Michigan Law Review

Volume 117 | Issue 7

2019

Carpenter's Legacy: Limiting the Scope of the Electronic Private Search Doctrine

Sarah A. Mezera
University of Michigan Law School

NOTE

CARPENTER'S LEGACY: LIMITING THE SCOPE OF THE ELECTRONIC PRIVATE SEARCH DOCTRINE

*Sarah A. Mezera**

One of the most significant challenges confronting courts and legal scholars in the twenty-first century is the application of Fourth Amendment doctrine to new technology. The circuit split over the application of the private search doctrine to electronic devices exemplifies how courts struggle to apply old doctrines to new circumstances. Some courts take the position that the old doctrine should apply consistently in the new context. Other courts have changed the scope of the old doctrine in order to account for the change in circumstances. The Supreme Court took the latter position in Carpenter v. United States *and held that the third-party doctrine does not apply to cell-site location information records. The Court's willingness to limit the scope of an established doctrine to preserve fundamental privacy interests suggests that* Carpenter *is just the beginning of a dramatic shift in Fourth Amendment law. This Note argues that the circuit split over the private search doctrine should be resolved by creating a narrow electronic private search doctrine based on the logic of* Carpenter.

TABLE OF CONTENTS

* J.D. Candidate, May 2019, University of Michigan Law School. I would like to thank my parents for all their love and support throughout my law school career. I would also like to thank every member of the *Michigan Law Review* who worked on and significantly improved this Note. Many special thanks to the Volume 117 Notes Office, Michael Abrams, Aviv Halpern, Ryan Marosy, Jun Ha Park, and Carolina Velarde, for being excellent editors, wonderful colleagues, and truly amazing friends.

INTRODUCTION

Recent and rapid advances in technology challenge traditional legal doctrines. The Fourth Amendment is one particular area of law facing such challenges.[1] The animating principle behind the Fourth Amendment has not changed in light of the digital age—individual privacy interests are weighed against important government interests.[2] But the fundamental and pervasive changes that accompany technological advances potentially alter the way that balance is struck. As technology continues to evolve, courts and legal scholars face important questions of how to preserve, amend, or reject existing Fourth Amendment doctrine.

One of the most notable recent changes to Fourth Amendment doctrine occurred in *Carpenter v. United States*.[3] In *Carpenter*, the Supreme Court protected individual privacy interests by declining to extend the third-party doctrine to cell-site location information (CSLI).[4] The third-party doctrine has been a part of Fourth Amendment law since 1976,[5] and it has been extended numerous times by the Court.[6] Yet the Court in *Carpenter* found that CSLI is a qualitatively different category of information to which the third-party doctrine does not apply.[7] This limitation of the third-party doctrine raises an important question: Should the capability of technology to amass incredible amounts of information similarly limit the scope of other doctrines under the Fourth Amendment?

The private search doctrine is closely related to the third-party doctrine at issue in *Carpenter*[8] and is a microcosm of the challenges the Fourth Amendment faces in the twenty-first century. Under the Fourth Amendment, government agents are generally required to get a warrant based on probable cause to conduct a search of persons or property.[9] There are, how-

---

1. *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004).

2. *See* Riley v. California, 573 U.S. 373, 407 (2014) (Alito, J., concurring) ("Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form. This calls for a new balancing of law enforcement and privacy interests.").

3. 138 S. Ct. 2206 (2018).

4. *Carpenter*, 138 S. Ct. at 2217.

5. United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities . . . .").

6. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 744 (1979) (applying the third-party doctrine to a pen register).

7. *Carpenter*, 138 S. Ct. at 2218–19.

8. United States v. Jacobsen, 466 U.S. 109, 130 (1984) (White, J., concurring in part and concurring in the judgment).

9. Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." (footnotes omitted)).

ever, several exceptions to the warrant requirement, including the private search doctrine.[10] The private search doctrine can be traced to *Walter v. United States*, in which the Supreme Court hinted that police may be allowed to reexamine materials searched by a private person without first obtaining a warrant.[11] Later, in *United States v. Jacobsen*, the Court officially announced that the private search doctrine was a formal exception to the warrant requirement.[12]

Under the private search doctrine, the police may reconstruct a private search without obtaining a warrant in advance.[13] The Court reasoned that because the owner's expectation of privacy was already frustrated by a private search, the subsequent government search did not implicate the Fourth Amendment.[14] The government search must remain within the same scope as the original private search unless the officer is "virtually certain" they will find similar evidence beyond the scope of the private search.[15] In *Jacobsen*, the scope of the government search was limited to the physical container searched by private parties.[16] But with new technology, the permissible scope of an electronic government search under the private search doctrine has become a contested question among federal circuits.[17]

Federal courts disagreed on the doctrine's scope even before cases applied the private search doctrine to electronic devices.[18] The dispute over the scope of the doctrine intensified when searches became electronic in na-

---

10. *See, e.g.*, Kentucky v. King, 563 U.S. 452 (2011) (exigent circumstances); Illinois v. Rodriguez, 497 U.S. 177 (1990) (consent); Coolidge v. New Hampshire, 403 U.S. 443, 444 (1971) (plain view); Chimel v. California, 395 U.S. 752 (1969) (search incident to arrest); Terry v. Ohio, 392 U.S. 1 (1968) (stop and frisk).

11. 447 U.S. 649, 657 (1980).

12. 466 U.S. at 119.

13. *Jacobsen*, 466 U.S. at 119. The Court in *Jacobsen* distinguished a private search from a "search" under the Fourth Amendment. The Fourth Amendment only proscribes government action; therefore, a search conducted by a private individual not acting as a government agent does not implicate the Fourth Amendment. *Id.* at 113.

14. *Id.* at 120. *See generally Katz*, 389 U.S. at 361 (Harlan, J., concurring).

15. *See Jacobsen*, 466 U.S. at 119 ("[T]here was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he already had been told.").

16. *See id.* ("Respondents could have no privacy interest in the contents of the package, since it remained unsealed and since the Federal Express employees had just examined the package . . . .").

17. *See* Matthew A. Lupo, *Privacy in the Digital Age: Preserving the Fourth Amendment by Resolving the Circuit Split over the Private-Search Doctrine*, 10 ALB. GOV'T L. REV. 414, 415 (2017).

18. *Compare* United States v. Rouse, 148 F.3d 1040, 1041 (8th Cir. 1998) (holding that the government searchers exceeded the scope of a private search because they had no previous information about some of the items they searched), *with* United States v. Simpson, 904 F.2d 607, 610 (11th Cir. 1990) (stating that the government searchers did not exceed the scope of a private search "simply because they took more time and were more thorough than" the private searchers).

ture.[19] Computers, smartphones, and various other electronic devices are like digital containers that can store an immense amount of information.[20] The difference in nature between an electronic device, such as a computer, and a physical container, such as a cardboard shipping box, has renewed the debate over how courts should strike the balance between individual privacy interests and important government interests under the private search doctrine. If the *Jacobsen* container-based approach is to be preserved, the fundamental question is: What is the electronic equivalent of a physical container?

