PRIVACY IN THE DIGITAL AGE: PRESERVING THE FOURTH AMENDMENT BY RESOLVING THE CIRCUIT SPLIT OVER THE PRIVATE-SEARCH DOCTRINE

Matthew A. Lupo

INTRODUCTION

In *United States v. Lichtenberger*,[1] the United States Court of Appeals for the Sixth Circuit granted a motion to suppress evidence of child pornography found on the defendant's laptop computer.[2] The court reasoned that police exceeded the scope of the private-search doctrine because they did not have "virtual certainty" that they would not discover information that the private searcher—the defendant's girlfriend—had not already discovered and revealed to police.[3] In effect, this decision extended the United States Supreme Court's decision in *Riley v. California*,[4] which held that the storage capacity of electronic devices[5] significantly increases the risk of violating privacy interests when balancing the government's interest against personal-privacy interests to determine a violation of the Fourth Amendment.[6]

Not long after *Lichtenberger*, the United States Court of Appeals for the Eleventh Circuit followed the Sixth Circuit's logic in *United States v. Johnson*.[7] In relevant part, the court concluded that police exceeded the scope of the private-search doctrine by viewing a video on the defendant's cell-phone that the initial private searcher had not viewed.[8] The court reasoned that allowing police

---

1 United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015).

2 *Id.* at 480.

3 *Id.* at 488–89.

4 Riley v. California, 134 S. Ct. 2473 (2014).

5 For example, cell-phones, laptops, etc.

6 *Riley*, 134 S. Ct. at 2488–89 (discussing how courts balance legitimate government interest with defendants' privacy interests).

7 United States v. Johnson, 806 F.3d 1323, 1335–36 (11th Cir. 2015).

8 *Id.* at 1335–37. Unlike *Lichtenberger*, the *Johnson* court ultimately denied the petitioner's motion to suppress evidence. However, it did so on other

to view the video when the private searcher had not already viewed it was not protected under the private-search doctrine, and would therefore be inconsistent with *Riley*.[9]

According to Professor Orin Kerr of the George Washington University Law School, the *Lichtenberger* ruling created a circuit split between the Sixth Circuit, and the Fifth and Seventh Circuits, with respect to what the particular "unit" of a private search is—specifically, the device itself versus the individual files and data contained therein.[10] Furthermore, Professor Kerr has since argued that the more recent ruling in *Johnson* added an additional layer to the split.[11] With regard to the split, in *United States v. Runyan*,[12] the Fifth Circuit adopted a fairly broad interpretation of the private-search doctrine by only partially excluding evidence of computer disks alleged to contain child pornography that the government had found through a warrantless search.[13] In doing so, the court ruled that:

> police exceed the scope [of the private-search doctrine] . . . when they examine a closed container that was not opened by . . . 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.[14]

Upholding this rule a decade later in *Rann v. Atchison*,[15] the Seventh Circuit held that one memory card and one zip drive that

---

grounds—specifically, that police had properly obtained a warrant for other incriminating evidence that was not the subject of the appeal. *Id.*

9 *Id.* at 1336. *See also Riley*, 134 S. Ct. at 2488–89 (holding that, as a result of the vast storage capabilities of electronic-storage devices, personal-privacy interests outweigh government interests when determining whether police have violated the Fourth Amendment).

10 Orin Kerr, *Sixth Circuit creates circuit split on private search doctrine for computers*, THE WASHINGTON POST (May 20, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/20/sixth-circuit-creates-circuit-split-on-private-search-doctrine-for-computers/.

11 Orin Kerr, *11th Circuit deepens the circuit split on applying the private search doctrine to computers*, THE WASHINGTON POST (Dec. 2, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/02/11th-circuit-deepens-the-circuit-split-on-applying-the-private-search-doctrine-to-computers/.

12 United States v. Runyan, 275 F.3d 449, 465–66 (5th Cir. 2001).

13 *Id.*

14 *Id.* at 463.

15 Rann v. Atchison, 689 F.3d 832, 834 (7th Cir. 2012).

a victim of child pornography and her mother gave to police were admissible evidence.[16] The court reasoned that the police could be "substantially certain" that the devices contained child pornography because the victim and her mother knew the precise contents of the drives when they handed them over to police.[17]

Professor Kerr's assertion, the reasoning employed by the *Lichtenberger* and *Johnson* courts, and other case law pertaining to the private-search doctrine demonstrate the imperative need for a resolution to the circuit split.[18] First articulated in *United States v. Jacobsen*,[19] the private-search doctrine is the theory that once a private individual frustrates another private individual's expectation of privacy—that is, conducts a private search—the Fourth Amendment does not bar the government from using that now non-private information.[20] With that said, the Fourth Amendment still prohibits the government from exceeding the scope of the initial private search when the government chooses to conduct a follow-up search without a warrant.[21]

Professor Kerr's argument, as well as the logic employed by the *Lichtenberger* and *Johnson* courts, also demonstrates the problematic and varied applications of the private-search doctrine to electronic-storage devices.[22] In light of the Court's ruling in *Riley*,[23] the prevalence of electronic-storage devices,[24] such devices' capacity to store vast quantities of information about all aspects of

---

16 *Id.*

17 *Id.* at 837–38.

18 *See* discussion *infra* Part III.

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

20 *Id.*

21 *Id.* at 116.

22 *See* United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015) (holding that police exceeded the scope of the private-search doctrine because they did not have virtual certainty they would not discover anything that the private searcher had not already discovered); United States v. Johnson, 806 F.3d 1323, 1336 (11th Cir. 2015) (holding that police exceeded the scope of the private-search doctrine by viewing a video on a phone that the private searcher had not already viewed); Kerr, *supra* notes 10–11 (discussing the circuit splits regarding the private-search doctrine).

23 Riley v. California, 134 S. Ct. 2473, 2488–89 (2014) (holding that, as a result of the vast storage capabilities of electronic-storage devices, personal-privacy interests outweigh government interests when determining whether police have violated the Fourth Amendment).

24 *See* Monica Anderson, *Technology Device Ownership: 2015*, PEW RESEARCH CTR. (Oct. 29, 2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015 (outlining statistics of ownership rates and uses for modern-day electronic-storage devices).

a person's life,[25] and the difference between physical and digital evidence,[26] it is critical to address this circuit split in order to protect individual liberties.[27] If courts fail to adapt the doctrine to modern technology by resolving this circuit split, then it is not only possible but even likely that government actors will infringe upon citizens' Fourth Amendment rights.[28] Furthermore, the government may prosecute more defendants similar to *Lichtenberger*, in which trials are predicated on evidence obtained through invalid searches, potentially allowing wrongdoers to evade convictions by successfully moving to exclude such evidence.[29] The issues raised in *Riley* suggest that the Supreme Court should be willing to reconsider across the board whether courts should treat physical and digital evidence differently and how that might impact the scope of the private-search doctrine.[30]

Scholarly attention to this issue is relatively scant,[31] and this Note proposes a simple and readily-obtainable solution by which courts may solve this issue while providing law enforcement and private citizens a necessary level of predictability in the realm of private searches of electronic-storage devices.[32] In short, the Supreme Court should rule that the virtual-file test[33] is the only appropriate scope of a warrantless government search following a private search of an electronic-storage device.[34] This proposal is unique in that it predicates itself on the practical consequences of the unfathomable and ever-evolving storage capability of modern-day electronic-storage devices.[35] Such advanced technology was

---

25 *See, e.g.*, *iPhone*, APPLE, http://www.apple.com/iphone-6s/specs/ (last visited Oct. 26, 2015) (outlining the vast storage capability of modern-day electronic-storage devices, which includes pictures, videos, and related personal information).

26 *See* State v. Rupnick, 280 Kan. 720, 735–36 (2005) (discussing the differences between hard drives and physical containers).

27 *See infra* Part III.

28 *See id.*

29 *See, e.g.*, United States v. Lichtenberger, 786 F.3d 478, 491 (6th Cir. 2015) (granting the defendant's motion to suppress evidence because police exceeded the scope of the private-search doctrine by searching through files that the private searcher had not already viewed).

30 *See* Riley v. California, 134 S. Ct. 2473, 2488–89 (2014) (holding that, as a result of the vast storage capabilities of electronic-storage devices, personal-privacy interests outweigh government interests when determining whether police have violated the Fourth Amendment).

31 *See infra* Section I.C.

32 *See infra* Section III.B.

33 *See infra* Subsection I.C.1.b.

34 *See infra* Sections III.A-B.

35 *See infra* Subsection I.C.3. *See also infra* Section II.B.

not even within the Supreme Court's imagination at the private-search doctrine's inception,[36] and has already changed dramatically since the Fifth and Seventh Circuits adopted the physical-device approach.[37] Therefore, this proposal offers a new, forward-looking basis on which the Supreme Court can protect the constitutional right to privacy by taking into account modern-day technological implications.[38]

Part I of this Note discusses the development of Fourth Amendment jurisprudence regarding the private-search doctrine, tracing its origin in *Jacobsen* to its application in *Lichtenberger*.[39] Part II examines various applications of the private-search doctrine with an emphasis on the context of electronic-storage devices.[40] Finally, Part III calls for the Supreme Court to resolve the circuit split by reviewing the private-search doctrine and declaring the virtual-file test to be the proper scope.[41]

I. THE PRIVATE-SEARCH DOCTRINE: LEGAL CONSEQUENCES

At the heart of search-and-seizure law lies the Fourth Amendment to the United States Constitution.[42] Based on this Constitutional foundation, the private-search doctrine took its roots in, and has evolved through, case law.[43] Understanding the doctrine's big-picture Constitutional implications as well as its development over the past thirty years is essential to grasp the consequences of the circuit split.[44]

A. The Fourth Amendment as a Starting Point

To garner a clear understanding of the implications of the

---

36 *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984). (creating the private-search doctrine, explaining that a private search frustrates an individual's expectation of privacy).

37 *See* Rann v. Atchison, 689 F.3d 832, 838 (7th Cir. 2012) (adopting the rule from *Runyan*); United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001) (holding that under the private-search doctrine police may view items that a private searcher has not already viewed if police are "substantially certain" as to what the items contain). For an explanation of the physical-device approach, *see infra* Subsection I.C.1.a.

38 *See infra* Part III.

39 *See infra* Section I.B.

40 *See infra* Part II.

41 *See infra* Part III.

42 *See infra* Section I.A.

43 *See infra* Section I.B.

