GET A WARRANT: A BRIGHT-LINE RULE FOR DIGITAL SEARCHES UNDER THE PRIVATE-SEARCH DOCTRINE

DYLAN BONFIGLI*

TABLE OF CONTENTS

INTRODUCTION

A girlfriend hacks her boyfriend's computer and discovers evidence of tax evasion. She contacts a local law enforcement officer who arrives at her house and looks at the files she found. Without a warrant, the officer opens

* Executive Articles Editor, Southern California Law Review, Volume 90. J.D. Candidate, University of Southern California, Gould School of Law (2017); B.A. Political Science, University of San Diego (2014). Many thanks to Professors Sam Erman, Thomas Griffith, and Del Dickson for outstanding feedback on multiple drafts. I would also like to extend my deepest gratitude to my parents; without their support, this would not have been possible. All errors are my own.

other files in the same folder the girlfriend had searched. The officer notices another folder labeled "xxx." He opens the folder and discovers child pornography. The officer seizes the computer based on what he found. The boyfriend is indicted for possession of child pornography and tax evasion. Before trial, the boyfriend moves to suppress all evidence obtained pursuant to the officer's warrantless search of the computer. What evidence should the judge suppress?[1]

The answer turns on the Fourth Amendment's private-search exception. Under this exception, a government agent may recreate a search conducted by a private individual so long as the agent does not "exceed the scope" of the prior private search.[2] The question under the existing framework is: at what point did the officer exceed the scope of the prior search—if at all? Was it when he viewed files the girlfriend had not viewed, when he opened files in a different folder, or did he stay within the scope of the girlfriend's search by only searching the computer's hard drive? This is what I will refer to as the denominator problem, which asks what courts should use as the unit of analysis to measure the scope of a digital search.[3]

There are at least four competing approaches to the denominator problem, discussed in Part II, and the Supreme Court has provided little guidance on how the private-search doctrine applies to digital searches,[4] resulting in a circuit split.[5] Until this issue is resolved, law enforcement has

1. This hypothetical combines facts from multiple private-search-doctrine cases. *See* United States v. Lichtenberger, 786 F.3d 478, 479–81 (6th Cir. 2015); United States v. Stierhoff, 477 F. Supp. 2d 423, 437–42 (D.R.I. 2007); People v. Emerson, 766 N.Y.S.2d 482, 487–88 (N.Y. Sup. Ct. 2003).

2. United States v. Jacobsen, 466 U.S. 109, 116 (1984); Walter v. United States, 447 U.S. 649, 657 (1980).

3. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 556–57 (2005) [hereinafter Kerr, *Searches and Seizures*] (arguing that the exposed information—what the private individual actually viewed—should be treated as the denominator).

4. *See* Petition for Writ of Certiorari at i, Gunter v. United States, 135 S. Ct. 2335 (2015) (No. 14–1234) (asking "[w]hether the Court should resolve the differing approaches to testing 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?").

5. Orin S. Kerr, *Sixth Circuit Creates Circuit Split on Private Search Doctrine for Computers*, WASH. POST (May 20, 2015), [hereinafter Kerr, *Sixth Circuit Creates Split*] https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/20/sixth-circuit-creates-circuit-split-on-private-search-doctrine-for-computers; Orin S. Kerr, *11th Circuit Deepens the Circuit Split on Applying the Private Search Doctrine to Computers*, WASH. 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. *See also* Benjamin Holley, *Digitizing the Fourth Amendment: Limiting the Private Search Exception in Computer Investigations*, 96 VA. L. REV. 677, 690–96, 701–11 (2010) (discussing various approaches to the denominator

little guidance on when to obtain a warrant following a private search and can unknowingly subject individuals to unreasonable invasions of privacy, which may result in suppression of relevant evidence.[6] One recent example is *United States v. Lichtenberger*.[7]

In *Lichtenberger*, the Sixth Circuit adopted a narrow approach to defining the scope of digital searches and held that a police officer exceeded the scope of a prior search because there was no "virtual certainty" that his search would reveal the same data exposed in the private search.[8] The decision came shortly after and discussed the recent Supreme Court case *Riley v. California*, which recognized that society has a heightened interest in digital information stored on a cell phone.[9] The Sixth Circuit did, however, refuse to extend laptops the same protection that it provides private dwellings—exemption from the private-search doctrine.[10] I disagree with this holding.

This Note rejects the four existing approaches and argues that the private-search exception should not allow warrantless digital searches because society's significant privacy interest in information stored on digital devices outweighs any legitimate government interest in a warrantless search of that device. Instead of using the traditional private-search framework, the Sixth Circuit should have created a bright-line rule, as the Supreme Court did in *Riley*,[11] exempting digital searches from the private-search doctrine. This approach would require law enforcement to

problem and suggesting that a file-based approach should prevail). *Compare* United States v. Sparks, 806 F.3d 1323, 1331 (11th Cir. 2015) (noting that law enforcement exceeded the scope of a prior search when officers viewed a video that was not viewed during the private search, but affirming the district court's denial of defendants' motions to suppress on other grounds), *and Lichtenberger*, 786 F.3d at 490–91 (holding that an officer exceeded the scope of a prior private search when he viewed files that the private individual did not view), *with* Rann v. Atchison, 689 F.3d 832, 836–38 (7th Cir. 2012) (holding that a police officer did not exceed the scope of the prior search when he viewed images that where not uncovered during the prior private search because he was "substantially certain" that the zip drive contained illicit images), *and* United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001) (holding that police officers did not exceed the scope of a prior private search when they viewed files on floppy disks that a private individual had accessed, despite the private individual viewing different files).