This Note argues that the scope of the private search doctrine as applied to electronics should be limited to only the exact data viewed by the private searcher. Part I discusses the current circuit split over how the private search doctrine applies to electronic devices and contrasts how different circuits have defined an electronic "container." Part II analyzes how *Carpenter*'s limitation on the third-party doctrine will affect the private search doctrine's scope. Part III argues that the Court should resolve the circuit split by adopting a narrow rule that defines an electronic "container" as only the exact data viewed by the private searcher and limits the scope of the government search to just the data exposed on a device's screen.

I. THE DIFFICULTY OF DEFINING AN ELECTRONIC "CONTAINER"

When the Supreme Court established the private search doctrine in 1984, it did not consider how the doctrine would apply to electronic devices.[21] This lack of foresight left lower courts to decide how to apply the doctrine to electronic devices as technology developed rapidly. The Fifth and Seventh Circuits have adopted a rule that allows the government to search the entire electronic device after a private search.[22] The Sixth and Eleventh Circuits have adopted a rule that allows the government to search only the data that a private searcher viewed.[23] This Part will discuss the two approaches to defining an electronic "container"—a bright-line rule and a more flexible standard.

The Fifth Circuit's opinion in *United States v. Runyan* outlines one side of the circuit split.[24] The Fifth Circuit was the first to apply the private search

19. *See* Alexandra Gioseffi, Comment, Lichtenberger, Sparks, *and* Wicks*: The Future of the Private Search Doctrine*, 66 EMORY L.J. 395, 399 (2017).

20. *See* Benjamin Holley, Note, *Digitizing the Fourth Amendment: Limiting the Private Search Exception in Computer Investigations*, 96 VA. L. REV. 677, 682 (2010).

21. *See Jacobsen*, 466 U.S. 109.

22. Brianna M. Espeland, *Implications of the Private Search Doctrine in a Digital Age: Advocating for Limitations on Warrantless Searches Through Adoption of the Virtual File Approach*, 53 IDAHO L. REV. 777, 781 (2017).

23. *Id.* at 782.

24. 275 F.3d 449 (5th Cir. 2001). The electronic devices at issue in *Runyan* were CDs and floppy disks. *Runyan*, 275 F.3d at 453.

doctrine to electronic devices, doing so in 2001.[25] The Fifth Circuit took the view that an electronic device (in this case, a CD or floppy disk) is a "container," similar to the physical shipping box at issue in *Jacobsen*.[26] The court treated each CD or floppy disk as a separate "container."[27] Once a private searcher accessed the disk, the government could search the entire device.[28] The court reasoned that defining an entire device as a "container" created a clear and administrable rule.[29] Additionally, this rule would "preserve[] the competing objectives underlying the Fourth Amendment's protections against warrantless police searches."[30] The court's approach protects a defendant's expectation of privacy in containers unopened by a private searcher[31] and "discourages police from going on 'fishing expeditions' by opening closed containers."[32] The *Runyan* rule is clear and administrable, but it is loosely tailored and exposes excess data to government searches.[33]

The *Runyan* rule has been cited as persuasive precedent in other federal courts. The rule created in *Runyan* was explicitly adopted by the Seventh Circuit in *Rann v. Atchison*.[34] In *Rann*, the court held that the police would not exceed the scope of a private search if they viewed the entire contents of a zip drive and a camera memory card.[35] The *Runyan* rule has also been adopted by district courts outside the Fifth and Seventh Circuits. For example, the Northern District of California cited the *Runyan* rule as persuasive

---

25. *See id.* at 461 ("Due to the lack of definitive guidance from the Supreme Court and the lack of consensus among our sister circuits regarding the precise nature of the evaluation required, we must tread carefully in our disposition of this issue."); *see also* Espeland, *supra* note 22, at 796–815 (outlining the circuit decisions applying the private search doctrine to electronic devices).

26. *See Runyan*, 275 F.3d at 463–64 (discussing the container-based approach in *Jacobsen* and applying that approach to CDs and floppy disks).

27. *See id.* at 464 (finding that any evidence police obtained from each disk not searched by the private searchers was potentially subject to suppression).

28. *See id.* at 463 ("[T]he police exceed the scope of a prior private search when they examine a closed container that was not opened by the private searchers . . . .").

29. *See id.* at 464–65 ("Any evidence that police obtain from a closed container that was unopened by prior private searchers will be suppressed unless they can demonstrate to a reviewing court that an exception to the exclusionary rule is warranted . . . .").

30. *Id.* at 463.

31. *Id.* at 463–64.

32. *Id.* at 464.

33. *See* Lupo, *supra* note 17, at 427 ("[I]n *United States v. Runyan*, the Fifth Circuit held that a private searcher who opened only a few files on a computer had effectively searched the entire hard drive. As a consequence, it was irrelevant that police opened storage files different than those the original private searcher had opened . . . ." (footnotes omitted)).

34. 689 F.3d 832, 837 (7th Cir. 2012) ("We find the Fifth Circuit's holding in *Runyan* to be persuasive, and we adopt it.").

35. *Rann*, 689 F.3d at 838 ("[E]ven if the police more thoroughly searched the digital media devices than S.R. and her mother did and viewed images that S.R. or her mother had not viewed, per the holding in *Runyan*, the police search did not exceed or expand the scope of the initial private searches.").

precedent in *United States v. Guindi*.[36] The court in *Guindi*, however, refrained from fully adopting the *Runyan* rule and emphasized that the private searcher in that case had viewed almost every file on the CDs before the government search.[37] Thus, the *Runyan* rule embodies one side of the circuit split over how the private search doctrine applies to electronic devices.

The Sixth Circuit articulates the other side in *United States v. Lichtenberger*.[38] The court in *Lichtenberger* found that the police exceeded the scope of a private search when they searched an entire laptop.[39] Instead of applying the container-based approach from *Jacobsen*, the court focused on the "virtual certainty" language used in *Jacobsen*.[40] The *Lichtenberger* court reasoned that because a laptop has the capacity to hold vast amounts of information, the threshold of "virtual certainty" to search beyond what the private searcher viewed was a high bar to meet.[41] Additionally, the court argued that the larger storage capacity of the laptop greatly increased the privacy interests of the defendant.[42] The *Lichtenberger* standard limits the government search to just the data viewed by a private searcher, and the government cannot search beyond that data without a warrant unless they are "virtually certain" of what they will find.[43] This standard provides more protection for individual privacy interests but lacks the clarity of the *Runyan* rule because it requires a fact-intensive analysis into what a private searcher actually viewed.[44]

The *Lichtenberger* standard has been both implicitly and explicitly adopted by other federal courts. The Eleventh Circuit took a similar approach in *United States v. Sparks* but did not cite to *Lichtenberger* specifically.[45] In *Sparks*, the Eleventh Circuit found that the police exceeded the scope

---

36. 554 F. Supp. 2d 1018, 1024 (N.D. Cal. 2008) ("This Court finds *Runyan* to be particularly on point.").