44 *See infra* Sections I.A-C.

private-search doctrine, it is necessary to first understand the Fourth Amendment as it applies to government searches of private citizens' property. Under the Fourth Amendment,

> The right of the people to be secure in their persons, houses, papers, and effects, *against unreasonable searches and seizures*, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[45]

The Fourth Amendment's prohibition of "unreasonable" searches and seizures embodies two sometimes-conflicting values: privacy and security.[46] In recognition of this goal and the necessary balance between privacy and security, Supreme Court jurisprudence has identified two sets of law enforcement conduct: methods of investigation that the Fourth Amendment regulates, and methods that the Fourth Amendment does not regulate.[47] As a consequence, the Fourth Amendment requires the government to obtain a warrant to search particular pieces of property and places, whereas the government is free to survey other areas—mainly places open to the public eye—without interference.[48] Traditionally, law enforcement has relied on a juxtaposition of these two categories when investigating criminals.[49] As a starting point, police survey areas not regulated by the Fourth Amendment

---

45 U.S. CONST. amend. IV (emphasis added).

46 *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 574 (2009) (discussing that the prohibition on unreasonable searches is "premised on a balance between privacy and security").

47 *See id.* (discussing "two basic categories" of law enforcement conduct created by the Supreme Court).

48 *See id.*

> [T]he Fourth Amendment protects a person's home and private packages. If the government wants access to those places, it must ordinarily have a search warrant. On the other hand, occurrences in public or on open fields are not protected by the Fourth Amendment. If the government wants to monitor such places, the Fourth Amendment does not interfere: The monitoring is not a search or seizure.

Id. (citing Payton v. New York, 445 U.S. 573, 585 (1980); California v. Ciraolo, 476 U.S. 207, 213 (1986)).

49 *See* Kerr, *supra* note 46, at 574 ("From an investigative standpoint, the two categories work together.").

in hopes of discovering behavior or other information indicative of criminal activity.[50] Then, if such surveillance proves fruitful, the evidence obtained may warrant further investigation.[51]

In general, determining whether a search violates the Fourth Amendment will turn on reasonableness.[52] Fourth Amendment jurisprudence has established that a search generally requires a warrant in order to be deemed reasonable.[53] However, the Supreme Court has also established a number of circumstances under which warrantless searches do not violate the Fourth Amendment.[54] First, a warrantless search may be upheld under the Fourth Amendment if it falls under a particular set of circumstances that render the search reasonable.[55] Such circumstances include "[w]hen [police are] faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like."[56] Second, police must also execute a

---

50 *See id.* at 575 (discussing the investigation process that police follow).

51 *Id.* ("If the evidence is strong enough, it can support invasions of protected spaces with a warrant.").

52 *See* Riley v. California, 134 S. Ct. 2473, 2482 (2014) ("As the text [of the Fourth Amendment] makes clear, 'the ultimate touchstone of the Fourth Amendment is 'reasonableness.'") (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)). *See also* Maryland v. King, 133 S. Ct. 1958, 1969 (2013) ("[T]he ultimate measure of the constitutionality of a governmental search is 'reasonableness.'") (quoting Veronia School District 47J v. Acton, 515 U.S. 646, 652 (1995)).

53 *See Riley*, 134 S. Ct. at 2482 ("Where a search is undertaken by law enforcement officials to discover evidence . . . reasonableness generally requires the obtaining of a judicial warrant.") (quoting *Veronia School District 47J*, 515 U.S. at 653).

54 *See King*, 133 S. Ct. at 1969 (listing such circumstances). The Court points out that "the Fourth Amendment's proper function is to constrain, not against all intrusions as such, but against intrusions which are not justified in the circumstances, or which are made in an improper manner." *Id.* (quoting Schmerber v. California, 384 U.S. 757, 768 (1966)). *See also Riley*, 134 S. Ct. at 2483 (discussing the incident-to-arrest doctrine).

55 *See King*, 133 S. Ct. at 1969 ("[T]he ultimate measure of the constitutionality of a governmental search is 'reasonableness.'"). Importantly, such reasonableness typically involves "some quantum of individualized suspicion." *Id.* (quoting United States v. Martinez-Fuerte, 428 U.S. 543, 560–61 (1976)). *See also* Riley, 134 S. Ct. at 2482–83 (explaining that certain exceptions to the warrant requirement exist).

56 *See King*, 133 S. Ct. at 1969.

> Those circumstances diminish the need for a warrant, either because the public interest is such that neither a warrant nor probable cause is required, or because an individual is already on notice, for instance because of his employment, or the conditions of his release from government custody, that some reasonable police intrusion on his privacy is to be expected. The

warrantless search properly in order for it to be upheld under the Fourth Amendment.[57] To determine whether a warrantless search has been executed properly, courts balance privacy against governmental interests.[58]

In a "world with no advanced technology," the Fourth Amendment requirements police must follow typically enable police to gather evidence sufficient to successfully prosecute criminals because "traditional crimes" are often committed at least partly in public.[59] However, paralleling Professor Kerr's discussion regarding the third-party doctrine, cyber-based crimes eschew this traditional model.[60] Wrongdoers who commit cyber-based crimes using laptops, cell-phones, and related devices are not vulnerable

---

> need for a warrant is perhaps least when the search involves no discretion that could properly be limited by the interpolation of a neutral magistrate between the citizen and the law enforcement officer.

Id. (internal citations omitted). For examples of such circumstances, *see* Maryland v. Buie, 494 U.S. 325, 330–31 (1990) (explaining that public interest outweighs the warrant requirement); National Treasury Employees Union v. Von Raab, 489 U.S. 656, 667 (1989) (explaining the lowest threshold of the warrant requirement exists when there is no need for discretion by a "neutral magistrate"). *See also Riley*, 134 S. Ct. at 2483 (explaining that searches incident to arrest without a warrant are reasonable); Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (police may not require a warrant to "render emergency assistance to an injured occupant or to protect an occupant from imminent injury").

57 *See King*, 133 S. Ct. at 1970 ("Urgent government interests are not a license for indiscriminate police behavior.").

58 *Id.* (explaining that the court weighs "the promotion of legitimate governmental interests" against "the degree to which [the search] intrudes upon an individual's privacy") (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

59 *See* Kerr, *supra* note 46, at 574–75.

> The public component of most traditional crimes is critical to the traditional balance of Fourth Amendment rules. . . . Because the police normally begin an investigation with only speculation that a particular person is a lawbreaker, the public portion of crimes give the police an opportunity to develop more evidence.

Id. at 575.

60 *See id.* at 575 ("[T]hird parties act as remote agents that permit wrongdoers to commit crimes entirely in private."). Comparing Professor Kerr's analysis of the issues related to the Third-Party Doctrine to the Private-Search Doctrine, individuals who commit crimes on computers may do so in private. *See id.* However, this comparison is not entirely sound. Professor Kerr points out that "[w]ithout the third party, the wrongdoer would have needed to go out into public spaces" to commit the crime. *Id.* However, that does not hold true when it comes to the issues discussed in this Note: specifically, individuals who commit crimes in cyberspace are typically not out in public for police to freely investigate. *See id.* at 574 (explaining how police may only conduct surveillance without a warrant when investigating public places).

to police investigation unregulated by the Fourth Amendment so long as they remain out of public areas and forums.[61] As a consequence, offenders who use the Internet as a primary platform for criminal activity may evade law enforcement.[62] In an attempt to flesh out the criminals who seek shelter in this haven inadvertently created by the Fourth Amendment, the Supreme Court created the private-search doctrine.[63]

Having served as an established exception to the warrant requirement for a little over three decades, the private-search doctrine has been applied in an array of different contexts.[64] The various applications and exceptions to the private-search doctrine, although sound in their respective functions, provide only dated guidance for digital searches in this technological age.[65] The evolution, rationale, and case law surrounding the private-search doctrine demonstrate the doctrine's need for the Supreme Court's clarification.[66]

B. The Establishment of and Rationale Behind the Private-Search Doctrine

The Supreme Court first articulated the private-search doctrine in *United States v. Jacobsen*.[67] As a threshold matter, the Fourth Amendment only applies to governmental action.[68] Consequently, the Fourth Amendment does not preclude a private individual from conducting a search or seizure, even if the search is unreasonable, so long as the private individual is not acting as a governmental agent or with the government's knowledge or participation.[69] Therefore, in the event that a private individual conducts a search against another private individual and discovers

---

61 *See id.* at 574–75 (explaining how the public nature of traditional crimes is essential to police investigation).

62 *See id.*

63 *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984) (creating the private-search doctrine and explaining that a private search frustrates an individual's expectation of privacy).

64 *See infra* Section I.B.

65 *See infra* Section I.C.

66 *See id.*

67 *Jacobsen*, 466 U.S. at 117.

68 *See id.* at 113 (explaining that the Fourth Amendment does not regulate private conduct).

69 *See id.* at 113–14 (explaining that the Fourth Amendment is "wholly inapplicable 'to a search or seizure . . . effected by a private individual'") (citing Walter v. United States, 447 U.S. 649, 662 (1980) (Blackman, J., dissenting)). For further discussion on this limitation, *see infra* note 122 and accompanying text.

incriminating information, the searcher is within his or her full legal right to turn that information over to the government.[70] Founded on this idea, the private-search doctrine states that if a private individual decides to turn over such information to the government, then the Fourth Amendment does not prohibit the government from using that information.[71]

Although *Jacobsen* went to great pains to highlight the point that the Fourth Amendment does not apply to private searches,[72] subsequent jurisprudence has placed important limitations on the application of the private-search doctrine.[73] First, the government's search *following* a private search may not exceed the scope of the initial private search.[74] As a means of gauging the reasonableness of the government's follow-up search in relation to the initial private search, the Court installed the virtual-certainty requirement.[75] This requirement dictates that the government, in conducting a search following an initial private search, must have "virtual certainty" that the search will reveal nothing more than what the initial private searcher has already revealed.[76] Second,

---

70 *See Jacobsen*, 466 U.S. at 113–14.

71 *See id.* at 117–18. The Court's rationale for the private-search doctrine is one of practicality:

> It is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit government use of that information. *Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information*.

Id. (emphasis added). This notion holds true "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in a third party will not be betrayed." *Id.* at 117 (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

72 *Jacobsen*, 466 U.S. at 113–14 (explaining that the Fourth Amendment does not regulate private conduct).

73 *See id.* at 117–20.

74 *See id.* at 117 ("The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated."). Furthermore, "*Jacobsen* directs courts to inquire whether the government learned something from the police search that it could not have learned from the private searcher's testimony and, if so, whether the defendant had a legitimate expectation of privacy in that information." United States v. Runyan, 275 F.3d 449, 461 (5th Cir. 2001) (citing *Jacobsen*, 466 U.S. at 118–20).

75 *See Jacobsen*, 466 U.S. at 119 (discussing that the police, in conducting their follow-up search, could determine the contents of defendant's package with "virtual certainty").

