warrant. As noted in Part III, the preservation process of § 2703(f) is designed to thwart evidence destruction.[130] Consider a case in which the government sends a preservation letter to Dropbox on day one. On day thirty, the user deletes a document. On day 170, the government serves a search warrant for the account on Dropbox. If Dropbox produces the copy it made on day one, it will produce the deleted file. Dropbox will produce the document that the user deleted because it has made the preservation copy. If there had been no preservation, the Dropbox would not be able produce it.

Professor Kerr recognizes that this is the only scenario in which suppression would be a possible remedy, for he notes that the inevitable discovery doctrine would protect any items that were not deleted from suppression.[131]

This Part examines the questions raised by an ISP's production of an item that would not have been present on the day of execution of the warrant were it not for the preservation, by first looking at the problem using Professor Kerr's physical world seizure analysis—that copying is a seizure, and then assessing the problem from the privacy perspective. For many providers, this will not be an issue. Gmail, for example, often archives deleted e-mails, depending on the user's settings. After choosing to delete a message, one must then affirmatively act to delete the message from the archive and even then, Gmail will hold it for

129. The warrant requirement to get access to preserved data distinguishes such data from the copying in *Gorshkov*, where the government had immediate access to the data. Although it chose not to search the data until it obtained a warrant, there was always a risk that some government agent would look at it. There is no such risk with data copied pursuant to a preservation letter. *See* United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001).

130. *See supra* Part III.

131. Kerr 2021, *supra* note 1, at 807: "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, 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 by using only the warrant copy.'"

thirty days, in case the user reconsiders.[132] Otherwise, e-mail remains in the archive forever. Dropbox will hold a deleted file for thirty days in case the customer reconsiders.[133]

A. Employing the Physical World Seizure Analysis

Professor Kerr's reliance upon physical world seizure analysis prompts an examination of the attempted deletion under that paradigm. The act of deletion changes the subscriber's legal interest in the data deleted. Until that moment, the customer owned the data, and the ISP held it as a bailee; the government could not search it without a warrant.[134] But at the moment of deletion, the customer now abandons the property and gives it to the ISP to get rid of. In a physical world scenario, consider a murderer who wants to get rid of the murder weapon, so he gives it to a friend to throw into the river. To make this more analogous to the ISP situation, imagine that the defendant was hiding, so the police went to all his friends and relatives and specifically requested that if the defendant sent anything to them, they should call the police and turn it over. Weeks later, the police return to the friend, who reveals that the defendant sent him a package and asked him to destroy the contents. By delivering the package to someone else to destroy it, the defendant has abandoned it and given any Fourth Amendment rights solely to the recipient.

Deleting a file held by an ISP is the digital equivalent of throwing a physical object away.[135] In the physical world, that constitutes abandonment.[136] Merely putting a physical item in the trash is not only expressing a lack of privacy expectation in it, but also abandoning the property.[137] The test for abandonment

132. *See Control Email and Chat Message Storage*, GOOGLE, https://support.google.com/a/answer/151128?hl=en&ref_topic=9973341 [https://perma.cc/U9NL-FHUB] (last visited Jan. 23, 2022).

133. *See Deleted File Recovery and Version History,* DROPBOX, https://www.dropbox.com/features/cloud-storage/file-recovery-and-history [https://perma.cc/T5YC-77HN] (last visited Dec. 27, 2020).

134. *Ex Parte* Jackson, 96 U.S. 727, 735 (1877) (mail); United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010) (e-mail).

135. Because the ISP holds the file, there is a relinquishment of ownership. This is different from the case of a person who possesses the data on her own computer and deletes the file. In that situation, the person retains custody of the medium that holds the now-deleted file and has not abandoned the property. United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999).