6. *See* Lily R. Robinton, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311, 315 (2010) (noting that courts have "struggled to apply Fourth Amendment principles to digital searches to ensure the searches do not expand into exploratory hunts that threaten individual privacy").

7. *Lichtenberger*, 786 F.3d at 488–89.

8. *Lichtenberger*, 786 F.3d at 488–89.

9. Riley v. California, 134 S. Ct. 2473, 2478, 2489–91 (2014).

10. *Lichtenberger*, 786 F.3d at 483–84.

11. *Riley*, 134 S. Ct. at 2495 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

obtain a warrant before reconstructing a private search of digital information.

To support this argument, I distinguish society's privacy interest in digital storage devices from the physical container the Supreme Court based the private-search doctrine on. I will also draw an analogy between digital storage devices and homes, focusing on cases in which courts have refused to extend the private-search exception to private dwellings.[12] At first blush, this approach may appear to be anti-law enforcement, but as I discuss in Part III, law enforcement stands to lose very little from this approach and gains a great deal of clarity when compared to the existing approaches.

This Note will proceed in three parts. Part I describes the background of the private-search exception and various methods that law enforcement uses to carry out digital searches. Part II explains the competing approaches to the denominator problem and problems that arise under each approach. Part III argues that the heightened privacy interests in digital information move digital searches outside the scope of the private-search exception, requiring that law enforcement obtain a warrant before reconstructing a private search of digital data.[13]

I. BACKGROUND

A. THE FOURTH AMENDMENT

The Fourth Amendment provides,

> 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.[14]

12. *E.g.*, United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997); State v. Wright, 114 A.3d 340, 352 (N.J. 2015).

13. Although it is outside the scope of this Note, the 2016 dispute between Apple and the Department of Justice raises a number of unanswered Fourth Amendment questions. *See generally* Orin S. Kerr, *Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case: Part 3, the Policy Question*, WASH. POST (Feb. 24, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/24/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-3-the-policy-question (positing that the Apple/Federal Bureau of Investigation dispute raises the novel question, "what is the optimal amount of physical box security," i.e., how much power should an owner have to prevent non-consensual access to his mobile device).

14. U.S. CONST. amend. IV.

Put simply, the Fourth Amendment protects people from unreasonable searches and seizures.[15] The Fourth Amendment, however, only protects against *government* searches and seizures—"it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the government or with the participation or knowledge of any governmental official.'"[16]

Two of the most important aspects of the Fourth Amendment are the warrant requirement and the exclusionary rule. First, the Fourth Amendment requires that law enforcement obtain a warrant before conducting a "search" unless an exception to the warrant requirement applies.[17] A search occurs when the government (1) obtains information by trespassing on a constitutionally protected area or (2) infringes on an individual's reasonable expectation of privacy.[18] The warrant requirement ensures that a neutral magistrate, as opposed to a zealous officer, determines that probable cause exists.[19] Second, courts generally must exclude any evidence seized in violation of the Fourth Amendment under the exclusionary rule.[20] The purpose of the exclusionary rule is to deter police misconduct, and thus, the rule does not apply when the cost of exclusion outweighs the deterrent effect.[21]

If law enforcement has "probable cause to believe that a container holds contraband or evidence of a crime," it may seize the container and then seek a warrant to examine its contents.[22] The Court has even suggested that law enforcement may briefly seize a container if they have reasonable suspicion—a lower standard than probable cause—that the container holds contraband or evidence of a crime.[23] Once a container is seized, however, law enforcement needs a search warrant to examine its

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

16. *Id.* at 113–14 (citing Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)).

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

18. United States v. Jones, 132 S. Ct. 945, 950–52 (2012).

19. Johnson v. United States, 333 U.S. 10, 13–14 (1948) ("The point of the Fourth Amendment, which is not often grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.").

20. Mapp v. Ohio, 367 U.S. 643, 655 (1961).

21. United States v. Leon, 468 U.S. 897, 906–07, 916 (1984).

22. United States v. Place, 462 U.S. 696, 701 (1983).

23. *Id.* at 697–98.

contents.[24]

Three things are required for a search warrant: (1) it "must be issued by [a] neutral, disinterested magistrate[]"; (2) "those seeking the warrant must demonstrate to the magistrate their probable cause to believe that 'the evidence sought will aid in a particular apprehension or conviction' for a particular offense"; and (3) it "'must particularly describe the things to be seized,' as well as the place to be searched."[25] Probable cause is established if the magistrate determines that "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[26]

Warrantless searches are only reasonable if an exception to the warrant requirement applies.[27] When evaluating exceptions to the warrant requirement, courts must balance "the need for the particular search against the invasion of personal rights that the search entails" to determine reasonableness, taking into account "the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted."[28] As the late Justice Scalia noted, however, exceptions to the warrant requirement continue to eat away at the rule.[29]

B. THE PRIVATE-SEARCH EXCEPTION

The private-search exception allows a government agent to reconstruct a search that was already carried out by a private individual.[30] Two elements must exist for the private-search exception to apply. First, the private individual must not act as an agent of the government.[31] Second, the

24. *Id.* at 701 ("Where law enforcement authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Court has interpreted the Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents, if the exigencies of the circumstances demand it or some other recognized exception to the warrant requirement is present.").