37. *Guindi*, 554 F. Supp. 2d at 1025.

38. 786 F.3d 478 (6th Cir. 2015).

39. *Lichtenberger*, 786 F.3d at 491.

40. *Id.* at 488 ("Officer Huston had to proceed with 'virtual certainty' that the 'inspection of the [laptop] and its contents would not tell [him] anything more than he already had been told [by Holmes.]' " (alterations in original) (quoting United States v. Jacobsen, 466 U.S. 109, 119 (1984))).

41. *See id.* at 488–89 (discussing the low probability that a previously unopened file on the laptop would contain similar images of child pornography).

42. *See id.* ("[T]here was a very real possibility Officer Huston . . . could have discovered something *else* on Lichtenberger's laptop that was private, legal, and unrelated to the allegations prompting the search—precisely the sort of discovery the *Jacobsen* Court sought to avoid . . . ."); *see also id.* at 489 ("The same folders . . . could have contained, for example, explicit photos of Lichtenberger himself: legal, unrelated to the crime alleged, and the most private sort of images. Other documents, such as bank statements or personal communications, could also have been discovered among the photographs.").

43. *See* John M. Walton III, Note, *Virtually Certain to Frustrate: The Application of the Private Search Doctrine to Computers and Computer Storage Devices*, 43 N. KY. L. REV. 465, 479–80 (2016).

44. *See id.* at 489–90.

45. 806 F.3d 1323 (11th Cir. 2015).

of a private search by viewing a video stored on a cell phone that the private searcher had not viewed.[46] The police did not exceed the scope of the private search, however, by viewing photos and videos that the private searcher already viewed.[47] Implicitly, the *Sparks* ruling endorsed the *Lichtenberger* standard that only the data viewed by a private searcher can be searched by the government unless the police have "virtual certainty" of what they will find outside the original data viewed.

Two district courts outside of the Sixth and Eleventh Circuits also endorsed a standard similar to the *Lichtenberger* standard. Seven years before the Sixth Circuit decided *Lichtenberger*, the Middle District of Pennsylvania adopted a similar approach in *United States v. Crist*.[48] The *Crist* court held that the police exceeded the scope of a private search when officers searched the entire hard drive of a computer on which a private searcher had only viewed a couple of videos.[49] The court also distinguished the *Runyan* rule by stating that "[a] hard drive is not analogous to an individual disk. Rather, a hard drive is comprised of many platters, or magnetic data storage units, mounted together. Each platter, as opposed to the hard drive in its entirety, is analogous to a single disk as discussed in *Runyan*."[50] The *Crist* court reasoned that the privacy interests of the defendant would not be adequately protected by analogizing the entire hard drive to a single container.[51] *Crist* highlighted concerns over applying the *Runyan* rule to evolving technology—concerns that, after seven additional years of technological evolution, would later influence the *Lichtenberger* analysis. In addition to implicit endorsements of the *Lichtenberger* standard by several courts, the District of Puerto Rico explicitly adopted the standard in *United States v. Rivera-Morales*.[52] Overall, the *Lichtenberger* standard embodies the other side of the circuit split on how the private search doctrine applies to electronic devices.

Determining the extent to which the concept of physical containment applies to electronic storage is the key issue animating the circuit split. To determine the scope of a permissible reconstruction, a court must define a "container" for electronic data.[53] This definition is not obvious. The Court in *Jacobsen* struggled to define the bounds of a *physical* container.[54] Even though there was a closed tube containing bags of drugs within the shipping

46. *Sparks*, 806 F.3d at 1336.

47. *Id.*

48. 627 F. Supp. 2d 575 (M.D. Pa. 2008).

49. *Crist*, 627 F. Supp. 2d at 585–86.

50. *Id.* at 586.

51. *See id.* ("While Crist's privacy interest was lost as to the 'couple of videos' opened by Hipple, it is no foregone conclusion that his privacy interest was compromised as to all the computer's remaining contents.").

52. *See* 166 F. Supp. 3d 154, 166 (D.P.R. 2015) (describing the *Lichtenberger* standard as "after-the-fact confirmation of a private search").

53. Espeland, *supra* note 22, at 781.

54. *See* United States v. Jacobsen, 466 U.S. 109, 120 n.17 (1984).

box, the Court ultimately chose to define the scope of the permissible search by the physical boundaries of the shipping box and found that opening the tube did not go beyond that scope.[55] A box-within-a-box scenario complicates the analysis of the scope of a search, and electronic devices increasingly convolute this assessment.[56]

Electronic devices act like Russian nesting dolls.[57] They can almost infinitely subdivide their contents into smaller and smaller groups.[58] The bigger and more complex the device, the more complicated this boxes-within-boxes nesting can get. For example, on any standard laptop a single picture could be stored in the following way: "Files"–"Documents"–"Folder X"–"Folder Y"–"Folder Z"–"Document A"–"Page 25"–"Picture." This is only one of an almost infinite number of possible organizational schemes, not to mention the possibility of duplicate documents or files stored under different labels. The question, however, remains the same as that in the *Jacobsen* case: At which subdivision does an expectation of privacy become frustrated?[59]

It cannot be the case that every possible item capable of holding others is its own container. Neither the size of the shipping box nor the potential number of smaller boxes it could hold influenced the *Jacobsen* Court's determination.[60] The Court's silence regarding these factors could imply that they do not change the analysis. Or the silence could simply be a product of the specific facts of the case, such that the factors could potentially change the container analysis under different circumstances.

The circuit split in the electronic context highlights both interpretations of the Court's silence on the size and capacity factors. The courts in *Runyan* and *Rann* primarily focused on clearly defining the scope of a search.[61] Tailoring the analysis based on the storage capacity of devices would only serve to create uncertainty for police officers in the field and potentially interfere with efficient investigations.[62] On the other hand, the courts in *Lichtenberger*

---

55. *Id.* at 120.

56. *See* Holley, *supra* note 20, at 682–83; Walton, *supra* note 43, at 487–88.

57. Holley, *supra* note 20, at 682–83.

58. *See id.* at 682.