136. California v. Hodari D., 499 U.S. 621, 629 (1991).

137. California v. Greenwood, 486 U.S. 35, 39–40 (1988); United States v. Redmon, 138 F.3d 1109, 1114 (7th Cir. 1998); United States v. Scott, 975 F.2d 927, 929 (1st Cir. 1992) (throwing away is abandonment; shredding document before throwing it away does not restore the expectation of privacy); United States v. Reicherter, 647 F.2d 397, 399 (3d Cir. 1981) (decided before *Greenwood*). *Scott* shows the distinction between the possessory and privacy interests. Throwing away the document abandons the possessory interest. Shredding was a subjective expression of the privacy interest, but one which is not reasonable. Professor Kerr cited *Scott* for the proposition that shredding does not create an expectation of privacy in his article arguing that encryption does not

in the physical world is expressed in various ways all looking to whether the person voluntarily discarded the property or relinquished his interest in it.[138] A person who deletes a file in cloud storage or in an e-mail account is clearly voluntarily discarding it. The fact that the ISP holds onto it is the same risk run by the murderer who gives the weapon to a friend to destroy. The main difference, however, is that with the murder weapon, the police can just ask the friend for it. With the deleted file, law enforcement must produce a search warrant to get it.[139] The warrant requirement is not a constitutional requirement with abandonment, but it is a statutory requirement in the case of digital evidence in cloud storage.

B. The Privacy Analysis

When a person opts to store a file online, as opposed to on a home computer, they make a choice to surrender a part of their privacy in the file. They make the same choice when choosing to send an e-mail or online message, rather than a letter.[140] In both cases, the file or message is entrusted to a bailee. Nothing about this surrender of privacy changes when they instruct the provider to delete the file. The person's privacy interest in the file remains the same. As noted above,[141] making a preservation copy does not change that. The act of entrusting reflects the choice that the provider will keep a copy. The preservation copy does not have any impact on that because no one can see the preservation copy that could not see the data before. The loss of privacy remains constant. The risk that the provider might keep a copy indefinitely was accepted by the user at the time they uploaded the file or sent the message. The person does not lose any constitutional right of privacy until the government obtains access. That is possible only when the government obtains a search warrant.[142]

create an expectation of privacy. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create A "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 513 (2001).

138. *See e.g.*, Bond v. United States, 77 F.3d 1009, 1013 (7th Cir. 1996); United States v. Lehder-Rivas, 955 F.2d 1510, 1522 (11th Cir. 1992); United States v. McKennon, 814 F.2d 1539, 1546 (11th Cir. 1987) (the critical inquiry is "whether the person prejudiced by the search . . . voluntarily discarded, left behind, or otherwise relinquished his interest in the property in question so that he could no longer retain a reasonable expectation of privacy with regard to it at the time of the search."); United States v. Hershenow, 680 F.2d 847, 855 (1st Cir. 1982).

139. 18 U.S.C. § 2703(a).

140. The choice made by sending a letter or an e-mail involves surrendering the privacy interest in those documents to the recipient as well.

141. *See supra* Part V.A.

142. As noted *supra* note 129, the warrant requirement makes the preservation letter situation different from what occurred in *Gorshkov*.

C. There is No "Right to Delete"

Professor Kerr's concerns are based upon a "right to delete,"[143] for he concludes that only items produced by an ISP that the user sought to delete after the preservation letter should be suppressed.[144] There are those who assert, forthrightly, that there is a right to delete and that copying interferes with that right.[145] This idea seems unique to digital information. No one has the right to destroy physical evidence, and no one suggests that anyone should have such a right. We have obstruction crimes to deal with destruction of physical evidence. There are many statutes that require businesses to keep records for inspection.[146] Such laws go beyond prohibiting destruction and require the creation of evidence. If there is to be such a right to delete for digital evidence, there needs to be something special about digital evidence that distinguishes it from physical evidence. However most digital evidence consists of things such as documents, photographs, videos, etc. All of these have physical world counterparts, and the obstruction statutes bar the destruction of this kind of physical evidence. There is no rational basis to distinguish the destruction of the digital counterparts of these physical objects.