76 *See* United States v. D'Andrea, 648 F.3d 1, 9 (1st Cir. 2011) ("[T]he [*Jacobsen*] Court [emphasized] that an antecedent private search does not

the Court of Appeals for the Sixth Circuit has consistently held that the private-search doctrine does not apply to the private searches of residences.[77] Third, the Supreme Court has noted that a private party's violation of another person's expectation of privacy neither renders that expectation of privacy nonexistent nor deems the expectation unreasonable.[78] As a consequence, the private-search doctrine as articulated in *Jacobsen* essentially requires that a private party who conducts a search reveal the findings of that search to police before police may proceed with a follow-up search.[79] Over roughly three decades since *Jacobsen*, courts have addressed the private-search doctrine in various other, more nuanced applications.[80]

C. Relevant Commentary on Fourth Amendment Jurisprudence and the Private-Search Doctrine

The courts have provided ample Fourth Amendment and private-search-doctrine jurisprudence.[81] With that having been said, several noteworthy legal commentators have also addressed private searches in an attempt to understand the issues and

---

amount to a free pass for the government to rummage through a person's effects.").

77 *See* United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997) (declining to extend *Jacobsen* to the private searches of residences). The court reasoned that the defendant "had a . . . significant privacy interest in the contents of his [residence] . . . and this privacy interest was not breached in its entirety merely because [a private individual] . . . viewed some of [the room's] . . . contents." *Id.* The court distinguished this case from *Jacobsen*, reasoning that where *Jacobsen* involved a mail package, *Allen* involved a motel room. *Id.* The Sixth Circuit reaffirmed this holding over a decade later in United States v. Spicer, 432 F. App'x 522, 524 (6th Cir. 2011) ("[W]e decline to stretch the private-search doctrine to residential searches, including police searches of hotel rooms.").

78 *See* Walter v. United States, 447 U.S. 649, 658 n.12 (1980) (explaining that petitioners' expectation of privacy was not "undone" by a private search, because "it is difficult to understand how petitioners' subjective expectation of privacy could have been altered in any way by subsequent events of which they were obviously unaware."). *See also Jacobsen*, 466 U.S. at 132 (White, J., concurring) ("As Justice Stevens has previously observed . . . a person's expectation of privacy cannot be altered by subsequent events of which he was unaware.") (citing *Walter*, 447 U.S. at 659 n.12).

79 *See Jacobsen*, 466 U.S. at 117 ("[The] standard follows from the analysis applicable when private parties reveal other kinds of private information to the authorities."). *See also* United States v. Oliver, 630 F.3d 397, 417 (5th Cir. 2011) (Garza, J., dissenting) (explaining that *Jacobsen* requires "a private individual sharing information with police.").

80 *See* United States v. Lichtenberger, 786 F.3d 478, 488–91 (6th Cir. 2015).

81 *See supra* Section I.B.

provide any potential solutions.[82] To adequately capture the implications necessary to understand an analysis of the private-search doctrine, these authors' commentaries and arguments regarding parallel issues must come into the fore.[83]

1. Accessing Digital Evidence and the Scope of the Search

The application of the Fourth Amendment within the realm of digital evidence is most relevant to this circuit split.[84] While searches of persons, homes, and packages have always had their place in search-and-seizure law,[85] the advent of the digital age and the relatively recent, exponential increase in the use of computers has opened the door to a new Fourth Amendment application: computer hard drives and related electronic-storage devices.[86] Professor Kerr presents four distinguishing factors inherent in digital evidence: (1) There are various forms of digital evidence;[87] (2) Searches of digital evidence usually take place on government property as opposed to a suspect's property;[88] (3) Electronic-storage devices have a vast storage capacity;[89] and (4) Searches of electronic devices take much longer than searching physical

---

82 *See* Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 537 (2005). *See also* Brian L. Williams, *Criminal Constitutional Law—An Attack on Fourth Amendment Protection: Security Guards and the "Private" Search Doctrine*, 18 WM. MITCHELL L. REV. 175, 178 (1991).

83 *Id.*; Kerr, *supra* note 82, at 537.

84 *See id.*

85 *See, e.g.*, United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997) (declining to extend *Jacobsen* to the private searches of residences).

86 *See* Kerr, *supra* note 82, at 537 ("The dynamics of computer searches turn out to be substantially different from the dynamics of home searches."). For a discussion of "computer forensics" and how data retrieval works, *see id.* at 537–38.

87 *See id.* at 538. Examples of these various forms include "hard drives, floppy disks, thumb drives, and Zip disks." *Id.* (citing JIM KEOGH, THE ESSENTIAL GUIDE TO COMPUTER HARDWARE 140 (2002)). "While houses are divided into rooms, computers are more like virtual warehouses. . . . The differences between homes and computers prompt an important question: what does it mean to 'search' a computer storage device?" *See* Kerr, *supra* note 82,. at 539–40.

88 *See id.* at 541 (distinguishing between private property and bitstream copies).

89 *See id.* at 541–42 ("Computers can only store data, but the amount of data is staggering."). Professor Kerr also highlights that "computer storage capacities tend to double about every two years." *Id.* at 542. Importantly, "[c]omputers are also remarkable for storing a tremendous amount of information that most users do not know about and cannot control." *Id.*

evidence.[90]

As a result of these differences, it is more difficult to plan searches of digital evidence in advance than for searches of physical evidence.[91] The impact of these differences all play an important role in applying the Fourth Amendment to searches of digital evidence.[92]

As a threshold matter, a collection of case law has firmly resolved that the expectation of privacy granted to private citizens with respect to homes and packages also extends to electronic-storage devices.[93] Against this backdrop, accessing the data contained within electronic-storage devices constitutes a "search" for purposes of the Fourth Amendment.[94] To determine when an individual has "accessed the data," Professor Kerr advocates for an "exposure-based approach," which holds that data is deemed accessed when it is exposed to the human eye, such as an individual viewing it on a computer-screen.[95]

---

90 *See id.* at 544 ("Computer searches tend to require fewer people but more time.").

91 *See* Kerr, *supra* note 82, at 547 (explaining that "it is more difficult to plan a computer search *ex ante*").

92 *Id.* ("The question is, should these dynamics impact the rules that courts use to review the scope of computer searches—and if so, how?").

93 *See id.* at 549 ("A suspect's hard drive is his private property, much like other sealed containers, and the same rules should apply."). *See also* United States v. Runyan, 275 F.3d 449, 458 (5th Cir. 2001) (discussing the reasonable expectation of privacy in computer disks); United States v. Reyes, 922 F. Supp. 818, 832–33 (S.D.N.Y. 1996) (reasonable expectation of privacy in data stored in a digital pager); United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995) (discussing the same); United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (discussing the same); United States v. Blas, No. 90-CR-162, 1990 WL 265179, at *56 (E.D. Wis. Dec. 4, 1990) ("[A]n individual has the same expectation of privacy in a pager, computer or other electronic data storage and retrieval device as in a closed container."). Professor Kerr also points out that "[i]n most circuits . . . the fact that the Fourth Amendment applies equally to computer storage devices has been implicit in decisions that focused on other questions." *See* Kerr, *supra* note 82, at 549 n.79 (citing United States v. Carey, 172 F.3d 1268, 1273–76 (10th Cir. 1999) (plain view and warrant case); United States v. Upham, 168 F.3d 532, 536–37 (1st Cir. 1999) (warrant case)).

94 *See* Kerr, *supra* note 82, at 550 ("In general, an investigator who sees a suspect's computer and starts looking through files is conducting a Fourth Amendment search.").

95 *Id.* at 551 (explaining that data is accessed when "exposed to possible human observation, such as when it appears on a screen"). This approach is ideal because it "reinforces the traditional Fourth Amendment concern with limiting the scope of searches. Defining searches in terms of data exposure provides a simple and intuitive yardstick for measuring the scope of a search." *Id.* at 552. Additionally, "[i]t is far easier for humans to control and understand exposure than to control and understand the technical functioning of a computer." *Id.*

Given the point at which data is considered accessed, courts have applied different approaches in determining the scope of a search of an electronic-storage device.[96] Among those approaches are the physical-box test, virtual-file test, and exposed-data test.[97] The applicable approach in a given case is of utmost importance because police who exceed the scope of the initial private search generally cannot rely on evidence found to prosecute wrongdoers, no matter how heinous the evidence.[98]

a. Physical Box

The physical-box approach[99] defines the unit of a search of an electronic-storage device in terms of the device itself.[100] For purposes of the private-search doctrine, this approach would allow police to search an entire device after a private party searches any files or folders within the device and reveals any incriminating contents to police.[101] For example, in *United States v. Runyan*,[102] the Fifth Circuit held that a private searcher who opened only a few files on a computer had effectively searched the entire hard drive.[103] As a consequence, it was irrelevant that police opened storage files different than those the original private searcher had opened because the scope of the search was defined in terms of the physical device itself.[104]

---

96 *See id.* at 554 ("The zone of a search determines the extent to which a particular search in a space eliminates privacy protection elsewhere in that space.").

97 *See id.*

98 *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984) (explaining that police exceed the scope of the private-search doctrine when police "use information with respect to which the expectation of privacy has not already been frustrated.").

99 Kerr, *supra* note 82, at 554–55.

100 *Id.*

101 *See id.* at 555 (explaining the legal application of the physical-device approach).

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

103 *Id.* at 464–65. "There was no record of what specific files the wife (private searcher) had observed, but the Fifth Circuit concluded it did not matter: having legally accessed a few files under the private search doctrine, she had 'searched' the entirety of the disks." *See* Kerr, *supra* note 82, at 555 (discussing the *Runyan* decision) (citing *Runyan*, 275 F.3d at 464–65).

104 *Runyan*, 275 F.3d at 464–65. *See also, e.g.*, United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002) (applying the physical-device test, police did not exceed the scope of the private-search doctrine even though they searched items that the private searcher had not searched); Kerr, *supra* note 82, at 555 n.107. Professor Kerr provides a succinct overview of how applying the physical-device

b. Virtual File

The virtual-file approach essentially states that the scope of a search of an electronic-storage device is defined in terms of each specific, individual file.[105] Under this approach, police exceed the scope of the private-search doctrine by opening or viewing individual files that an initial private searcher had not already opened and revealed to police.[106] In *United States v. Lichtenberger*,[107] the court provides an excellent illustration of how the virtual-file approach can impact the reasonableness of police's application of the private-search doctrine.[108] The Sixth Circuit held in *Lichtenberger* that police exceeded the scope of the private-search doctrine because they had no virtual certainty that the files they viewed on the laptop contained incriminating evidence, or were the same files the initial private searcher had viewed.[109]

---

approach may influence the constitutional and related legal implications in the police's follow-up search:

> An analogous issue was addressed but not resolved by the Supreme Court in *Walter v. United States*, 447 U.S. 649 (1980). In *Walter*, boxes containing reels of obscene films were sent to the wrong address. The recipients at the wrong address opened the boxes, noted that the labels were pornographic, and attempted to view portions of the film by holding it up to the light. They then contacted the FBI, and the FBI viewed the entire film on a projector. The question before the Court was whether by viewing part of the film, the recipients had "searched" the entire film. No majority view emerged. Four Justices said yes, modeling the film as a physical box, *see id.* at 663 (Blackmun J., dissenting); two Justices said no, modeling the film as the information it contained, *see id.* at 659 (Stevens, J., announcing the judgment of the Court); and three Justices either did not resolve the case on that ground, *see id.* at 660 (White, J., concurring in the judgment), or did not explain their rationale, *see id.* (Marshall, J., concurring in the judgment).