25. Dalia v. United States, 441 U.S. 238, 255 (1979) (citations omitted).

26. Illinois v. Gates, 462 U.S. 213, 238 (1983).

27. Riley v. California, 134 S. Ct. 2473, 2482 (2014) (citing Kentucky v. King, 563 U.S. 452, 459 (2011)) ("In the absence of a warrant, a search is only reasonable if it falls within a specific exception to the warrant requirement.").

28. Bell v. Wolfish, 441 U.S. 520, 559 (1979).

29. California v. Acevedo, 500 U.S. 565, 582–83 (1991) (Scalia, J., concurring) (remarking that "[i]n 1985, one commentator cataloged nearly 20 . . . exceptions [to the warrant requirement]"). *See also* Craig M. Bradley, *Two Models of The Fourth Amendment*, 83 MICH. L. REV. 1468, 1473 (1985) ("There are over twenty exceptions to the probable cause or the warrant requirement or both.").

30. *See* United States v. Jacobsen, 466 U.S. 109, 115–17, 120–21 (1984); Walter v. United States, 447 U.S. 649, 661–62 (1980) (plurality opinion).

31. *See* United States v. Jarrett, 338 F.3d 339, 344–45 (4th Cir. 2003) ("[T]he Courts of Appeals

subsequent government search may not exceed the scope of the prior private search.[32] The first prong ensures that there was no government action during the initial search, which would implicate the Fourth Amendment.[33] This means that the government may use illegally obtained evidence so long as it merely receives the evidence from a private party and was not involved in the illegal private search.[34] The second prong is based on the reasoning that the initial private search extinguishes the owner's expectation of privacy, allowing a government official to learn what the private individual learned.[35]

The two Supreme Court cases that establish the private-search exception are *Walter v. United States* and *United States v. Jacobsen*.[36] In *Walter*, the Supreme Court left open the possibility that the government could conduct a warrantless search based on a prior private search,[37] and in *Jacobsen*, the Court used this dicta to hold that the Fourth Amendment does not apply when the government replicates a prior private search that "enable[s] [it] to learn nothing that had not previously been learned during the private search."[38] A brief summary of each case helps illustrate the private-search doctrine.

have identified two primary factors that should be considered in determining whether a search conducted by a private person constitutes a government search triggering Fourth Amendment protections. These are: (1) whether the government knew of and acquiesced in the private search; and (2) whether the private individual intended to assist law enforcement or had some other independent motivation."); United States v. Hall, 142 F.3d 988, 993–94 (7th Cir. 1998) (holding that a computer repairman's search of a computer did not violate the Fourth Amendment because the repairman was not acting as a government agent).

32. *Jacobsen*, 466 U.S. at 115.

33. Paul G. Reiter, *Annotation, Admissibility, in Criminal Case, of Evidence Obtained by Search by Private Individual*, 36 A.L.R.3D 553, § 3[a] (1971) (collecting cases agreeing that the Fourth Amendment is intended to restrain government action, not private conduct).

34. For a discussion and critique of this rule, in particular to how it relates to digital data, 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 (2005). Another troubling implication of this rule is that the U.S. government can conduct warrantless searches of items that were previously searched by foreign governmental officials, such as the United Kingdom's Serious Fraud Office. *See* United States v. Odoni, 782 F.3d 1226, 1240 (11th Cir. 2015) ("[W]e are convinced British officials reviewed [Defendant's] data files before sending them to the United States. As a result, [Defendant] had no reasonable expectation of privacy in the files when the U.S. officials examined them."); Caitlin T. Street, Note, *Streaming the International Silver Platter Doctrine: Coordinating Transnational Law Enforcement in the Age of Global Terrorism and Technology*, 49 COLUM. J. TRANSNAT'L L. 411, 411 (2011) ("Under the international silver platter doctrine, courts admit the evidence gathered by foreign authorities abroad unless the unreasonable search is deemed a 'joint venture' between U.S. and foreign authorities.").

35. *See Jacobsen*, 466 U.S. at 117.

36. *See generally id.*; Walter v. United States, 447 U.S. 649 (1980) (plurality opinion).

37. *See Walter*, 447 U.S. at 657 n.9.

38. *Jacobsen*, 466 U.S. at 119–21.

In *Walter*, several packages of 8mm films depicting homosexual activity were misdelivered to a private company.[39] Employees examined the boxes, finding "suggestive drawings" and "explicit descriptions of the contents."[40] The Federal Bureau of Investigation ("FBI") retrieved the films after one of the private employees tried without success to view the contents of a film by holding it up to a light.[41] Without a warrant, FBI agents viewed the films on a projector.[42]

A majority of the Court concluded that the search violated the Fourth Amendment, but there was no majority opinion.[43] Justice Stevens, joined by Justice Stewart, announced the opinion of the Court and reasoned that "[t]he projection of the films was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search."[44] No exception to the warrant requirement applied to the FBI agents' actions, and thus viewing the films without a warrant violated the Fourth Amendment.[45] In Justice Stevens' opinion, *Walter* left open the possibility that the government could conduct a warrantless search if it does not exceed the scope of the prior private search.[46]

Justice White, in a concurring opinion joined by Justice Brennan, argued that the plain-view exception allowed the FBI agents to examine the contents of the box when it was turned over by the private employees because "the government saw no more than what was exposed to plain view,"[47] but Justice White disagreed with Justice Stevens' suggestion that the government could have watched the films if the private party watched them before turning them over.[48] In dissent, Justice Blackmun, joined by

39. *Walter*, 447 U.S. at 651.