In the physical world, the Supreme Court has explicitly rejected such a right. In *Segura v. United States*, the Court wrote, "the essence of the dissent is that there is some 'constitutional right' to destroy evidence. This concept defies both logic and common sense."[147] Preservation of evidence is one of the three reasons justifying the government's right to make a search incident to arrest.[148] It is also the rationale permitting temporary seizures under exigent circumstances.[149]

Moreover, while the criminal obstruction statutes are not constitutional in nature,[150] they do reflect a judgment about what society recognizes as

143. Kerr 2021, *supra* note 1, at 765 ("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."). *See also id.* at 34 ("Preservation eliminates that control. A person who wants to delete a private message will *think* he can delete it. A person who wants to delete his entire account will *think* it is gone. But when contents are preserved, users can't do that.").

144. *Id*. at 58.

145. See generally Paul Ohm, The Fourth Amendment Right to Delete, 119 HARV. L. REV. F. 10 (2005).

146. For example, insured banks are required to keep such records as the Secretary of the Treasury, or the Federal Reserve Board may require. 12 U.S.C. § 1829b.

147. Segura v. United States, 468 U.S. 796, 816 (1984).

148. Arizona v. Gant, 556 U.S. 332, 351 (2009); Chimel v. California, 395 U.S. 752, 763 (1969).

149. *See generally* Segura v. United States, 468 U.S. 796 (1984).

150. There are several federal statutes that specifically prohibit the altering or destruction of documents. *See e.g.*, 18 U.S.C. § 1505 (concealing or destroying documentary material in an antitrust civil investigative demand). *Id*. § 1519 (destroying or concealing records or documents to

reasonable. For example, Section 1519 of Title 18, U.S. Code, makes destruction or alteration of records a crime, if it is done to "influence" a federal investigation, even if no such investigation is occurring.[151] The crime is destruction in contemplation that such an investigation might come into being. The statute of limitations for obstruction offenses is five years,[152] suggesting that the government's right to obtain evidence is superior to any right to delete for at least five years. The statute reflects a societal judgment that we do not want people deleting files that might turn out to be useful in a criminal prosecution.[153] The five-year statute of limitations for obstruction crimes also suggests that the 180-day preservation period is reasonable. If there is a right to delete, then the obstruction statutes would be unconstitutional.

Once again, the assault on the Capitol on January 6, 2021, provides a good example of why we do not want people deleting evidence. Many of the people who entered the Capitol building made videos and photographs of their actions. They posted them to social media sites. If there were a right to delete, it would permit these people to destroy all that evidence to avoid the consequences of their actions. There should be little doubt that after some of those who entered the Capitol learned that others were being arrested based upon their social media postings, they would have tried to delete the images that they had posted. Only preservation letters will impede their success.

However, one could ask the following question applying the preservation letter concept to the physical world: "Could the government issue a preservation letter to an individual to preserve physical evidence?" Although this scenario is unlikely, it is worth noting that the obstruction statutes do just that. A physical world preservation letter would be an improvement over these obstruction statutes for it would provide better notice to a person of the danger of destruction. The general rule is that "ignorance of the law is no excuse."[154] A person does not have to know that it is a crime to destroy evidence to be found guilty.[155] A preservation letter would have the value of informing the person of this danger.

impede, obstruct, or influence and investigation within the jurisdiction of any department of the United States or under Title 11 [Bankruptcy], "or in contemplation of any such matter or case.").

151. 18 U.S.C. § 1519

152. *Id*. § 3282.

153. Although there is no right to delete as such, the government's interest clearly expires after the statute of limitations for any underlying crime is gone. After the statute of limitations has run, the government has no legitimate interest in retention of the data.