Kerr, *supra* note 82, at 555 n.107. *See further* Rann v. Atchison, 689 F.3d 832 (7th Cir. 2012). The physical-device approach was applied in a slightly different manner in this case. *Id.* at 837–38 (in *Rann*, the court held that a memory card and a zip drive an initial private searcher gave to police were admissible evidence because the private searcher knew the precise contents of the devices before handing them over to police).

105 *See* Kerr, *supra* note 82, at 554–55 (discussing the virtual-file approach).

106 *See id.* at 555.

107 United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015).

108 *Id.* at 488.

109 *Id.* at 489 ("The same folders—labeled with numbers, not words—could have contained [non-incriminating evidence]."). *Compare with* Runyan, 275 F.3d

c. Exposed Data

The exposed-data approach defines the scope of the search in terms of "whatever information appears on the output device," such as a computer or cell-phone screen.[110] There is little case law displaying the effects of this approach because most cases involving this issue revolve around child pornography, in which case the illegal image is "both the file and the contents of the exposed data."[111] In application, this approach would allow an officer to search the entire contents of a 100-page document that is open on a desktop, even if the private party had only searched a few pages.[112]

These three different approaches provide sturdy background for the importance of harmonizing the scope of the private-search doctrine.[113] However, the scope of the follow-up search is meaningless if the initial searcher acts with the knowledge or

---

at 464–65 (contrasting *Lichtenberger* with the result and reasoning in *Runyan*: had the Sixth Circuit applied the physical-device test, police could not have been deemed to exceed the scope of the private-search). For this reason and others, Professor Kerr strongly prefers the virtual-file approach over the physical-device approach. *See* Kerr, *supra* note 82, at 556 ("When assessing how the Fourth Amendment applies to the collection of information, courts should focus on that information rather than the physical storage device that happens to contain it. Using the physical box . . . would also lead to unpredictable, unstable, and even disturbing results.").

110 *See* Kerr, *supra* note 82, at 556 (discussing the difference between the expose-data test and the virtual-file test).

111 *See id.*

112 *See id.* at 557. While the differences between the virtual-file approach and the exposed-data approach seem subtle—if not non-existent—Professor Kerr highlights their key differences:

> First, much information stored on a computer does not appear in a file. If the law is keyed to files, how can it apply to information not stored in a file? Second, this approach fits nicely with the exposure-based approach to searches. Once again, what matters is exposure to human observation. Third, virtual-files are not robust concepts. Files are contingent creations assembled by operating systems and software. Fourth, an analyst who takes a mouse, clicks, and pulls down the file to see parts of the file not previously exposed has done nothing different from another analyst who double clicks on a second file to open it. In both cases, the analysts are exposing information not previously exposed. Both actions should be treated as searches.

See id.

113 *See supra* Subsections II.C.1.a–c.

participation of the government.[114] As such, it is important to determine when the government has played too large a role in the initial private search.[115]

2. Distinguishing Private Action from Government Action

Although the Fourth Amendment does not prohibit private searches, a search will not evade Fourth Amendment scrutiny simply because it is conducted by a private party.[116] If a private party conducts a search while acting as an instrument or agent of the government, then the Fourth Amendment along with all of its limitations on unreasonable searches and seizures will apply.[117] It is up to a trial court to make a factual determination as to whether a private actor served as an agent of the government.[118] Originally, courts had one of two tests to apply when making this factual determination: the critical-factors test and the government-instigation test.[119] However, private-search jurisprudence suggests the tests have merged over time into one test comprising several factors.[120]

---

114 *See* United States v. Jacobsen, 466 U.S. 109, 113–14 (1984) (explaining that in order for the Fourth Amendment to not apply to private conduct, the private searcher must not be acting as an agent of the government).

115 *See infra* Subsection I.C.2.

116 *See Jacobsen*, 466 U.S. at 113 (finding no Fourth Amendment violation because of the private nature of the searcher).

117 *See* Williams, *supra* note 82, at 178. *See also* Skinner v. Ry. Labor Exec.'s Ass'n, 489 U.S. 602, 615–16 (1989) (reasoning that because government removed legal barriers to employee drug testing and encouraged and participated in testing, Fourth Amendment is implicated); Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (reasoning that because murder suspect's wife did not act as instrument or agent of government when she voluntarily provided police officers with incriminating evidence, Fourth Amendment is not implicated).

118 *See* Williams, *supra* note 82, at 178 ("Whether a private search is transformed into government action is a factual determination which belongs to the trial court.") (citing Minnesota v. Buswell, 460 N.W.2d 614, 618 (Minn. 1990), *reh'g denied*, (Minn. Oct. 8, 1990), *cert. denied*, 111 S. Ct. 1107 (1991)). *See also* United States v. D'Andrea, 648 F.3d 1, 10 (1st Cir. 2011) (remanding the case to the trial court to determine, using the critical-factors test, whether the searcher was a government agent); United States v. Koenig, 856 F.2d 843, 849 (7th Cir. 1988) (holding that trial court's finding that private mail carrier examined packages for its own reasons was not clearly erroneous). "Moreover, such factual determinations will be reversed only if clearly erroneous." *Buswell*, 460 N.W.2d at 618–19.

119 *See* Williams, *supra* note 82, at 178–79 (explaining two tests to determine government intervention).

120 *See* cases cited *infra* note 122.

First articulated in *United States v. Walther*,[121] the most current form of the critical-factors test includes three relevant factors for distinguishing private and government action for purposes of the Fourth Amendment: (1) the government's role in the search; (2) the government's intent in conjunction with its control over the search and the searcher; and (3) the private party's objective in conducting the search.[122] However, despite these factors, the mere fact that a government may have a particular interest in the outcome of a search is not enough to implicate the Fourth Amendment.[123]

Unpacking the critical-factors test, courts have a series of standards to apply in analyzing each factor. First, in determining the government's role in the search, courts determine whether the government ordered the search, requested the private party to conduct the search, or jointly participated in the search.[124] Second,

---

121 United States v. Walther, 652 F.2d 788 (9th Cir. 1981).

122 *See D'Andrea*, 648 F.3d at 10 (quoting United States v. Momoh, 427 F.3d 137, 140–41 (1st Cir. 2005)). Other circuit courts also apply the critical-factors test. *See, e.g.*, United States v. Pierce, 893 F.2d 669, 673–74 (5th Cir. 1990), *reh'g denied*, 897 F.2d 528 (5th Cir.1990) (holding that airline employees failed to demonstrate intent to assist law enforcement efforts when they opened "suspicious" package which contained drugs); Pleasant v. Lovell, 876 F.2d 787, 798 (10th Cir. 1989) (holding that IRS special agents knew of and acquiesced in the conduct of private actor who provided them documents for investigative purposes); United States v. Feffer, 831 F.2d 734, 740 (7th Cir. 1987) (holding that actor's seizure of company documents for IRS agents failed to demonstrate intent to assist law enforcement officials); United States v. Miller, 688 F.2d 652, 661–62 (9th Cir. 1982) (holding that the private party was not acting as an agent of the government after being the victim of theft and going to defendant's property to look for the stolen property); United States v. Smythe, 84 F.3d 1240, 1243 (10th Cir. 1996) ("While government agents may not circumvent the Fourth Amendment by acting through private citizens, they need not discourage private citizens from doing that which is not unlawful."); United States v. McAllister, 18 F.3d 1412, 1418 (7th Cir. 1994) (holding that a confidential informant did not have requisite intent to be considered a government agent because "the record is clear that the informant acted completely on his own initiative"); United States v. Malbrough, 922 F.2d 458, 460–63 (8th Cir. 1990) (concluding that the private party, a burglary suspect enlisted by police to assist in narcotics purchases, was not government agent when he trespassed on defendant's property, looked through open doors of greenhouse, and observed marijuana plants).

123 *See* United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009) ("We will not find state action simply because the government has a stake in the outcome of a search.").

124 *See, e.g.*, Lustig v. United States, 338 U.S. 74, 79 (1949) (holding that government participation in search was established when official "was in it before the object of the search was completely accomplished"), *overruled in part on other grounds*, Elkins v. United States, 364 U.S. 206 (1960); United States v. Knoll, 16 F.3d 1313, 1320 (2d Cir. 1994) (noting that the district court failed to recognize that prosecutor may have "directed . . . and tacitly approved" unlawful private

in determining the government's intent,[125] courts generally require government "knowledge of the illegal search coupled with a failure to protect the petitioner's rights against such a search."[126] Third, in determining the private searcher's intent, courts analyze whether the private party has some "legitimate independent motivation" apart from a successful prosecution of the suspect.[127]

Evidently, there is a thorough record of jurisprudence regarding the private-search doctrine.[128] However, case law and legislation with respect to private searches are inadequate within the realm of modern-day electronic-storage devices.[129] Today's ever-evolving technology has outpaced the search-and-seizure doctrine, leaving a gaping opportunity for unconstitutional violations of privacy.[130]

3. The Doctrine's Inability to Maintain Pace with Technology

Since *Jacobsen* in 1984, technology has vastly evolved not only with regard to types of devices but also their storage capabilities.[131]

---

search when he asked private party to provide more specific evidence from documents that were burglarized).

125 "Intent" may include mere "knowledge or acquiescence." *See* Momoh, 427 F.3d at 140–41.

126 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.8(b), at 225 (3d ed. 1996). Professor LaFave asserts that the "'failure to protect the petitioner's rights'" has been interpreted to mean that police failed to instruct the private searcher not to carry out the search or to take steps to prevent the search after acquiring knowledge of the private search. *Id.* at 225–26 (citation omitted). Although there is no blanketed rule that police are required to deter private parties from conducting searches, an illegal search may trigger a duty on the part of law enforcement to advise the private searcher as to the limits of the law. *See id.*

127 United States v. Ellyson, 326 F.3d 522, 528 (4th Cir. 2003) (upholding the district court's conclusion that private party's "actions were not motivated by a desire to aid the police in building their case" but by a desire to preclude "law enforcement from holding her responsible for any items subsequently discovered in trailer.") (quoting trial record). *See also* McClelland v. McGrath, 31 F. Supp. 2d 616, 619 (N.D. Ill. 1998) (holding that the jury could reasonably find that the private party was acting as government agent because it "acted at the government's request," "the government knew of and agreed to [its] actions," and it "was motivated by its desire to help the officers rather than to protect its own property").