59. *See Jacobsen*, 466 U.S. at 121 ("[T]he package could no longer support any expectation of privacy; it was just like a balloon 'the distinctive character [of which] spoke volumes as to its contents—particularly to the trained eye of the officer.' " (quoting Texas v. Brown, 460 U.S. 730, 743 (1983) (plurality opinion))).

60. *See id.* at 118–19 ("Even if the white powder was not itself in 'plain view' because it was still *enclosed in so many containers* and covered with papers, there was a virtual certainty that nothing else of significance was in the package . . . ." (emphasis added)).

61. *See* United States v. Runyan, 275 F.3d 449, 461–63 (5th Cir. 2001) ("[T]he police exceed the scope of a prior private search when they examine a closed container that was not opened by the private searchers unless the police are already substantially certain of what is inside that container based on the statements of the private searchers, their replication of the private search, and their expertise."); *see also* Rann v. Atchison, 689 F.3d 832, 837 (7th Cir. 2012) (adopting the holding of *Runyan*).

62. *See Runyan*, 275 F.3d at 465 (arguing that if the police exceeded the scope of the private search every time they encountered an item in the container that the private searcher did

and *Sparks* primarily focused on limiting the types of information exposed to a warrantless search.[63] The devices in those cases had large storage capacities, and that fact fundamentally changed the courts' container analysis.[64] Under this type of analysis, clear, workable rules are considered a secondary concern because electronics are viewed as Fourth Amendment game-changers.[65] Without a clear definition of an electronic container, lower courts will continue to struggle with size and capacity factors when applying *Jacobsen* to electronic private searches. The Supreme Court will need to decide whether size and capacity factors change the *Jacobsen* analysis when applied to electronics and clearly define the scope of an electronic "container" in order to resolve this circuit split.

II. QUANTITATIVE AND QUALITATIVE DIFFERENCES: *CARPENTER*'S DIVIDING LINE

If the Supreme Court does resolve this circuit split, the *Carpenter* opinion's heavy emphasis on the unique nature of CSLI records should greatly influence its analysis of the private search doctrine as applied to electronic devices. This Part explains the relationship between the private search and third-party doctrines, analyzing how the quantity and quality of information stored on electronic devices affects Fourth Amendment analysis. It argues that the circuit split should be resolved based on the logic of *Carpenter*.

The *Jacobsen* Court used reasoning similar to that underlying the third-party doctrine when creating the private search doctrine.[66] The third-party doctrine is based on the idea that a person does not have a reasonable expectation of privacy in any information that they voluntarily disclose to a third party.[67] The private search doctrine, by contrast, does not contain a volun-

---

not find, the result "would over-deter the police, preventing them from engaging in lawful investigation of containers where any reasonable expectation of privacy has already been eroded").

63. *See* United States v. Sparks, 806 F.3d 1323, 1336 (11th Cir. 2015) ("While Widner's private search of the cell phone might have removed certain information from the Fourth Amendment's protections, it did not expose every part of the information contained in the cell phone."); United States v. Lichtenberger, 786 F.3d 478, 489 (6th Cir. 2015) ("[Folders searched on the laptop] could have contained, for example, explicit photos of Lichtenberger himself: legal, unrelated to the crime alleged, and the most private sort of images. Other documents, such as bank statements or personal communications, could also have been discovered among the photographs. . . . The reality of modern data storage is that the possibilities are expansive.").

64. *Sparks*, 806 F.3d at 1336 (discussing the large storage capacity of cell phones, the range of information types cell phones are able to store, and the potentially intimate nature of that information); *Lichtenberger*, 786 F.3d at 488 (discussing the many types of data computers are able to store in vast amounts for long periods of time).

65. *Lichtenberger*, 786 F.3d at 486–87 ("[S]earches of physical spaces and the items they contain differ in significant ways from searches of complex electronic devices under the Fourth Amendment.").

66. United States v. Jacobsen, 466 U.S. 109, 117 (1984).

67. *See* United States v. Miller, 425 U.S. 435, 442 (1976).

tariness requirement—it generally applies to situations where a person did not give a third party permission to access their information.[68] The lack of a voluntariness element arguably creates a greater individual privacy interest in the private search doctrine than in the third-party doctrine. In a government search under the former, the individual did not necessarily intend to share their information with a third party and assume the risk that the third party would disclose that information to the police. Notably, the Court in *Carpenter*, when analyzing third-party doctrine, found that CSLI is not voluntarily shared by cell phone users and gave greater protection to privacy interests as a result.[69] At the very least, individual privacy interests under the private search doctrine are on par with those under the third-party doctrine. But can the logic applied in *Carpenter* be applied to the private search doctrine?

Carpenter focused on the uniqueness of CSLI and technological advances generally.[70] The Court emphasized "the *seismic shifts* in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years."[71] These "seismic shifts" made CSLI a "distinct category of information" to which the Court declined to extend the third-party doctrine.[72] *Carpenter* was not the first time that the Court limited an established doctrine under the Fourth Amendment due to the quantity and quality of information made available through digital technology. The Court in *Riley v. California* found that the high storage capacity of electronic devices and their ability to connect to the internet made them categorically different from other physical items.[73] The *Riley* Court declined to extend the search-incident-to-arrest exception to the

68. *See Jacobsen*, 466 U.S. at 130 (White, J., concurring in part and concurring in the judgment) (arguing that the analogy between the third-party doctrine and the private search doctrine "is imperfect since the risks assumed by a person whose belongings are subjected to a private search are not comparable to those assumed by one who voluntarily chooses to reveal his secrets to a companion").

69. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements." (alteration in original) (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979))).

70. *See id.* at 2219 ("While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision. . . . [W]ireless carriers already have the capability to pinpoint a phone's location within 50 meters.").

71. *Id.* (emphasis added).

72. *Id.* at 2219–20.

73. 573 U.S. 373, 393–97 (2014) (discussing the vast amount of information that electronics can store and how the internet can store even more information).

warrant requirement and held that police must obtain a warrant before digitally searching electronic devices incident to arrest.[74] Taken together, *Carpenter* and *Riley* signal that digital technology is a turning point for Fourth Amendment law.