40. *Id.* at 651–52. *See also* United States v. Sanders, 592 F.2d 788, 790–91 (5th Cir. 1979) (explaining the specific descriptions of the *Walter* film boxes by noting that "[t]he top of each film box showed the name 'David's Boys' and a drawing of two nude males embracing and kissing; on the back of each were the title of the individual movie and a detailed description, in explicit terms, of the bizarre homosexual acts depicted in the films").

41. *Walter*, 447 U.S. at 652.

42. *Id.*

43. *Id.* at 659.

44. *Id.* at 657.

45. *Id.* at 657, 659.

46. *See id.* at 657 n.9 ("Since the viewing was first done by the Government when it screened the films with a projector, we have no occasion to decide whether the Government would have been required to obtain a warrant had the private party been the first to view them.").

47. *Id.* at 660–661 (White, J., concurring).

48. *Id.* at 661–62.

Justices Burger, Powell, and Rehnquist, claimed that the FBI did not need a warrant to view the films because Walter lost any expectation of privacy in the films when the private employees opened the box and ascertained the nature of the films.[49]

Four years later, the Court answered the question raised in *Walter*—whether the government can replicate a prior private search without a warrant.[50] In *Jacobsen*, Federal Express ("FedEx") employees discovered zip-lock plastic bags containing a white powdery substance in a damaged package.[51] The FedEx employees placed the plastic bags back into the box and notified the Drug Enforcement Administration ("DEA").[52] The DEA agent who arrived at the scene removed the plastic bags from the container, conducted a field test, and identified the substance as cocaine.[53] All of this was done without a warrant.[54]

Writing for the Court, Justice Stevens distinguished *Walter* and held that the DEA agent did not exceed the scope of the prior private search because "the removal of the plastic bags from the tube and the agent's visual inspection of their contents enabled the agent to learn nothing that had not previously been learned during the private search."[55] Because the DEA agent did not exceed the scope of the prior search, which frustrated Jacobsen's expectation of privacy as to the contents of the package, the DEA agent did not violate the Fourth Amendment.[56] Put another way, the agent did not conduct a Fourth Amendment "search" because Jacobsen had no reasonable expectation of privacy in the contents of the package after the private search.[57]

Unlike *Walter*, in which law enforcement learned more than the private search had uncovered when it viewed the videos—that the videos were actually obscene, the DEA agent in *Jacobsen* only found that the package contained plastic bags filled with white powder, the same thing the

49. *Id.* at 663 (Blackmun, J., dissenting).

50. *Id.* at 657 n.9. *See* United States v. Jacobsen, 466 U.S. 109, 125–26 (1984).

51. *Jacobsen*, 466 U.S. at 111.

52. *Id.*

53. *Id.* at 111–12.

54. *Id.*

55. *Id.* at 119–20. Justice Stevens reasoned that the seizure (field test) was also justified because "[t]he agents had already learned a great deal about the contents of the package from the [FedEx] employees, all of which was consistent with what they could see." *Id.* at 120–21. For a discussion of the Justices' vote at conference, see THE SUPREME COURT IN CONFERENCE (1940-1985): THE PRIVATE DISCUSSIONS BEHIND NEARLY 300 SUPREME COURT DECISIONS 465–66 (Del Dickson ed., 2001).

56. *Jacobsen*, 466 U.S. at 120.

57. *Id.*

FedEx employees had already discovered.[58] Thus, *Jacobsen* allows law enforcement officers to reconstruct a private search so long as they only confirm what was already learned in the private search, and nothing more.[59] In essence, the Court does not consider it a Fourth Amendment "search" when law enforcement learns what a private party already discovered because the owner's expectation of privacy as to that information has already been frustrated.[60] However, the government needs a warrant if it would uncover facts that were not apparent from the private search because a reasonable expectation of privacy still exists as to the unseen information.[61]

C. COMPUTER SEARCHES

The modern computer or cell phone is capable of storing "millions of pages of text, thousands of pictures, or hundreds of videos."[62] As Professor Orin S. Kerr notes, the storage capacity of cell phones and computers is constantly expanding, allowing us to carry even greater amounts of information in our pockets.[63] The quantity of information we store in digital format can make it difficult for law enforcement to locate incriminating evidence on a cell phone or computer. [64]

Because of this, most computer searches begin with law enforcement generating a bitstream copy of a storage device, such as a hard drive, as opposed to searching the original device.[65] A bitstream copy is essentially an identical image of the contents of the original device, which allows law enforcement to view, but not edit, the files that were stored on the original device.[66]

58. *See* Walter v. United States, 447 U.S. 649, 657 (1980) (plurality opinion) (discussing how the videos thought to be obscene were not actually viewed until the FBI seized them); *Jacobsen*, 466 U.S. at 120.

59. *See Jacobsen*, 466 U.S. at 120.

60. *See id.*

61. *See id.*

62. Riley v. California, 134 S. Ct. 2473, 2478, 2489 (2014) (citing Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 404 (2013) [hereinafter Kerr, *Foreword*]).

63. Kerr, *Foreword*, *supra* note 62, at 404–05.

64. *See Riley*, 134 S. Ct. at 2491; Kerr, *Searches and Seizures*, *supra* note 3, at 569.