128 *See* Walter v. United States, 447 U.S. 649, 656–60 (1980); United States v. Jacobsen, 466 U.S. 109, 115–16 (1984); United States v. Runyan, 275 F.3d 449, 461–65 (2001).

129 *See infra* Subsection I.C.3.

130 *See id.*

131 *See generally* Laura Arredondo-Santisteban, *Stealing Glances: Electronic Communications Privacy and the Necessity for New Legislation in the Digital Age*,

For example, e-mail platforms, once capable of exchanging no more than text-only messages, now provide many gigabytes of free storage for messages, pictures, videos, and the like—all compiled in one monumental storage facility.[132] Even further beyond the imagination of the *Jacobsen* court, individuals can now access this colossal pool of data from virtually anywhere via their smartphones or tablets.[133] As of October 2015, "68% of U.S. adults have a smartphone . . . and . . . 45% [of] adults [own tablets] . . . [Eighty-six percent] of those aged 18-29 have a smartphone, as do 83% of those ages 30-49 and 87% of those living in households earning $75,000 and up annually."[134] Furthermore, smartphones and tablets come equipped with massive storage capabilities themselves, harboring a seemingly endless supply of text messages, videos, photos, and other personal files.[135]

The size and complexity of an electronic-storage device's memory banks are similarly staggering.[136] Digital storage is measured in terms of bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), and sometimes terabytes (TB).[137] A kilobyte is typically 1024 bytes, a megabyte 1024 kilobytes, and a gigabyte 1024 megabytes.[138] To make matters more complex, however, "measures of hard disk capacity often take [one megabyte] to be 1,000,000 bytes (not 1,024,768 bytes) and so on."[139] As a result, two devices that are labelled with the same storage capacity can actually have different storage capacities, leading to some debate among members of the computer industry.[140] Typically, word

14 N.C. J.L. & TECHNOLOGY ONLINE 205, 216, 222 (2013) (discussing how the evolution of technology has in many respects rendered current legislation covering electronic-communications privacy obsolete).

132 *See* Ian Peter, *The History of Email*, NETHISTORY, http://www.nethistory.info/History%20of%20the%20Internet/email.html (last visited Mar. 10, 2017).

133 *See* Kathryn Zickuhr & Aaron Smith, *Digital Differences*, PEW RESEARCH CTR. 2 (Apr. 13, 2012), http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_Digital_differences_041312.pdf.

134 Monica Anderson, *Technology Device Ownership: 2015*, PEW RESEARCH CTR. (Oct. 29, 2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

135 *See iPhone 6s*, APPLE, http://www.apple.com/iphone-6s/specs/ (last visited May 7, 2017) (one of Apple's most current iPhones holds up to 128 gigabytes of data).

136 *See* Christopher Barnatt, *Computer Storage*, EXPLAININGCOMPUTERS.COM, http://explainingcomputers.com/storage.html (last visited Mar. 10, 2017) (describing the sizes of different file types).

137 *Id.*

138 *Id.*

139 *Id.*

140 *Id.*

documents and spreadsheets consist of files ranging from a few hundred kilobytes to a few megabytes.[141] Image files on average comprise several megabytes, likely more if they are professionally done.[142] Much more significant are video files, which consume hundreds of megabytes if not a few gigabytes of storage.[143] Impressively, video files can be even larger depending on their type and quality: For example, "standard definition" will consume about two gigabytes per minute of footage whereas "high definition" will consume roughly over nine gigabytes per minute of footage.[144]

The hierarchy of file types is especially germane to external data-storage units, which have come a remarkably long way in a relatively short period of time since the antiquated floppy disk.[145] Furthermore, the variance among common data-storage units' respective capacities demonstrates the insignificance one file can have in light of an entire pool of data.[146] Compact disks—more commonly known as CDs—can hold up to roughly 700 megabytes.[147] DVDs come in multiple formats, ranging from a "standard capacity" of a little less than five gigabytes to a commercial version holding almost nine gigabytes.[148] The most recent installment in disk media, Blu-Ray, can hold up to twenty-five gigabytes on a single-layer disk and as many as fifty gigabytes on a dual-layer disk.[149] Today's most popular flash-memory cards, SD cards,[150] come in different storage capabilities ranging from two gigabytes up to as many as sixty-four gigabytes.[151] Similarly, USB-memory sticks—commonly referred to as "pen drives," "thumb drives," and "flash drives"—range from 512 megabytes to 256 gigabytes.[152] In sum, modern-day file types weave together with

---

141 *Id.*

142 Barnatt, *supra* note 136.

143 *Id.* ("For example, an hour of DV format video footage consumes about 12GB of storage.").

144 *Id.*

145 *See id.* (noting that "the last few years have seen the death of the floppy disk (with its 1.44MB capacity).").

146 *See id.*

147 *Id.*

148 Barnatt, *supra* note 136.

149 *Id.* The author also points out that "multi-hundred GB disks are already in the lab and on the consumer horizon." *Id.*

150 *See* Rann v. Atchison, 689 F.3d 832, 834 (7th Cir. 2012) (such a memory card was one of the data-storage units at issue).

151 *See* Barnatt, *supra* note 136. The author also mentions that, in theory, such memory cards could hold up to two terabytes of data; however, the highest currently available on the market only go up to sixty-four gigabytes. *Id.*

152 *Id.* The author points out that USB drives are the "dominant means of

smartphones, computers, and related external devices to form the incredibly complex web of data storage.[153]

Even more astonishing than electronic-storage devices' ownership rates and storage capability is their functionality and varied uses.[154] "[F]or a number of Americans, smartphones serve as an essential connection to the broader world of online information."[155] As of 2015, "30% of smartphone-dependent Americans say that they 'frequently' reach the maximum amount of data" allowed on their cellular plan, and "51% say that this happens to them at least occasionally."[156] On a related note, "62% . . . have used their phone[s] [to retrieve health information;] 57% have used their phones to conduct online banking; 44% have used their phones too look up real estate [or housing information]; 43% [have used their phones for a job search]; and 40% [have used their phones for] government services."[157] Additionally, "67% use their phone to share pictures, videos, or commentary about events happening in their community, with 35% doing so frequently."[158]

Perhaps the most flooring statistics are those representing users' sentiment toward their smartphones: "46% say [their smartphone is a device] they couldn't live without"; "70% [say their smartphone] represent[s] freedom"; and "72% [say the phone is] 'connecting' rather than 'distracting.'"[159] In a series of surveys conducted twice daily over a one-week period, the Pew Research Center developed a relatively clear picture of what daily smartphone use looks like for three separate age groups: 18–29; 30–49; and over 50.[160] As for the youngest age group: 100% texted; ninety-seven percent used the Internet; ninety-three percent engaged in voice/video calls; ninety-one percent used for e-mail;

---

removable, re-writable portable data storage" due in part to their "ever-increasing capacity." *Id.*

153 *See id.*

154 *See generally* Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RESEARCH CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/. This article places emphasis on smartphones, although the basic ideas may be extrapolated to relate to similar electronic-storage devices that are relevant to this Note. *See id.*

155 *Id.*

156 *Id.*

157 *Id.* "Smartphones are used for much more than calling, texting, or basic internet browsing. Users are turning to these mobile devices as they navigate a wide range of life events." *Id.*

158 Smith, *supra* note 154.

159 *Id.*

160 *Id.*

ninety-one percent used for SNS;[161] seventy-five percent used for videos; and sixty-four percent used for music.[162] As for the middle age group: ninety-eight percent texted; ninety percent used the Internet; ninety-one percent engaged in voice/video calls; eighty-seven percent used for e-mail; seventy-seven percent used for SNS; forty-six percent used for videos; and thirty-nine percent used for music.[163] Finally, as for the oldest age group: ninety-two percent texted; eighty percent used the Internet; ninety-four percent used for voice/video calls; eighty-seven percent used for e-mail; fifty-five percent used for SNS; thirty-one percent used for videos; and twenty-one percent used for music.[164]

American citizens' placing of so much personal and would-be private data into these devices that are interconnected by the Internet, and cellular networks, poses a unique opportunity for private individuals to assist law enforcement in the apprehension of cyber criminals.[165] In several cases, courts have admitted evidence obtained intrusively, and likely illegally, by private searches of alleged criminals' electronic-storage devices.[166] Due to the great ease with which individuals can hack into electronic-storage databases,[167] there is grave potential for private parties to carry out duties identical to those of law enforcement, all the while circumventing individuals' Fourth Amendment protections.[168]

---

161 "SNS" refers to "social networking service," such as Facebook or Twitter.

162 *See* Smith, *supra* note 154.

163 *Id.*

164 *Id.*

165 *See generally* Monica R. Shah, *The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace,* 105 COLUM. L. REV. 250, 250 (2005) (explaining how cyber criminals have illegally assisted law enforcement by hacking into private individuals' computers).

166 *See* United States v. Kline, No. 03-50349, slip op. at 5–6 (9th Cir. filed Oct. 4, 2004) (holding that hacker who collected inculpatory files through unauthorized access to defendant's computer was a private party not subject to Fourth Amendment constraints); United States v. Jarrett, 338 F.3d 339, 346–48 (4th Cir. 2003) (holding the same); United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003) (holding the same); United States v. Segal, 299 F. Supp. 2d 856, 861–63 (N.D. Ill. 2004) (admitting inculpatory evidence obtained through employee who hacked into company computer files).

167 *See* Neil Tweedie, *Just how easy is it to hack into your life?*, THE TELEGRAPH (June 25, 2011), http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/8597757/Just-how-easy-is-it-to-hack-into-your-life.html (discussing how "invading our lives [via electronic databases] couldn't be easier").

168 *See* Shah, *supra* note 165, at 252–53 ("[C]ourts thus far have declined to extend the definition of government agent to cover private parties who gather evidence about suspected criminals by illegally hacking into the suspects' computers."). Shah references several cases in support. *See* cases cited, *supra*

In an analogous argument, Attorney Monica Shah asserts that the private-search doctrine is no longer adequate for searches of Internet-connected devices because the critical-factors test does not address the "unique nature of Internet technology—namely the ability of one hacker to conduct anonymous, highly efficient searches of numerous computers connected to the Internet."[169] Importantly, Shah goes on to explain how this gap in the private-search doctrine raises special concern because, in effect, the doctrine not only allows but also "implicitly sanctions" such illegal searches.[170] Although Shah's argument focuses on a different scope than that of this Note, the common ground fleshes out the same principle: Given the monumental advances in technology since the inception of the private-search doctrine, the doctrine is no longer capable of adequately protecting suspects' Fourth Amendment rights against unreasonable searches.[171]

The hard drive of an electronic-storage device "is the digital equivalent of its owner's home, capable of holding a universe of private information."[172] In this light, the variability among courts in applying the private-search doctrine demonstrates the potential

---

note 166. Private searchers are only subject to Fourth Amendment scrutiny when acting as agents of the government. *See* Williams, *supra* note 117, and accompanying text. Therefore, an individual who illegally intrudes into another's electronic database could theoretically provide law enforcement with ill-gotten boons. *See id.* For a discussion of instances in which police not only incorporated but also relied upon the fruits of an illegal hacker, *see* Shah, *supra* note 165, at 262–66.