Many scholars have argued that electronics are qualitatively different from other physical items and should be treated differently under the Fourth Amendment.[75] Their argument centers on the fact that "[m]odern computers are able to store vast amounts of information, equal to approximately eighty million pages of text, with capacity doubling approximately every two years."[76] Not only do electronic devices have astonishingly large storage capacities, they contain an immense amount of personal information and hold "the privacies of life."[77] Any given smartphone might hold "a wealth of detail about [one's] familial, political, professional, religious, and sexual associations."[78] Professor Orin Kerr argues that digital searches of electronic devices are more invasive of privacy interests than searches of the home.[79] According to Kerr, the need to create different Fourth Amendment rules for digital technology will become self-evident as technology continues to advance.[80]

The qualitative differences between digital devices and other physical objects are further underscored by the fact that most digital devices can connect to the internet.[81] The Court in *Riley* expressed concern over how an internet connection could drastically change the nature of a search.[82] In *Riley*, Chief Justice Roberts stated that the analogy of a cell phone to a container "crumbles entirely when a cell phone is used to access data located else-

---

74. *Riley*, 573 U.S. at 401–03. It should be noted that both *Lichtenberger* and *Sparks* cited the *Riley* decision as part of their reasoning. United States v. Sparks, 806 F.3d 1323, 1336 (11th Cir. 2015); United States v. Lichtenberger, 786 F.3d 478, 487 (6th Cir. 2015). Additionally, both *Runyan* and *Rann* were decided years before *Riley*, so the *Riley* decision could potentially alter the Fifth and Seventh Circuits' analysis in the future.

75. *See, e.g.*, Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

76. Holley, *supra* note 20, at 682 (footnotes omitted) ("For context, this is more information than is contained in one floor's worth of academic journals in the average university library." (footnote omitted)).

77. *Riley*, 573 U.S. at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)); Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 405 (2013) ("Much of the information stored in a person's cellular phone is deeply personal. The information can include photographs, text messages, e-mails, personal notes, records of visited websites, and many other kinds of personal information.").

78. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

79. *See* Kerr, *supra* note 75, at 569.

80. Kerr, *supra* note 77, at 407–08 ("Over time, advancing technology will cause the digital to seem more and more different from the physical. The need for different rules governing digital devices eventually will seem obvious.").

81. *See* Andrew Meola, *What is the Internet of Things (IoT)? Meaning & Definition*, BUS. INSIDER (May 10, 2018, 1:06 PM), http://www.businessinsider.com/internet-of-things-definition [https://perma.cc/FDG4-E92W].

82. *See Riley*, 573 U.S. at 397.

where, at the tap of a screen."[83] "Cloud computing," the ability of "Internet-connected devices to display data stored on remote servers rather than on the device itself," is a good example.[84] The rise of cloud computing has altered our understanding of what it means for information to be contained on a device because "[c]ell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference."[85] These device features are why many argue that the *Jacobsen* standard should be limited to physical containers only.[86] In *Jacobsen*, the police could not open any other box and find the exact same drugs that were inside the shipping box. If a person can access "the cloud" from any device that can connect to the internet, the analogy of electronics to containers breaks down at a fundamental level.

Beyond the quantitative and qualitative factors, *Carpenter*'s logic regarding voluntariness can be applied to the private search circuit split as well. Cell phones and electronic devices are pervasive in society.[87] That fact has not gone unnoticed by the Court.[88] In *Carpenter*, the Court went so far as to say that "carrying [a cell phone] is indispensable to participation in modern society."[89] The indispensable nature of cell phones and electronic devices in modern society decreases the likelihood that a person is knowingly assuming the risk that a third party will view their information. In fact, most people carry their mobile devices on their person for nearly twenty-four hours a day[90]—effectively keeping them away from third parties. In essence, our electronic devices have become extensions of ourselves. They follow us

83. *Id.*

84. *Id.*

85. *Id.*

86. *See, e.g.*, Dylan Bonfigli, Note, *Get a Warrant: A Bright-Line Rule for Digital Searches Under the Private-Search Doctrine*, 90 S. CAL. L. REV. 307, 331 (2017) ("Because of the differences in privacy concerns, courts should not treat personal computers in the same way as the cardboard box in *Jacobsen* and other physical containers."); Walton, *supra* note 43, at 493 ("Due to the extensive privacy interests at stake, and the impracticability of applying the private search doctrine to computers—under either the physical device approach or the data or file approach—courts should preclude the government's use of the private search doctrine when the 'container' involved is a computer.").

87. *See Mobile Fact Sheet*, PEW RES. CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/G6XC-JYFZ] (stating that 95% of U.S. adults own a cell phone, 77% own a smartphone, 73% own desktop or laptop computers, and 53% own a tablet computer).

88. *See Riley*, 573 U.S. at 395 ("According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.").

89. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

90. *See id.* at 2218 ("[T]hey compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.").

wherever we go and record our lives in detail.[91] The deeply personal nature of the contents of electronic devices and their immense storage capacity weigh heavily in favor of applying a *Carpenter*-like rule to the private search doctrine, despite the fact that the doctrine does not have a voluntariness requirement. The *Carpenter* Court recognized that technological advancements change the Fourth Amendment balancing act due to large shifts in privacy interests.[92] It is time for the Court to do the same with the private search doctrine.

III. CREATING A NARROW ELECTRONIC PRIVATE SEARCH DOCTRINE

The private search doctrine must be very narrowly applied to electronic devices. The Court should use the logic of *Carpenter*, in the context of the third-party doctrine, to narrow the scope of the private search doctrine because of the close relationship between those two doctrines. The original balance of interests struck in *Jacobsen* must be altered to give sufficient protection to privacy interests in this new context. This Part proposes a narrow rule in order to resolve the circuit split, addresses possible counterarguments, and provides policy justifications for the proposed rule.

The scope of a digital government search should be limited to just the data viewed by a private searcher. This rule is based on Professor Kerr's exposed-data approach to digital searches generally.[93] Kerr's argument is based on the concept of plain view: if the officer does not have a warrant to search the computer, the scope of his search authority is limited to just that information displayed on the screen without any manipulation by the officer.[94] This supports narrowing the private search doctrine for electronic devices because the Court in *Jacobsen* cited to the plain view doctrine when creating the private search doctrine.[95] Thus, when a private party shows a government agent data related to criminal activity, the government agent is allowed to view what is exposed on the screen, so long as what is shown is what the private party previously saw. No other data can be viewed, and the agent

---

91. *See, e.g.*, Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html (on file with the *Michigan Law Review*).

92. *See Carpenter*, 138 S. Ct. at 2220 ("[This case] is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* or *Miller*.").

93. *See* Kerr, *supra* note 75, at 556–57 ("The scope of a computer search should be whatever information appears on the output device, whether that output device is a screen, printer, or something else. Under this approach, scrolling down a word processing file to see parts of the file that were previously hidden is a distinct search of the rest of the file.").

94. *See id.* (discussing the fact that searches of any kind are generally related to human observation and that data can be organized in many different ways).