65. *See* Kerr, *Searches and Seizures*, *supra* note 3, at 557.

66. *See id.* at 541 ("[T]he bitstream copy duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original."). *See also* DARREN R. HAYES, A PRACTICAL GUIDE TO COMPUTER FORENSICS INVESTIGATIONS Ch. 3, Section Cloning Devices (2014) ("On average, successfully cloning a SATA drive takes less than an hour. Of course, the time to clone depends on the size of the source hard drive

Intuitively, creating a bitstream copy seems like a seizure, but Supreme Court precedent suggests otherwise.[67] In *Arizona v. Hicks*, the Supreme Court held that a seizure did not occur when a police officer wrote down the serial numbers of a stereo system because writing down the serial numbers did not "'meaningfully interfere'" with Hicks' possessory interest in the numbers or the stereo.[68] Lower courts have interpreted this to mean that a seizure does not occur when law enforcement generates a bitstream copy of an electronic device because generating a bitstream copy does not interfere with the owner's possessory interest in the data.[69] The Fourth Amendment is implicated, however, when the government later searches the bitstream copy.[70]

Once law enforcement has a bitstream copy, it can use forensic tools to examine files on the copy.[71] These tools, such as the computer program EnCase, allow an analyst to locate specific types of files even if a user has taken steps to mask the contents of the file.[72] In private-search-exception cases, however, law enforcement usually conducts a simple on-site search of the original device without any forensic tools.[73] A simple search would involve an officer using the search functions on the computer in the same way an ordinary citizen would.[74] A simple search may be ineffective because "[c]omputer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent."[75] As I will discuss in Part III, this makes it important for law enforcement to have a set procedure for searching and seizing digital information, which minimizes the risk of loss of evidence.

and the cloning equipment being used."); ORIN S. KERR, COMPUTER CRIME LAW 320 (2006) ("[A] bitstream image copies every bit and byte on the target drive in exactly the order it appears on the original.").

67. *See* Arizona v. Hicks, 480 U.S. 321, 324 (1987); Kerr, *Searches and Seizures*, *supra* note 3, at 560.

68. *Hicks*, 480 U.S. at 324 (citation omitted).

69. *See* United States v. Gorshkov, No. CR00-550C, 2001 U.S. Dist. LEXIS 26306, at *8 (W.D. Wash. 2001) ("The copying of the data had absolutely no impact on [the defendant's] possessory rights. Therefore it was not a seizure under the Fourth Amendment." (footnote omitted) (citing *Hicks*, 480 U.S. at 324)).

70. *See* Kerr, *Searches and Seizures*, *supra* note 3, at 560–61.

71. G. Robert McClain, Jr., Note, United States v. Hill*: A New Rule, but No Clarity for the Rules Governing Computer Searches and Seizures*, 14 GEO. MASON L. REV. 1071, 1094 (2007).

72. Kerr, *Searches and Seizures*, *supra* note 3, at 544–45.

73. *See* McClain, Jr., *supra* note 71, at 1092 ("The simplest approach is to turn on the suspect's computer and simply start looking around for incriminating files, starting, for example, in the My Documents folder, and then browsing through the various folders until the officer sees something that catches his or her eye.").

74. *See id.*

75. United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998).

D. RILEY'S BALANCING TEST

The unique nature of computer storage often raises novel legal issues that question existing Fourth Amendment jurisprudence.[76] While the recent Supreme Court case *Riley v. California* dealt with the search-incident-to-arrest exception, the Court's approach suggests that it will not formalistically apply existing Fourth Amendment exceptions to digital searches.[77] *Riley* may signal a trend that the Court will favor privacy interests in digitally stored information when there is little justification or need for a warrantless search.[78]

In *Riley*, the Supreme Court recognized that important privacy interests are implicated during the search of a cell phone when it held that the search-incident-to-arrest exception does not apply to cell phones.[79] David Riley was arrested for driving with an expired registration, and police officers searched his cell phone without a warrant shortly after the arrest.[80] Information from his cell phone allowed the police to charge him in connection with an earlier shooting.[81] The government claimed that the search-incident-to-arrest exception applied,[82] and thus, it had the right to "'search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime.'"[83] Indeed, existing search-incident-to-arrest precedent suggested that law enforcement had unlimited discretion to search containers found on an arrestee's person even if the policy reasons for a search incident to arrest did not apply.[84] The Court disagreed,

76. *See* Jacob Gershman, *Alito Says He's Startled by White House Assertions of Executive Power*, WALL ST. J.: LAWBLOG (Sept. 21, 2015), http://blogs.wsj.com/law/2015/09/21/alito-says-hes-startled-by-white-house-assertions-of-executive-power ("Alito moved onto privacy and the Fourth Amendment . . . 'During the past ten years, the Court has applied the Fourth amendment's prohibition against unreasonable search and seizure to modern technology. I think this is going to be a very big issue moving forward.'").

77. *See* Richard Raysman & Peter Brown, *How Has Digital Ubiquity Affected Fourth Amendment Law?*, NEW YORK L.J. (June 9, 2015), https://advance.lexis.com/search?crid=bed6628d-65b0-4fa5-9f37-4c7726170b0d&pdsearchterms=LNSDUID-ALM-NYLAWJ-1202728535476&pdbypasscitatordocs=False&pdmfid=1000516&pdisurlapi=true.