169 Shah, *supra* note 165, at 266.

170 *Id.* *See Steiger*, 318 F.3d at 1043–44 (discussing anonymous hacker's admission that his "trap," a Trojan horse program, caught at least 2,000 child pornographers); *Jarrett*, 338 F.3d at 341 ("When Steiger downloaded the picture to his own computer, he inadvertently downloaded the Trojan Horse program, which then permitted [the anonymous hacker] to enter Steiger's computer undetected via the Internet."). In these two cases, "[e]ven the FBI recognized the hacker's strength in acquiring evidence and considered him a 'valuable resource.'" *See* Shah, *supra* note 165, at 267–68 (quoting United States v. Jarrett, 229 F. Supp. 2d 503, 515 (E.D. Va. 2002)).

171 *See supra* INTRODUCTION.

172 United States v. Mitchell, 565 F.3d 1347, 1352 (11th Cir. 2009) (quoting Kan. v. Rupnick, 280 Kan. 720, 735–36 (2005)). The *Rupnick* court's logic lent great support to this assertion:

> [A] computer is not truly analogous to a simple . . . container or . . . file cabinet, even a locked one. . . . Further, a computer's outward appearance . . . tells the observer nothing about the content or character of the information or potential evidence contained on its hard drive.

Rupnick, 280 Kan. at 735–36.

for violations of private citizens' Fourth Amendment rights.[173] Upon analyzing the variations within private-search-doctrine case law, it becomes apparent that the scope of the private-search doctrine needs to be refined in order to ensure the doctrine's viability in an increasingly-digital world.[174]

II. THE PRIVATE-SEARCH DOCTRINE IN APPLICATION: A CIRCUIT SPLIT

The courts' analyses within the cases foundational to the private-search doctrine provide an overview of the substantive law that helps to explain the doctrine as it stands today.[175] However, focusing on each critical case's scope of the follow-up search is paramount to understanding the variances among courts in applying the private-search doctrine.[176] Different circuits' adoption of different scopes in factually similar cases has given rise to a circuit split regarding the scope of the government's follow-up search.[177] In so doing, the circuit courts have demonstrated how applying a different scope can very much dictate the outcome of the case.[178]

A. Fifth and Seventh Circuits

In *United States v. Runyan*,[179] the Fifth Circuit addressed the scope of the government's follow-up search from three different perspectives, two of which are relevant to this Note.[180] First, the

---

173 *See infra* Sections II.A–C.

174 *Id.*

175 *See supra* Part I.

176 *See infra* Sections II.A–C.

177 *See infra* Sections II.A–B.

178 *See id.*

179 United States v. Runyan, 275 F.3d 449 (5th Cir. 2001). A private party discovered child pornography after searching the defendant's property. *Id.* at 453. The pornography was contained within twenty-two CDs, ten ZIP disks, and eleven floppy disks, all of which were turned over to a police deputy. *Id.* The private searcher only viewed "approximately twenty" of the twenty-two CDs and eleven floppy disks and did not view any of the ten ZIP disks before turning them over to police. *Id.* Law enforcement viewed all of the contents that had been handed over to them. *Id.* at 454. After being charged for child pornography, the defendant argued that the evidence found by the private party and handed over to police should be suppressed because it violated his Fourth Amendment rights. *Id.* at 455.

180 *Runyan*, 275 F.3d at 461–62.

> Today, we address . . . narrow questions: (1) whether a police

court found that police exceed the scope of the initial private search if police open a closed container not originally opened by the private party unless police have substantial certainty as to what is inside that container.[181] Second, the court found that police do not exceed the scope of the initial private search by examining "more items within a closed container" than the private searchers.[182] Within the context of *Runyan*, the "container" was an electronic-storage device similar to a CD, floppy disk, or ZIP drive, whereas "more items within a closed container" pertained to specific files within such storage devices.[183]

Adopting the *Runyan* court's rule in *Rann v. Atchison*,[184] the Seventh Circuit held that police do not exceed the scope of the follow-up search by viewing the contents of a digital-media device

---

> search exceeds the scope of the private search when private searchers examine selected items from a collection of similar closed containers and police searchers subsequently examine the entire collection; (2) whether a police search exceeds the scope of the private search when the police examine more items within a particular container than did the private searchers.

Id.

181 *Id.* at 463. Police may derive substantial certainty from "statements of the private searchers, their replication of the private search, and their expertise." *Id.* The court reasoned that a private search may "render[] obvious" the contents of a container, therefore frustrating the defendant's expectation of privacy with respect to the whole container. *Id.* at 463–64.

182 *Id.* at 464 ("[P]olice do not exceed the scope of a prior private search when they examine the same materials that were examined by the private searchers, but they examine these materials more thoroughly than did the private parties."). The court reasoned that "an individual's expectation of privacy in the contents of a container has already been compromised if that container was opened and examined by private searchers." *Id.* (citing United States v. Jacobsen, 466 U.S. 109, 119 (1984)).

183 *Id.* at 453–54 (discussing the devices that were the subject of litigation).

184 Rann v. Atchison, 689 F.3d 832, 833 (7th Cir. 2012). The defendant's biological daughter reported to police that the defendant took pornographic pictures of her when she was a minor. *Id.* at 834. The victim delivered to police a memory card containing images of the defendant sexually assaulting her. *Id.* The victim's mother also delivered to police a ZIP drive containing additional pornographic images of the same victim and an additional underage victim, the defendant's stepdaughter. *Id.* The record contained no evidence that police were present when the victim and mother procured the drives, nor is there evidence that police knew of or encouraged the searches. *Id.* On this evidence, the defendant was convicted of possession of child pornography. *Id.* at 833. On appeal, the defendant argued he had ineffective counsel because his attorney did not move to suppress the evidence given to police by the victim and her mother. *Rann*, 689 F.3d at 833. After losing on appeal, the defendant petitioned for a writ of habeas corpus. *Id.* Although the district court denied the writ, they allowed the defendant to bring this appeal. *Id.*

given to them by a private party.[185] This holding is significant because there was no record to indicate to police the scope of the initial private search.[186] Furthermore, the court reasoned that even if police had "more thoroughly searched" the storage devices, they still could not be deemed to have exceeded the scope.[187] Pursuant to *Runyan*, the police had "substantial[] certain[ty]" as to the illegality of the drive's contents because the private parties knew the contents of the drives before handing them over to police.[188] In so holding, the Fifth and Seventh Circuits adopted the "physical-device" approach[189] as opposed to the "virtual-file" approach.[190]

B. Sixth and Eleventh Circuits

In *United States v. Lichtenberger*, the Sixth Circuit held that police exceed the scope of the private-search doctrine when they have no virtual certainty that the files contained within an electronic-storage device harbor incriminating evidence or are the same files the initial private searcher viewed.[191] The court reasoned that police exceeded the scope of the doctrine by viewing files on a laptop computer without virtual certainty that the initial private searcher had already viewed the files.[192] In so doing, the Sixth Circuit adopted the virtual-file approach[193] and simultaneously created a circuit split with the Fifth and Seventh Circuits.[194] Specifically, the *Rann* court's holding that police could not have exceeded the scope of the private-search doctrine even if they "more thoroughly searched" the storage *device,*[195] directly

185 *Id.* at 837.

186 *Id.* The court discussed "the Illinois Appellate Court's finding that '[a]lthough no testimony exists regarding how the images on the zip drive came to be there . . . it seems highly likely that [the victim's] mother [compiled] the images on the zip drive herself, downloading them from the family computer.'" *Id.* As such, the court reasoned that "it is entirely reasonable to conclude that [the private searchers] knew that the digital media devices contained that evidence," and the police therefore could not have exceeded the scope by searching the drives. *Id.* at 838.

187 *Id.* at 838.

188 *Id.* (citing *Runyan*, 275 F.3d at 463).

189 *See* Kerr, *supra* note 82, at 555 (explaining the physical-device approach).

190 *See id.* at 554–55 (explaining the virtual-file approach).

191 United States v. Lichtenberger, 786 F.3d 478, 488–89 (6th Cir. 2015).

192 *Id.*

193 *See* Kerr, *supra* note 82, at 555 (explaining the virtual-file approach).

194 *See supra* Section II.A.

195 Rann v. Atchison, 689 F.3d 832, 838 (7th Cir. 2012).

contradicts the *Lichtenberger* court's holding that police exceeded the scope of the doctrine because they could not be sure that they were searching the same *files* as the initial private searcher.[196]

Following the *Lichtenberger* court's reasoning in *United States v. Johnson*,[197] the Eleventh Circuit drove a wedge further into the split by issuing a two-part holding on the scope of the private-search doctrine.[198] First, the court held that police do not exceed the scope of the private-search doctrine by viewing photos or videos the initial searcher viewed.[199] Second, the court held that police do exceed the scope of the doctrine by viewing a video that the initial searcher did not view.[200] As such, the Eleventh Circuit effectively adopted the virtual-file approach,[201] falling in line with the Sixth Circuit.[202]

Although federal circuit courts have not been explicit as to which approach they have adopted, their analyses with respect to the private-search doctrine demonstrate their inherent choices.[203] Because courts have not articulated the scope quite so well as Professor Kerr,[204] the circuit split regarding the scope of the private-search doctrine is less pronounced than would traditionally be expected.[205] However, this makes resolving the split no less important and has critical implications for Fourth Amendment jurisprudence.[206]

C. Implications of a Circuit Split

The Supreme Court recently passed on an opportunity to put this dilemma to rest in *Gunter v. United States*.[207] On appeal, the question presented to the Court was "[w]hether the Court should resolve the differing approaches to testing the scope of the search

196 *Lichtenberger*, 786 F.3d at 488.

197 United States v. Johnson, 806 F.3d 1323, 1323, 1329 (11th Cir. 2015). The defendants forgot their cell-phone at a Walmart store. *Id.* at 1329. A Walmart employee discovered the phone and looked through its contents to find child pornography. *Id.* The employee looked through thumbnail images on the phone, opening some to full size, and watched one video. *Id.* The employee turned the phone over to police, informing them of what she had viewed. *Id.*

198 *See id.* at 1336.