95. United States v. Jacobsen, 466 U.S. 109, 119–20 (1984) (citing Coolidge v. New Hampshire, 403 U.S. 443, 487–90 (1971)) ("The agent's viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment.").

cannot manipulate the screen in any way in order to expose more data. In order to search more, the agent must get a warrant.[96]

This bright-line rule comes with practical downsides. Under the proposed rule, police will likely have difficulty proving exactly what was on a screen during a private search. For instance, if a private searcher closes a file or turns off a device after finding evidence of a crime, the police will have to use extreme caution to reconstruct the private search. Police will have to ask the private searcher, "Can you show me *exactly* what you saw?" and engage in a factual inquiry that retraces the exact steps of the private searcher. Scrolling, clicking, or opening files will only be allowed if the private searcher performed those same actions previously. If the private searcher cannot remember their exact steps, the officer must stop and get a warrant to finish searching the device.[97] The ban on independent officer manipulation thus eliminates any discretion to widen the scope of a search.

This nonmanipulation rule is likely to impose a warrant requirement on a large swath of previously permissible searches under the private search doctrine. Some might even argue that the ban on independent officer manipulation will virtually eviscerate the private search doctrine because private searchers often do not remember exactly what they opened before finding the contraband or evidence.[98] While descriptions from a private searcher can be used as evidence to support a warrant application,[99] establishing probable cause could still be difficult without an officer's firsthand observations. These concerns are valid, but the proposed rule only requires officers to follow the same nonmanipulation principles in the digital world as they already do in the physical world.

These principles are most clearly presented by the plain view doctrine. If officers are legally authorized to be in a space, they are allowed to seize any contraband or evidence in plain view.[100] But officers are not allowed to abuse the doctrine by manipulating their surroundings in order to broaden their

96. Unless another exception to the warrant requirement, such as exigency, applies.

97. *See* Kerr, *supra* note 75, at 556–57.

98. *Cf.* Adam A. Bereston, Comment, *The Private Search Doctrine and the Evolution of Fourth Amendment Jurisprudence in the Face of New Technology: A Broad or Narrow Exception?*, 66 CATH. U. L. REV. 445, 472–73 (2016) ("When a private searcher cannot be certain whether the images shown to police are among the same images viewed during the initial private search, otherwise reasonable police conduct would be held unreasonable . . . . The aforementioned factual quandary created by this demanding standard may very well signal the death of the private search doctrine.").

99. *See* Illinois v. Gates, 462 U.S. 213, 238 (1983) ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.").

100. Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971) ("What the 'plain view' cases have in common is that the police officer in each of them had a prior justification for an intrusion in the course of which he came inadvertently across a piece of evidence incriminating the accused.").

search.[101] For example, the Supreme Court found that moving objects in order to view the serial number of a stereo was impermissibly manipulative under the plain view doctrine.[102] And under the related plain feel doctrine, officers cannot manipulate an item in a person's pocket during a *Terry* pat down in order to determine its contents.[103] Because the private search doctrine was created using reasoning similar to the plain view doctrine,[104] it follows that similar nonmanipulation principles should be extended to the private search context. The proposed rule places no more restrictions on officers in the digital context than in the physical world.

Another notable downside of the proposed rule is that its screen-based approach prevents officers from accessing metadata without a warrant. Metadata is "data about data."[105] It is used to "organize, manage, and facilitate the use and understanding of primary data."[106] Metadata typically does not appear on paper printouts of electronic files or on the screen when electronic files are opened.[107] Consequently, it is highly unlikely that a private searcher will ever see metadata during their initial search—thus requiring an officer to get a warrant before searching for that information. Metadata can be some of the most useful information to law enforcement.[108] The proposed rule will restrict police access to this useful information, but that is the cost that the Fourth Amendment requires in order to protect twenty-first century privacy interests. Police will still have tools available to get this coveted information: warrants and other exceptions to the warrant requirement.[109]

Despite its downsides, a narrow electronic private search doctrine preserves the central logic of *Jacobsen* but more effectively protects twenty-first century privacy interests by extending the logic of *Carpenter*. The logic of *Jacobsen* is straightforward: (1) A private party does not violate the Fourth

---

101. *See id.* ("[T]he 'plan view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.").

102. Arizona v. Hicks, 480 U.S. 321, 324–25 (1987).

103. Minnesota v. Dickerson, 508 U.S. 366, 379 (1993).

104. *See supra* note 95 and accompanying text.

105. Adam K. Israel, Note, *To Scrub or Not to Scrub: The Ethical Implications of Metadata and Electronic Data Creation, Exchange, and Discovery*, 60 ALA. L. REV. 469, 469–70 (2009) ("For example, metadata often reports the author's name and initials; the name of the company or organization where the document was created; the name of the author's computer; the name of the server or network on which the document was saved; the names of previous document authors; the original text, along with any revisions to the original text; template information; any digital comments made on the document; document versions; and hidden text.").

106. *Metadata*, BLACK'S LAW DICTIONARY (10th ed. 2014).

107. GEORGE L. PAUL & BRUCE H. NEARON, THE DISCOVERY REVOLUTION: E-DISCOVERY AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE 100 (2006); Steven C. Bennett & Jeremy Cloud, *Coping with Metadata: Ten Key Steps*, 61 MERCER L. REV. 471, 471 (2010).

108. *See, e.g.*, Parmy Olson, *Apple's Messages Metadata Could Be Valuable to Law Enforcement*, FORBES (Sept. 29, 2016, 1:07 PM), https://www.forbes.com/sites/parmyolson/2016/09/29/apples-messages-metadata-could-be-valuable-to-law-enforcement/ [https://perma.cc/82KA-BJQ9].

109. *See supra* notes 9–12 and accompanying text.

Amendment by searching the property of another;[110] (2) A person loses their expectation of privacy in information that a third party reveals to government officials;[111] (3) "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information."[112] The scope of what is nonprivate information during the government's subsequent search is what has caused the circuit split.

This is where *Carpenter*'s logic applies. The *Carpenter* Court focused on the fact that "the retrospective quality of the data here gives police access to a category of information otherwise unknowable."[113] If the scope of the government search is allowed to be any wider than the exposed and previously viewed data, there is a greater risk that the agent will view information unknown to the private searcher. That information might be of a completely different character than the previously searched data,[114] and the owner's expectation of privacy in that information might not be frustrated. The proposed rule makes *Jacobsen*'s "virtual certainty" standard into a bright-line rule by clearly stating that in the digital context, police can never be "virtually certain" of what they will find outside of the exposed and previously searched data.[115] For example, if while reconstructing a private search an officer sees an unopened file labeled "Murder Details," the officer would not be able to open the file under the proposed rule. The officer could not be "virtually certain" of the file's contents based on the label alone.[116] The best way to ensure that police do not use the window of nonprivate information conveyed by a private searcher to break into an entire warehouse of private information is to make the window as small as possible.