78. *See id.*

79. Riley v. California, 134 S. Ct. 2473, 2491, 2493, 2495 (2014).

80. *Id.* at 2480–81.

81. *Id.* at 2481.

82. *Id.* at 2485–86.

83. *Id.* at 2482 (quoting Weeks v. United States, 232 U.S. 383, 392 (1914)).

84. *See* United States v. Robinson, 414 U.S. 218, 237 (1973) (Powell, J., concurring) ("If the arrest is lawful, the privacy interest guarded by the Fourth Amendment is subordinated to a legitimate and overriding governmental concern. . . . This seems to me the reason that a valid arrest justifies a full search of the person, even if that search is not narrowly limited by the twin rationales of seizing

holding that the search-incident-to-arrest exception did not allow police to search an arrestee's cell phone without a warrant.[85]

The Court evaluated the exception as applied to cell phones by balancing the degree of intrusion on an individual's privacy with the "'promotion of legitimate governmental interests.'"[86] The Court reasoned that the policy concerns that justify the search-incident-to-arrest exception do not apply to searches of cell phones.[87] The two primary justifications for a warrantless search incident to arrest are: (1) protecting the arresting officer's safety and (2) preventing loss or destruction of evidence by the arrestee.[88]

The Court first determined that the data on a cell phone does not present any threat to an officer's safety or to facilitating an escape for the arrestee once the officer has confiscated the phone.[89] Second, the Court found that there was little threat that *the arrestee* could destroy any incriminating evidence because the officer would be able to remove the phone from the arrestee's possession.[90] The government's interest in warrantless searches of cell phones incident to arrest did not outweigh society's immense privacy interest in digital information.[91] Thus, law enforcement cannot use the search-incident-to-arrest exception to justify a

evidence and disarming the arrestee."); *id.* at 239 (Marshall, J., dissenting) ("[T]he majority turns its back on these principles, holding that 'the fact of the lawful arrest' always establishes the authority to conduct a full search of the arrestee's person, regardless of whether in a particular case 'there was present one of the reasons supporting the authority for a search of the person incident to a lawful arrest.'").

85. *Riley*, 134 S. Ct. at 2495.

86. *Id.* at 2484 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)) ("[W]e generally determine whether to exempt a given type of search from the warrant requirement 'by assessing on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" (citing *Wyoming*, 526 U.S. at 295)).

87. *Id.* at 2484–85.

88. *Id.* at 2483 (citing Chimel v. California, 395 U.S. 752, 762–63 (1969)); United States v. Robinson, 414 U.S. 218, 234 (1973) ("The justification or reason for the authority to search incident to a lawful arrest rests quite as much on the need to disarm the suspect in order to take him into custody as it does on the need to preserve evidence on his person for later use at trial.").

89. *Riley*, 134 S. Ct. at 2485.

90. *Id.* at 2486–88. The Court acknowledged that there is a risk that a third party could send a signal that would destroy evidence on the phone, but noted that this is different from the concern that the *defendant* will destroy evidence upon arrest. *Id.* at 2486–87. The Court also claimed that it is unlikely that a warrantless search would prevent a third party from remotely wiping the phone because the phone would still be vulnerable between the time of arrest and the later search. *Id.* at 2487. Finally, the Court pointed out that law enforcement could prevent remote wiping by disconnecting the phone from the wireless network, which can be done by turning off the phone or placing it in a bag that isolates it from radio waves. *Id.*

91. *See id.* at 2484–85, 2494–95.

warrantless search of an arrestee's cell phone.[92] This was a significant departure from prior cases that seemed to give law enforcement the right to open any containers found on the arrestee's person, even when there was no risk of harm to the officer or destruction of evidence.[93]

It has yet to be seen how society's heightened privacy interest in digital information will impact other exceptions to the warrant requirement. Lower courts will need to apply *Riley* to determine whether an individual's privacy interest in different types of digital data outweighs the government's interest in carrying out a warrantless search of that data.[94] In *Riley*, the Court easily found that the warrantless digital search was unreasonable because the government had little-to-no interest in carrying out the search under the search-incident-to-arrest exception.[95] However, it will be more difficult to evaluate warrantless searches under other exceptions when the government can articulate a legitimate interest in the search.[96]

With respect to the private-search exception, the government will likely argue that it has an interest in confirming the private party's description of what was found so that law enforcement can establish probable cause for a warrant.[97] In Part III, I argue that while there are certain circumstances when the government has an interest in reconstructing a private search of digital information, society's privacy interest in this information outweighs the government's.

92. *Id.* at 2495.

93. *See Robinson*, 414 U.S. at 235 ("A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification.").

94. *See* Adam Lamparello & Charles E. MacLean, Riley v. California*: Privacy Still Matters, but How Much and in What Contexts?*, 27 REGENT U. L. REV. 25, 34 (2014) ("[W]hat remains unknown is how weighty an individual's privacy interest will be outside of the arrest context, where the intrusion is less significant, or where the Government's interest is more substantial."); *id.* at 33 ("[F]uture cases involving digital privacy rights will involve balancing an individual's privacy interest against law enforcement's interest in crime prevention.").

95. *Riley*, 134 S. Ct. at 2484–85.

96. *See id.* at 2494; *id.* at 2497 (Alito, J., concurring) ("I would reconsider the question presented here if either Congress or state legislatures, after assessing the legitimate needs of law enforcement and the privacy interests of cell phone owners, enact legislation that draws reasonable distinctions based on categories of information or perhaps other variables.").