199 *Johnson*, 806 F.3d at 1336.

200 *Id.*

201 *See* Kerr, *supra* note 82, at 554–55 (explaining the virtual-file approach).

202 *See* United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015).

203 *See, e.g.*, *id.* at 485–86, 490–91.

204 *See* Kerr, *supra* note 82, at 554 (discussing different approaches to the private-search doctrine).

205 *See* Kerr, *supra* note 10 (explaining the subtlety of the circuit split).

206 *See supra* notes 207–220 and accompanying text.

207 Gunter v. United States, 135 S. Ct. 2335 (2015) (*aff'd mem.*).

necessary to deny to an individual the protection of the Fourth Amendment under the private search doctrine as it applies to electronic data files?"[208] Despite the petitioner's best efforts to convey the Fourth Amendment concerns also discussed at length in this Note,[209] the Court declined to hear the petitioner's case.[210]

The Court's lack of concern has not dissuaded other legal scholars from continuing to express the split's potential pitfalls.[211] Revisiting the topic discussed in his May 2015 article regarding the *Lichtenberger* ruling,[212] Professor Kerr discussed in a more recent article, the *Johnson* decision, as it relates to the circuit split over the scope of the private-search doctrine.[213] Upon reviewing the discrepancies among the holdings in *Runyan*, *Rann*, *Lichtenberger*, and *Johnson*, Professor Kerr asserts that the spilt over the scope of the doctrine now seems fairly even and well-

---

208 Petition for Writ of Certiorari at i, Gunter v. United States, 135 S. Ct. 2335 (2015) (No. 14-1234), 2015 W.L. 1642019, at *1. The "differing approaches" mentioned by the petition refer to the digital-file test and the physical-device test. *See supra* Subsections I.C.1.a–b. The petitioner's brief provided a succinct summary of the factual background of the case:

> [Defendant] was convicted of fraud and money laundering offenses, after a jury trial, arising out of the sale and marketing to foreign investors of shares of stock in publicly-traded United States companies, whose genesis was the product of corporate identity theft. The overwhelming bulk of the evidence offered against [Defendant] at trial came from his own electronic data files (*i.e.*, a laptop computer and memory stick) and the fruits thereof. Specifically, those electronic data files had been seized from [Defendant] by British authorities (without a warrant), who then imaged the files and turned over the images to United States law enforcement authorities. Federal agents then examined the data files without a search warrant and relied on the evidence from the data files to obtain warrants to search [Defendant's] business premises and Online Quick Books account in the United States.

Id. at *2. On appeal, the Eleventh Circuit, relying on *Jacobsen* and the private-search doctrine, held that the defendant had no "reasonable expectation of privacy in his electronic data files to the extent that his electronic data had been searched by foreign governmental officials." *Id.*

209 *See id.* at *9 ("The Court should grant review to clarify the scope of the search necessary to *deny an individual the protection of the Fourth Amendment* under the private search doctrine as it applies to electronic data files found in a computer and a memory stick.") (emphasis added) (caps omitted).

210 *Gunter*, 135 S. Ct. at 2335 (*aff'd mem.*).

211 *See, e.g.*, Kerr, *supra* note 10 (discussing the circuit split and its impact on Fourth Amendment application in the courts).

212 *See id.*

213 *See id.* (explaining how *Johnson* adds onto the already-existing circuit split).

entrenched.[214] The Fifth and Seventh Circuits have adopted the physical-device test,[215] whereas the Sixth and Eleventh Circuits have adopted the virtual-file test,[216] making the split an even two against two.[217]

Professor Kerr's commentary accurately conveys the importance of this issue in the realm of search-and-seizure law.[218] In the interest of consistency and predictability when applying the Fourth Amendment to cyber-crimes, it is imperative that the Supreme Court resolve this circuit split.[219] While some resolutions are more likely and feasible than others, one fact remains unwavering: the private-search doctrine must evolve to have a proper place in the ever-changing digital world.[220]

III. ANALYSIS: REFINING THE PRIVATE-SEARCH DOCTRINE TO PROTECT THE RIGHT TO PRIVACY

The variances of the private-search doctrine's applications and conclusions in the critical cases demonstrate the grave need to resolve the circuit split.[221] For instance, had the *Lichtenberger* court adopted the physical-device approach instead of the virtual-file approach, the court would have had to have concluded that police did not exceed the scope of the private-search doctrine by opening unviewed files on the laptop.[222] As such, the court would have reached the opposite result by ruling the evidence admissible.[223] Similarly, had the *Runyan* court adopted the virtual-file approach instead of the physical-device approach, the court would have had to have concluded that police exceeded the scope of the initial private search by examining files that had not been viewed by the private searcher.[224] As such, the court would have reached the opposite result by ruling the evidence

214 *See id.* ("The new case, *Johnson*, also adopts the data or file approach – thus deepening the 2-1 split into a 2-2 split.").
215 *See supra* Section II.A.
216 *See supra* Section II.B.
217 *See* Kerr, *supra* note 10.
218 *See* Kerr, *supra* notes 10–11.
219 *See* Kerr, *supra* note 10 (highlighting the inconsistencies and implications of the circuit split).
220 *See supra* Sections II.A–B.
221 *Id.*
222 United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015).
223 *Id.* at 491.
224 United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001).

inadmissible.[225] These case examples demonstrate that the scope of the private-search doctrine is very much a dispositive issue.[226]

Case law has been the primary vehicle for creating and evolving the private-search doctrine.[227] Consequently, it is logical to infer that the most likely and realistic body to further develop the doctrine and settle a split between two United States Courts of Appeals is the Supreme Court of the United States.[228] In doing so, the Court need only weigh in and settle on either the virtual-file approach[229] or the physical-device approach.[230] In an ever-changing digital world with electronic-storage devices' capabilities breaking bounds seemingly on a daily basis, the proper choice is the virtual-file approach.[231] However, before explaining the rationale underlying this choice, it is important to examine why the physical-device approach is ill-suited to modern-day electronic-storage devices.[232]

A. The Physical-Device Approach is Unfit for Modern-Day Electronic-Storage Devices

The physical-device test defines the scope of the follow-up search in terms of the device itself.[233] In other words, if a private searcher were to open one file on a laptop computer that contained incriminating evidence, then the physical-device test dictates that police would be free to conduct a warrantless search of the entire laptop.[234] This approach is not only incompatible with the rationale behind the private-search doctrine, but it also does not comport with the spirit of the Fourth Amendment.[235]

---

225 *Id.*

226 *See supra* Sections II.A–C.

227 *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 115, 124–25 (1984) (creating the private-search doctrine).

228 *See id.* (the Supreme Court created the private-search doctrine just over thirty years ago in *Jacobsen*, and assuming the doctrine remains good law, it is reasonable to conclude that the Supreme Court should be the final arbiter as far as ensuring the doctrine is suited for today's world).

229 *See supra* Subsection I.C.1.b.

230 *See supra* Subsection I.C.1.a.

231 *See* Kerr, *supra* note 82, at 556.

232 *See infra* Section III.A.

233 *See* Kerr, *supra* note 82, at 555 (explaining the physical-device approach).

234 *See id.* For an example of this approach in practice, *see* United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001) (finding that a private searcher who opened only a few files on a computer had effectively searched the entire hard drive).

235 *See* Kerr, *supra* note 82, at 573–74 (discussing the critical balance

The private-search doctrine was founded on the idea that the Fourth Amendment does not regulate private individuals from conducting searches, even if those searches are unreasonable.[236] As such, private individuals are free to turn over to police any incriminating information they discover while conducting a private search.[237] However, this liberty has one crucial limitation: In using such information, police must have "virtual certainty" that their follow-up search will reveal nothing more than was already discovered by the private individual.[238] In light of the unfathomable storage capability of today's electronic-storage devices,[239] it is unreasonable to conclude that police could conduct a follow-up search of an entire electronic-storage device with "virtual certainty" that they would not discover anything the private searcher did not already uncover.[240] Furthermore, as stated in *Riley v. California*, the storage capacity of electronic devices significantly increases the risk of violating privacy interests when balancing the government's interest against personal privacy interests to determine a violation of the Fourth Amendment.[241] Consequently, the physical-device test—when used in the context of electronic-storage devices—acts as a contrivance by which police and prosecutors may side-step the Fourth Amendment.[242]

To capture the ridiculousness of the physical-device test as applied to electronic-storage devices today, consider a recent version of the iPhone, which holds 128 gigabytes of storage.[243]

---

between privacy and security in the context of the Fourth Amendment).

236 *See* United States v. Jacobsen, 466 U.S. 109, 113–14 (1984).

237 *See id.*

238 *See* United States v. D'Andrea, 648 F.3d 1, 9 (1st Cir. 2011) ("[A]n antecedent private search does not amount to a free pass for the government to rummage through a person's effects.").

239 *See* Kerr, *supra* note 82, at 541–42 (explaining that computers store a "staggering" amount of data and that "computer storage capacities tend to double about every two years"). *See also, e.g.*, *iPhone 6s*, *supra* note 135 (explaining the storage capabilities of the iPhone).

240 *See D'Andrea*, 648 F.3d at 9 (discussing the virtual-certainty requirement).

241 Riley v. California, 134 S. Ct. 2473, 2489 (2014).

242 *See* Walter v. United States, 447 U.S. 649, 658 n.12 (1980) (explaining that an individual's expectation of privacy is not "undone" by a private search, because "it is difficult to understand how petitioners' subjective expectation of privacy could have been altered in any way by subsequent events of which they were obviously unaware").

243 *See iPhone 6s*, *supra* note 135 (outlining the data specifications of a recent version of the iPhone).

With slight variations depending on the particular device and file type, one gigabyte consists of approximately 1,024 megabytes.[244] The average digital-photograph file ranges from several megabytes to tens of megabytes in size depending on the image's quality.[245] This means that one picture file on that iPhone may constitute a miniscule 0.000076% of the phone's stored data.[246] Under the physical-device test, police would be able to conduct a warrantless search of the entire phone after a private searcher found incriminating evidence within that one file.[247] Stated in more practical terms, police would gain warrantless access to potentially thousands of photos after a private searcher found just one incriminating photo.[248]

Although the *Runyan* court held that police may apply the physical-device approach if they are "substantially certain" as to the device's contents, any argument that police could ascertain this degree of certainty from such a small fraction of the phone's vast pool of data is wholly illogical.[249] Additionally, the *Runyan* court's assertion that a private individual's search of a few files effectively constitutes a search of the entire hard drive makes little sense in light of the insignificant portion a few files consume of an entire hard drive.[250] Furthermore, there is a very real and likely chance that police could learn something from such a follow-up search that they would not have learned from the initial private searcher.[251] Therefore, such a warrantless search would exceed the scope of the initial private search under *Jacobsen*.[252]

---

244 *See* Barnatt, *supra* note 136 (explaining various file types and their sizes).