In order to protect the heightened privacy interests in the digital context, this rule does not extend the *Jacobsen* container-based approach. Although

---

110. United States v. Jacobsen, 466 U.S. 109, 113–14 (1984) (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)).

111. *Id.* at 117.

112. *Id.*

113. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

114. *Cf.* People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.").

115. *See Jacobsen*, 466 U.S. at 119. This bright-line rule distinguishes the proposal of this Note from the *Lichtenberger* standard. The *Lichtenberger* standard is narrow in scope, but it allows for officers to search beyond the data previously viewed by a private party without a warrant if the officers are "virtually certain" of what they will find. Walton, *supra* note 43, at 479–80.

116. *Cf.* RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 51 (2007) ("Criminals can easily hide evidence by mislabeling files. It is unlikely that a suspect will label a file 'evidence-of-a-crime.doc' or some other variation that clearly indicates that the file contains pertinent evidence. Additionally, evidence of a crime can be found in almost any type of file." (footnote omitted)).

the container-based approach provides a clear, administrable rule for law enforcement,[117] it sacrifices significant privacy interests. There is concern that a narrow rule will overdeter police and make officers reluctant to conduct a search under the private search doctrine at all for fear of mistakenly finding evidence that could later be suppressed at trial.[118] This concern is misplaced. A narrow rule will provide the police with more guidance about what is and is not a valid search under the private search doctrine. Giving the police wide discretion under the container-based approach will cause numerous suppression issues because courts can question every decision officers make during such broad searches. A narrow approach eliminates the discretionary element of a search and will likely reduce the number of suppression issues. Even if the narrow approach deters police from taking arguably reasonable action, that is not necessarily a bad outcome.[119] Promoting caution before searching through what could amount to an entire chronicle of someone's life restrains government overreach into individual privacy.

The narrow approach is also criticized for wasting time and resources by forcing police to obtain warrants based on limited information.[120] But there is no evidence that the administrative costs of obtaining warrants are astronomically large. Notably, many scholars have argued that the probable cause standard articulated in *Illinois v. Gates*[121] makes obtaining a warrant easier in the modern age.[122] Additionally, many states and the federal government permit police to obtain a warrant by telephone—greatly reducing time and resource costs.[123] Although it might be inconvenient for officers to obtain a

117. *See* Bereston, *supra* note 98, at 472 (arguing that police can be trusted to search an entire electronic device under the private search doctrine because police are reasonable actors).

118. *See, e.g.*, United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001) (arguing that a narrow approach "would over-deter the police, preventing them from engaging in lawful investigation of containers where any reasonable expectation of privacy has already been eroded"); Bereston, *supra* note 98, at 470 (arguing that a narrow approach "would lead police to be reluctant when conducting a subsequent search for fear that they will discover important evidence that will be subject to suppression simply because the private searcher did not happen to discover that evidence during his or her initial search").

119. *See* Lawrence Rosenthal, *Binary Searches and the Central Meaning of the Fourth Amendment*, 22 WM. & MARY BILL RTS. J. 881, 883 (2014) ("For [Justice Frankfurter], the central meaning of the Fourth Amendment, derived from its history, was that when discretion is afforded to law-enforcement officers to engage in search and seizure, it is all too likely to be abused, and accordingly searches and seizures not previously authorized by a warrant should be condemned in the absence of strict necessity.").

120. *See, e.g.*, *Runyan*, 275 F.3d at 465; Bereston, *supra* note 98, at 470–71.

121. 462 U.S. 213, 230–31 (1983).

122. *See, e.g.*, Phyllis T. Bookspan, *Reworking the Warrant Requirement: Resuscitating the Fourth Amendment*, 44 VAND. L. REV. 473, 476–77 (1991); Erica Goldberg, *Getting Beyond Intuition in the Probable Cause Inquiry*, 17 LEWIS & CLARK L. REV. 789, 792 (2013) ("Courts have determined, for example, that both positive alerts from drug sniffing dogs and fingerprint matches are sufficient on their own, without any other evidence, to satisfy probable cause [under *Gates*].").

123. *See* Barbara C. Salken, *Balancing Exigency and Privacy in Warrantless Searches to Prevent Destruction of Evidence: The Need for a Rule*, 39 HASTINGS L.J. 283, 329 (1988); *see also*

warrant, mere inconvenience cannot outweigh the heightened privacy interests in these types of cases.[124] Furthermore, many electronic private search cases involve easily recognizable contraband.[125] In these cases, the police will already have enough information to obtain a search warrant for the entire device. And in truly time-sensitive cases, the police can use the exigent circumstances exception to the warrant requirement.[126]

The narrow approach has the additional benefit of consistent application across all types of devices. Under the container-based approach, the scope of a search changes drastically if the device is a laptop or a CD.[127] The proposed rule's focus on the exposed data on the screen ensures that the scope of a search is sufficiently consistent across device types. Electronics are like icebergs. What is exposed on the screen at any given time is only a fraction of what the entire device contains. Limiting police to the tip of the iceberg prevents unfettered access merely because of a device's storage capacity.

John Michael Harlow, Note, California v. Acevedo*: The Ominous March of a Loyal Foot Soldier*, 52 LA. L. REV. 1205, 1243 n.186 (1992) ("Today, police may use a telephone to submit a warrant. Even in overworked metropolitan judicial systems, a search warrant can be obtained within four hours.").

124. *See* Mincey v. Arizona, 437 U.S. 385, 393 (1978) ("The investigation of crime would always be simplified if warrants were unnecessary. But the Fourth Amendment reflects the view of those who wrote the Bill of Rights that the privacy of a person's home and property may not be totally sacrificed in the name of maximum simplicity in enforcement of the criminal law." (citing United States v. Chadwick, 433 U.S. 1, 6–11 (1977)).

125. This most commonly occurs in child pornography cases. *See, e.g.*, United States v. Lichtenberger, 786 F.3d 478, 480–81 (6th Cir. 2015); United States v. Tosti, 733 F.3d 816, 818–19 (9th Cir. 2013); Rann v. Atchison, 689 F.3d 832, 834 (7th Cir. 2012). Many people in possession of child pornography have a "collector's mentality." Emily Bazelon, *The Price of a Stolen Childhood*, N.Y. TIMES MAG. (Jan. 24, 2013), http://www.nytimes.com/2013/01/27/magazine/how-much-can-restitution-help-victims-of-child-pornography.html [https://perma.cc/JA6F-NBCW]. Because of this mentality, it is very likely that a "collector" will have more than one image of child pornography in his or her possession. *See, e.g.*, United States v. Crist, 627 F. Supp. 2d 575, 579 (M.D. Pa. 2008) (stating that almost 1,600 images of child pornography were found on the defendant's laptop). Thus, the police will most likely have at least one image of child pornography obtained through the private search and the knowledge that it is highly likely that there are more images on the device. This should be sufficient to obtain a search warrant for the device.