97. *See* Kerr, *Sixth Circuit Creates Split*, *supra* note 5 ("[O]fficers may want to check to make sure there is probable cause, making reconstruction of what the private party saw helpful to getting a later warrant.").

II. APPROACHES TO DEFINING THE SCOPE OF DIGITAL SEARCHES

Courts and commentators have suggested at least four different approaches to defining the scope of a digital private search. All four approaches attempt to fit digital searches into the existing *Jacobsen* framework. The broadest approach analogizes a computer to a closed container and allows law enforcement to search the entire computer if a private party has examined any file on the computer. The competing approaches argue that this is too broad and that folders, files, or what is actually exposed to human observation should be treated as the "container" for Fourth Amendment purposes. The following section outlines the four approaches and discusses problems that arise under each.

A. THE FIFTH CIRCUIT *RUNYAN* APPROACH

In *United States v. Runyan*, the Fifth Circuit adopted the broadest approach to defining the scope of a digital search.[98] In *Runyan*, the defendant's wife and her friend searched roughly twenty of the defendant's CDs and floppy disks ("the devices") and discovered child pornography.[99] The friend turned over "twenty-two CDs, ten ZIP disks, and eleven floppy disks to [law enforcement]," and the wife also turned over items to the police.[100] The wife and her friend had not searched all of the devices they turned over to law enforcement.[101] Without a warrant, law enforcement officers viewed images on the devices the wife and her friend had searched, along with images on the devices that they had not searched.[102]

The Fifth Circuit analogized the devices to physical containers and held that the wife and her friend extinguished the defendant's reasonable expectation of privacy in all of the devices that they had searched.[103] The court reasoned that the law enforcement officers were simply examining the devices more thoroughly when they viewed files on the devices that the wife and her friend had already searched.[104] Put another way, by viewing one file on a disk, the wife and her friend frustrated the defendant's

98. United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001). The Seventh Circuit later adopted this approach in *Rann v. Atchison*, 689 F.3d 832, 837 (7th Cir. 2012).

99. *Runyan*, 275 F.3d at 453.

100. *Id.*

101. *Id.* at 460.

102. *Id.*

103. *Id.* at 464–65 ("[W]e find that the police do not exceed the scope of a prior private search when they examine particular items within a container that were not examined by private searchers . . . .").

104. *Id.* at 464.

expectation of privacy as to *all material* on that disk, even if they had only viewed some of the files.[105] The court did, however, hold that law enforcement agents exceeded the scope of the initial searches when they examined disks that the wife and her friend had not searched.[106]

While the search in *Runyan* was of floppy disks, ZIP disks, and CDs, courts have extended this approach to cover devices with much larger storage capacities, such as modern flash drives.[107] For instance, the Seventh Circuit applied the same approach to a camera memory card in *Rann v. Atchison*.[108] Thus, by viewing one file on a modern digital-storage device, a private party can extinguish an individual's reasonable expectation of privacy as to *all* data on that device under the *Runyan* approach. [109]

The troubling aspect of this approach is that digital devices may contain an immense amount of private information. In many cases, evidence of wrongdoing is intermingled with innocent, sensitive information.[110] A search for incriminating material can uncover the owner's financial or medical records.[111] This approach is also inconsistent with *Jacobsen* because law enforcement learns more than the private party did when it views files that the private party did not search.[112]

As Professor Kerr notes, cloud storage, the ability to store files on remote servers,[113] also poses problems under the *Runyan* approach.[114] "A

105. *Id.* at 464–65.

106. *Id.* at 464.

107. *See* Rann v. Atchison, 689 F.3d 832, 837, 838 (7th Cir. 2012) ("[E]ven if the police more thoroughly searched the digital media devices than [the private parties] did and viewed images that [the private parties] had not viewed, per the holding in *Runyan*, the police search did not exceed or expand the scope of the initial private searches.").

108. *Id.*

109. *Runyan*, 275 F.3d at 464–65.

110. United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011) ("[T]here is a far greater potential for the intermingling of documents and a consequent invasion of privacy when police execute a search for evidence on a computer." (internal quotation marks omitted)).

111. *See* United States v. Mitchell, 565 F.3d 1347, 1352 (11th Cir. 2009) ("[T]he hard drive of a computer . . . is the digital equivalent of its owner's home, capable of holding a universe of private information." (internal quotation marks omitted)); Kerr, *Searches and Seizures*, *supra* note 3, at 569 ("[C]omputer searches tend to be unusually invasive. A search for one type of digital evidence often reveals a tremendous amount of other evidence: a great deal comes into plain view. Of course, this can be true of many types of searches, including searches of homes.").

112. *See* United States v. Jacobsen, 466 U.S. 109, 120 (1984) ("[T]he removal of the plastic bags from the tube and the agent's visual inspection of their contents enabled the agent to learn nothing that had not previously been learned during the private search. It infringed no legitimate expectation of privacy and hence was not a 'search' within the meaning of the Fourth Amendment." (footnote omitted)).