245 *See id.*

246 *See id.* (128 gigabytes multiplied by 1,204 megabytes equals 131,072; assuming one file is ten megabytes, ten megabytes equal 0.000076 percent of 131,072 megabytes).

247 *See* Kerr, *supra* note 82, at 555 (explaining the physical-device test).

248 *See id.*

249 United States v. Runyan, 275 F.3d 449, 463 (5th Cir. 2001). Similarly, the *Rann* court found that police could search the rest of the applicable device with substantial certainty. *See* Rann v. Atchison, 689 F.3d 832, 837–38 (7th Cir. 2012). However, the unique facts of this case display how the court was able to reach that conclusion: the private searcher actually handed police a ZIP and memory drive that contained exclusively illegal information. *Id.* Therefore, even though the court defined the scope as the physical device, police were effectively employing the virtual-file approach. *Id.*

250 Runyan, 275 F.3d at 464–65. *See* Barnatt, *supra* note 136 (explaining how much data certain file types consume).

251 *See* United States v. Jacobsen, 466 U.S. 109, 118–20 (1984) (holding that police exceed the scope of the private-search doctrine when they discover information not already discovered by a private searcher).

252 *See id.*

In short, the physical-device approach is outdated in the context of electronic-storage devices.[253] By sheer nature of application to by-gone technology, *Runyan* now vies unsuccessfully for the physical-device approach in the context of electronic-storage devices.[254] Additionally, the unique facts in *Rann* fail to effectively counter the virtual-file approach's superiority.[255] Despite these shortcomings, though, the Supreme Court has an alternative, more sustainable path in the virtual-file test.[256]

B. The Virtual-File Test is the Proper Scope for Electronic-Storage Devices

The virtual-file approach defines the scope of the private-search doctrine in terms of each specific, individual file searched by the private searcher.[257] Under this approach, police officers, in conducting a warrantless search following a private search, may only open or view files that a private searcher has already opened and turned over to police.[258] The virtual-file test effectuates the rationale behind the private-search doctrine by allowing private citizens to reveal to police incriminating evidence,[259] all the while ensuring that police will not step outside the bounds of the Fourth Amendment.[260]

For instance, consider again the example of the 128-gigabyte

---

253 *Cf.* Arredondo-Santisteban, *supra* note 131, at 206–07 (discussing how the evolution of technology has in many respects rendered current legislation covering electronic-communications privacy obsolete); Shah, *supra* note 165, at 251 (explaining how legislation is not current enough to appropriately deal with Fourth Amendment violations in cyber-space).

254 *Runyan*, 275 F.3d at 453. The data-storage capability of the floppy disks the *Runyan* court analyzed in 2001 are hugely inferior to that of today's iPhone. *Compare id.* (analyzing floppy disks), *with iPhone 6s*, *supra* note 135 (explaining the data specifications of a recent version of the iPhone). Floppy disks are virtually extinct. *See* Barnatt, *supra* note 136.

255 *See* Rann v. Atchison, 689 F.3d 832, 837–38 (7th Cir. 2012) (discussing how private searchers knew the full contents of the drives that they handed to police).

256 *See infra* Section III.B.

257 *See* Kerr, *supra* note 82, at 554–55 (explaining the virtual-file approach).

258 *See id.* at 555 (explaining the legal application of the virtual-file approach).

259 *See* United States v. Jacobsen, 466 U.S. 109, 113–14 (1984) (explaining that private citizens can reveal information discovered during a private search to police because the Fourth Amendment does not apply to private searches).

260 *See id.* at 119 (discussing that police, in conducting their follow-up search, must have "virtual certainty" as to the illegality of the evidence searched).

iPhone.[261] If a private searcher were to search that phone, find one file to contain illegal data, and then turn that data over to police, the virtual-file approach would allow police to apprehend the wrongdoer without even slightly risking any violations of the wrongdoer's Fourth Amendment liberties.[262] Specifically, law enforcement's follow-up search would unquestionably comport with the virtual-certainty requirement from *Jacobsen*, which dictates that the police, in conducting their follow-up search, must be virtually certain that their search will not uncover anything that the private searcher has not already revealed.[263] And, of course, police could ultimately obtain a search warrant based on such evidence and search the entire device.[264] This would obviate any need for police to risk exceeding the scope of the private-search doctrine—for example, by applying the physical-device approach—ensuring that the wrongdoer could not evade prosecution.[265]

C. Opponents of the Adoption of the Virtual-File Test

As proponents of the physical-device approach are likely to point out, cyber criminals' electronic-storage devices often contain more than one sole file of illegal data.[266] Consequently, such critics might argue that analyzing how one file only makes up 0.000076% of an iPhone's storage capacity is an unfair depiction of the physical-device approach in its practical application.[267] Proponents of this view may attempt to bolster their position by arguing that police may ascertain the requisite level of "virtual

---

261 *See iPhone 6s*, *supra* note 135 (outlining data specifications for a recent version of the iPhone).

262 *See* Kerr, *supra* note 82, at 554–55 (explaining the legal application of the virtual-file approach).

263 *See Jacobsen*, 466 U.S. at 119 (explaining the virtual-certainty requirement).

264 *See* FED. R. CRIM. P. 41(c)(3) ("A warrant may be issued for . . . property designed for use, intended for use, or used in committing a crime.").

265 *See, e.g.*, United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015) (holding that police exceeded the scope of the private-search doctrine because they did not have virtual certainty that the files they searched would not reveal anything not already revealed by the private searcher).

266 *See, e.g.*, *id.* at 480 (explaining that defendant's girlfriend found multiple files of child pornography on defendant's computer); Rann v. Atchison, 689 F.3d 832, 832, 837–38 (7th Cir. 2012) (explaining that private searchers handed over to police storage devices filled with child pornography).

267 *See iPhone 6s*, *supra* note 135 (explaining the data specifications of a recent version of the iPhone); Barnatt, *supra* note 136 (explaining the sizes of different types of files).

certainty" after discovering a significant portion of illegal data on an electronic-storage device.[268] However, the *Runyan* court's holding that a private search of just *one* file frustrates an entire device's expectation of privacy deflates any support such an argument may lend.[269] Against this backdrop, it matters much less how much incriminating evidence police may commonly find, and much more what is very possible: Under the physical-device test, police could easily discover information that a private searcher has not already discovered.[270]

Similarly, proponents of the physical-device approach would likely argue that defining the scope of the private-search doctrine in terms of the entire device allows law enforcement to more effectively uncover criminals who hide their misdeeds in cyberspace.[271] As a consequence, proponents might further argue that limiting the scope of the doctrine would undermine law enforcement's ability to deter and prosecute cyber-criminals.[272] However, this position cannot prevail for two reasons.

First, the virtual-file approach would just as easily enable law enforcement officials to prosecute individuals harboring illegal pieces of media on their electronic-storage devices.[273] For instance, consider one last time the example of the 128-gigabyte iPhone.[274] If a private searcher found one file on that phone to contain incriminating evidence and turned that phone over to police, then the virtual-file approach would enable police to conduct a warrantless search of that file and bring charges against the

---

268 *See, e.g.*, United States v. Runyan, 275 F.3d 449, 463 (5th Cir. 2001) (finding that police had "virtual certainty" based on the files found).

269 *Id.* at 464–65. *See also* Kerr, *supra* note 82, at 555 (explaining that the physical-device approach allows police to search an entire device after finding just one illegal file).

270 *See* United States v. Jacobsen, 466 U.S. 109, 117–20 (1984) (holding that police exceed the scope of the private-search doctrine when they discover information not already discovered by a private searcher).

271 *See* Kerr, *supra* note 46, at 574–75 (explaining that although "traditional" crimes are normally executed in public areas unregulated by the Fourth Amendment and are therefore open to police surveillance, cyber-crimes are not).

272 *See id.*

273 *See* Kerr, *supra* note 82, at 555 (explaining the legal application of the virtual-file approach). For a practical example, consider the court's reasoning in United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015). Had police simply not gone outside the scope of the virtual-file test by looking at files that the private searcher had not already searched, the evidence would have been admissible. *Lichtenberger*, 786 F.3d at 488.

274 *See supra* note 25 and accompanying text.

individual who possessed it.[275] Second, as expressed by the *Riley* court, electronic-storage devices' capability of harboring vast pools of data poses a significant risk of Fourth Amendment violations.[276] The physical-device approach only further exacerbates these privacy concerns by granting police warrantless access to potentially thousands of files that a private searcher has not examined, significantly decreasing the likelihood that police can meet the virtual-certainty requirement.[277] Therefore, upon reviewing the private-search doctrine, the Supreme Court should find that the virtual-file test is the only appropriate scope when the government conducts a warrantless follow-up search of an electronic-storage device.[278]

CONCLUSION

In sum, the federal circuit courts' inability to agree on a uniform scope for a government search following a private search has caused courts to deliver vastly different results in applying the private-search doctrine to electronic-storage devices.[279] As a result, the defendant's jurisdiction could be the difference between admission and suppression of evidence under the same common-law principle.[280] This inconsistency undercuts the interests of fairness in the promotion of justice.[281] As such, the Supreme Court of the United States must review the private-search doctrine and unify the circuits with respect to the scope of the follow-up search as applied to electronic-storage devices.[282] Because of the vast storage capability of modern-day electronic-storage devices, the

---

275 *See* Kerr, *supra* note 82, at 554–55 (explaining the legal application of the virtual-file approach).

276 Riley v. California, 134 S. Ct. 2473, 2488–89 (2014).

277 *See* Kerr, *supra* note 82, at 555 (explaining that the physical-device approach allows police to search an entire device after finding just one illegal file). *See also* United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001) (holding that a private searcher who searched just a few files on a computer had effectively searched the entire hard drive).

278 *See supra* Section III.B.

279 *See supra* Part II.

280 *Compare Runyan*, 275 F.3d at 464 (ruling evidence admissible under the private-search doctrine), *and* Rann v. Atchison, 689 F.3d 832, 836–37 (7th Cir. 2012) (ruling the same), *with* United States v. Lichtenberger, 786 F.3d 478, 491 (6th Cir. 2015) (ruling evidence inadmissible under the private-search doctrine), *and* United States v. Johnson, 806 F.3d 1323, 1336 (11th Cir. 2015) (ruling the same).

281 *See supra* Section II.C.

282 *See supra* Part III.

physical-device test is no longer suitable for applying the private-search doctrine to these devices.[283] Therefore, the Supreme Court should rule that the virtual-file test is the proper scope for courts applying the private-search doctrine to electronic-storage devices.[284]

283 *See supra* Section III.A.
284 *See supra* Section III.B.