126. *See* Kentucky v. King, 563 U.S. 452, 455 (2011) ("It is well established that 'exigent circumstances,' including the need to prevent the destruction of evidence, permit police officers to conduct an otherwise permissible search without first obtaining a warrant."). Under the exigent circumstances exception, police are allowed to conduct a warrantless search in order to prevent the *imminent* destruction of evidence. Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (citing Ker v. California, 374 U.S. 23, 40 (1963) (plurality opinion)). The only additional restraint on police under this exception is that "[they do] not create the exigency by engaging or threatening to engage in conduct that violates the Fourth Amendment." *King*, 563 U.S. at 462. The exception would thus allow officers to bypass the proposed rule's warrant requirement in truly time-sensitive circumstances not unlawfully manufactured by the officers themselves.

127. *See Timeline of Computer History*, COMPUTER HIST. MUSEUM, http://www.computerhistory.org/timeline/memory-storage/ [https://perma.cc/F37X-7ZQX] (showing how the memory and storage capacity of electronic devices has changed over time and differs among devices).

Perhaps one of the greatest benefits of the proposed rule—besides protecting privacy interests—is that it promotes more thorough government investigations. It creates the same incentives for police that exist under the exclusionary rule: if evidence is repeatedly suppressed, investigatory behavior will adjust accordingly.[128] In the long run, this narrow rule promotes evidence gathering outside of the device itself in order to secure a warrant for the device. Better investigation practices benefit society because they help ensure that police action is based on facts rather than hunches and sloppy investigations.[129] For example, a rule that encourages police to look for more evidence can combat confirmation bias.[130] If police find evidence on an electronic device that supports their theory, they might be disinclined to fully consider an alternative theory or alibi evidence.[131] Thus, while the proposed rule may impose additional procedural hurdles, it does so to the benefit of law enforcement investigations, not the cost.

Finally, a narrow electronic private search doctrine complies with the spirit of the Fourth Amendment. As Justice Brennan described it, "[a]lthough the self-restraint and care exhibited by the officers . . . is commendable, that alone can never be a sufficient protection for constitutional liberties."[132] The Fourth Amendment was not designed to make law enforcement's job easy. It was designed as a barrier to the government's natural tendency to expedite the criminal justice process at the expense of individual liberty.[133] While the government's interest in detecting crime and convicting criminals is strong, the Fourth Amendment requires that interest to outweigh the individual interest in privacy before it can be pursued through searches and seizures. In the context of digital devices and the private search doctrine, absent narrowly defined circumstances, the individual's privacy interest should always be protected.

---

128. *Cf.* United States v. Leon, 468 U.S. 897, 955 (1984) (Brennan, J., dissenting) (noting that police officers operating under the exclusionary rule will "devote greater care and attention to providing sufficient information to establish probable cause" than they otherwise would).

129. *See, e.g.*, D. Kim Rossmo, *Criminal Investigative Failures: Avoiding the Pitfalls*, FBI L. ENFORCEMENT BULL., Sept. 2006, at 1, 4 (discussing how tunnel vision and satisficing can prevent police from investigating leads and looking for more evidence after they are satisfied that they have the right suspect).

130. *See id.* at 6 ("Confirmation (or verification) bias constitutes a type of selective thinking whereby individuals notice or search for evidence that confirms their theory while ignoring or refusing to look for contradicting information.").

131. *See id.*

132. *Leon*, 468 U.S. at 948 (Brennan, J., dissenting).

133. *See id.* at 929–30 ("While the machinery of law enforcement and indeed the nature of crime itself have changed dramatically since the Fourth Amendment became part of the Nation's fundamental law in 1791, what the Framers understood then remains true today—that the task of combating crime and convicting the guilty will in every era seem of such critical and pressing concern that we may be lured by the temptations of expediency into forsaking our commitment to protecting individual liberty and privacy.").

CONCLUSION

The scope of the private search doctrine has been contested since its inception.[134] The doctrine's application in the digital world, however, has made the debate even more important. Under the private search doctrine, an individual who did not consent to third-party search of his or her device is exposed to a second government search.[135] Under the container-based approach, an entire device could then be subject to government search without a warrant.[136] This essentially opens a person's entire life to government inspection without any judicial review.[137] In order to prevent this enormous intrusion into a person's privacy, the Court should create a narrow electronic private search doctrine. Requiring law enforcement to obtain a warrant if they wish to search an entire device is a necessary barrier to ensure that a small privacy intrusion by a third party does not open the door for extensive government intrusion into a digital chronicle of someone's life.

Technological advancements will continue to challenge the way we think about the Fourth Amendment. Digital devices have drastically changed everyday American life.[138] Our devices are overflowing with our personal thoughts, movements, and contacts.[139] As technology continues to evolve, Fourth Amendment doctrines will fail to meet the needs of modern society without significant alterations to account for ever-expanding digital worlds. The circuit split over how the private search doctrine applies to electronic devices is just one example of how technology challenges current Fourth Amendment doctrine.[140] As the *Carpenter* decision demonstrated, just because an established doctrine *can* be applied in the electronic context does not mean that it *should*.[141] As courts continue to confront difficult questions of Fourth Amendment law, they must use decisions like *Carpenter* as their guide to better protect privacy interests in the twenty-first century.

---

134. *See* United States v. Jacobsen, 466 U.S. 109, 134 (1984) (Brennan, J., dissenting); *see also supra* note 18 and accompanying text.

135. *See Jacobsen*, 466 U.S. at 119.

136. United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001).

137. *See supra* note 77.

138. *See, e.g.*, Brad Stone, *Breakfast Can Wait. The Day's First Stop Is Online.*, N.Y. TIMES (Aug. 9, 2009), https://www.nytimes.com/2009/08/10/technology/10morning.html [https://perma.cc/T4YE-Q642].

139. *See* Dominic Basulto, *Just Say No to Digital Hoarding*, WASH. POST (Dec. 16, 2014), https://www.washingtonpost.com/news/innovations/wp/2014/12/16/just-say-no-to-digital-hoarding/ [https://perma.cc/D3MC-4CYF].

140. *See, e.g.*, Lucy Bertino, *Courts Continue to Split on the Fourth Amendment in Cyberspace*, N.C. J.L. & TECH. (Feb. 22, 2017), http://ncjolt.org/circuit-split-4th-amendment-cyberspace/ [https://perma.cc/4XM6-KXFB] ("[T]here is a huge divide within the legal community as to what information the United States can compel when the information may not be stored within the jurisdictional boundaries of the United States.").

141. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216–17 (2018) ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.").