154. Bryan v. United States, 524 U.S. 184, 196 (1998).

155. United States v. McCoy, 2016 WL 1248743, at *8 (E.D. Ky. Mar. 29, 2016) (applying principle to 18 U.S.C. § 1519).

It is true that the coverage of a preservation letter is broader than that of an obstruction statute or even a litigation hold order.[156] Those types of preservation are limited to matters relevant to some investigation or litigation. A statutory preservation letter to an ISP applies to everything held by the ISP in the account. There are good reasons, however, for allowing a different scope for preservation letters. First, a preservation letter to the ISP is not a general restriction on the subscriber from destroying anything in the world, regardless of relevance. It is a limited order to the ISP that only applies to the files that the subscriber has entrusted to the ISP. Thus, it is much more narrowly focused. Second, while a preservation letter to a person or even a litigation hold order permits that person to make judgments about what matters are relevant to the litigation or investigation, an ISP is not in a position to do that. It has little or no idea about the nature of the investigation, and it has no people trained to conduct searches to find evidence that would be relevant to the investigation it does not know about. ISPs do not want to participate in the search process. Thus, for example, Google has objected to a search warrant that required it to look through an e-mail account for child exploitation material because it was "not competent to perform such an analysis and requiring it to do so [was] unfair and unduly burdensome."[157] Finally, the order presents a minimal burden on the ISP, which is in the business of keeping data. Under such circumstances an order that preserves only those things in the ISP account, and not everything a person owns (as a preservation letter to a person or a litigation hold order would do), for a short time, is a reasonable solution. It only preserves things that the ISP holds and recognizes the inability of the ISP to make the necessary judgments about what matters would be relevant.

CONCLUSION

Digital is different. Although to some this is just a slogan, it is a good reminder that the move from the physical world to the digital requires rethinking of some of our legal principles. Some rules of the physical world do not translate well in the digital environment. Thus, the physical world law of search incident to arrest had to change to recognize that the search of a package of cigarettes is different from the search of a cell phone.[158] On the other hand, there was no need for new law to decide what is a threat, when it is posted on Facebook, rather than in a letter or made orally.[159] Professor Kerr has been a leader in re-examining the law of search and seizure when applied to the digital world. His 2010 article

156. *See, e.g.*, FED. R. CIV. P. 26(f) (a litigation hold order arises out of the discovery obligations imposed on civil litigants); Shelley v. Kramer, 334 U.S. 1, 16 (1948) (court orders can be state action).

157. *In re* Search of Google Email Accounts, 99 F. Supp. 3d 992, 995 (D. Alaska 2015).

158. Riley v. California, 573 U.S. 373, 375 (2014).

159. Elonis v. United States, 575 U.S. 723, 745 (2015).

was an effort to bring the physical world definition of seizure into the digital world. His position has the common law virtue of keeping what we have and trying to interpret and modify it in light of new facts. However, to do so he had to create two "fudge factors"—ad hoc rules to render certain acts of copying not seizures. It was not that taking photos of a search scene or the use of government routers on the Internet did not fit the definition of seizure; it was that calling them seizures felt ludicrous. Creating ad hoc exceptions does not make for a consistent body of law.

We need to rethink what a seizure in the digital world is by examining the true concerns about digital copying. What concerns us is not the possessory interest in the data, but the privacy interest. Granted, this is a radical shift in the concept of seizure. It unmoors the definition from the physical world. However, that is a consequence of the non-rivalrous nature of data. This author suggests that we will do better in dealing with the problem of digital seizures if we recognize that we are concerned about privacy and create a body of law considering that. In the problem at hand, preservation letters, a focus on privacy addresses the true concerns. That focus also explains that, although a writer as influential as Professor Kerr has advanced the idea that preservation letters are seizures for more than a decade, few defense lawyers have challenged them, prosecutors continue to use them, and ISPs continue to honor them. The fact that the user loses neither access to their data, nor their privacy interest in the data, shows that there are no true Fourth Amendment implications in this procedure. When copying immediately invades privacy, we should consider that to be a seizure. However, when copying does not invade privacy, we ought not call it a seizure.