113. Some examples of the numerous cloud storage providers are Dropbox, Google Drive, and

single physical storage device can store the private files of thousands of different users."[115] Under *Runyan*, one could argue that law enforcement could examine all files, even those belonging to third parties, on a large server because law enforcement is only examining the server more thoroughly than the private party.[116] Professor Kerr correctly points out that this is illogical: "It would be quite odd if looking at one file on a server meant that the entire server had been searched, and that the police could then analyze everything on the server . . . ."[117]

What may have led to the court's decision in *Runyan*, in my view, was the fact that floppy disks store small amounts of information in comparison to modern hard drives, making any potential privacy invasion less significant. The small storage capacity of floppy disks increases the odds that a disk will contain similar material, unlike modern digital storage devices that usually store a wide variety of information.[118] It is much easier to analogize the storage capacity of a floppy disk to a suitcase than it is to draw the same analogy between a suitcase and a modern hard drive. Further, when *Runyan* was decided in 2001, cloud computing was still in its infancy.[119] The *Runyan* approach is at odds with *Jacobsen* and allows significant invasions of privacy that outweigh any government interest.

B. THE FOLDER-BASED APPROACH

In *People v. Emerson*, a New York court adopted a folder-based approach.[120] The folder-based approach represents a middle ground between the broad approach in *Runyan* and more narrow approaches, which are discussed in the following sections. In *Emerson*, a computer repair technician discovered a computer folder labeled "xxx" that contained images of child pornography and contacted local police after viewing multiple images in the folder.[121] When law enforcement arrived, the repair technician showed the officers several of the files that contained child pornography.[122] After the defendant was indicted, a discovery packet

Microsoft One.

114. *See* Kerr, *Searches and Seizures*, *supra* note 3, at 556; *id.* at 576 n.199 ("Similarly, searches of third-party computers, such as large computer servers, raise unusual problems.").

115. *Id.* at 556.

116. *See* United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001).

117. Kerr, *Searches and Seizures*, *supra* note 3, at 556.

118. *See supra* note 113.

119. *See* Arif Mohamed, *A History of Cloud Computing*, COMPUTERWEEKLY (March 2009), http://www.computerweekly.com/feature/A-history-of-cloud-computing.

120. People v. Emerson, 766 N.Y.S.2d 482, 487–88 (N.Y. Sup. Ct. 2003).

121. *Id.* at 484.

122. *Id.* at 484–85. The court assumed, without deciding, that the repairman acted as an agent of

provided to the defendant indicated that the repairman showed law enforcement a number of files that were unopened in the repairman's initial search.[123] These files were, however, in the same folder as the images found in his initial search.[124]

Although law enforcement viewed more files than the private search, the court reasoned that the label on the folder—"xxx"—and the labels on the files within the folder guaranteed that both searches concerned child pornography.[125] Thus, the court held that when the labels of folders and files suggests illicit content and a private searcher finds that a folder does contain illicit content, the defendant loses any expectation of privacy in all files in the folder.[126] Unlike *Runyan*, in which the court treated digital devices (floppy disks, CDs, and ZIP disks) as the containers, here the court treated the folders as the containers for Fourth Amendment analysis.[127]

The court seems to suggest that the labels and the earlier sampling of files ensured that law enforcement was virtually certain that all files within the folder contained illicit material.[128] This reasoning can, however, lead to a slippery slope. Benjamin Holley points out that this approach creates problems when a user has created folders within folders: "The reasoning could easily be extended such that officers could search every folder contained within a parent folder on the theory that the subfolders are likely to contain similar files or that the folders are suggestively named."[129]

As Judge Kozinski points out, "[t]here is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it."[130] While labels may suggest illicit or obscene material, as was the case in *Walter*, there is no

the government during the second search. *Id.* at 486.

123. *Id.* at 485.

124. *Id.* at 487.

125. *Id.* at 487–88.

126. *Id.* at 493–94. The court did little to elaborate on what the result would have been if the labels did not suggest that the files contained child pornography. Interestingly, the court seems to suggest that a file-based approach would have applied if the materials were only alleged to be obscene. *Id.* at 493 ("[A] warrant would have to be obtained to open the individual files labeled as sexually explicit, on an additional showing beyond the labeling that obscenity may probably be present.").

127. *Id.* at 487–88.

128. *See id.* at 493–94 ("In the context of child pornography . . . a labeling which clearly says that an image file contains a sexual performance by a child, in the context of [the private party's] earlier private search verifying the same during a sampling of the files, needs no additional viewing to determine that it is, indeed, contraband.").

129. Holley, *supra* note 5, at 707.

130. United States v. Hill, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004).

way for law enforcement to know with virtual certainty that the file will contain contraband.[131] A folder with an illicit title and illicit file names, however, would be strong evidence that it contains illicit images and would almost certainly provide probable cause for a warrant. Even if there is strong evidence that files within the folder will contain contraband, the approach is at odds with *Jacobsen* because the private party, having never viewed the actual contents of the folder, can only guess as to the entire folder's contents.

C. THE FILE-BASED APPROACH

Under a more narrow file-based approach, the government exceeds the scope of a prior private search when it views files that were not viewed in the prior private search.[132] In his 2010 note, Benjamin Holley advocates for this approach.[133] In *United States v. Barth*, a case that appears to have adopted the file-based approach,[134] a computer technician viewed what appeared to be child pornography on the defendant's hard drive and contacted the FBI.[135] Later and without a warrant, FBI agents "opened more files and discovered more images of child pornography."[136] The court reasoned that the technician only extinguished the defendant's reasonable expectation of privacy in the files that the technician viewed during his initial search, and thus, the defendant retained a reasonable expectation of privacy in the unviewed files on the hard drive.[137] Thus, the FBI agent exceeded the scope of the private search when he viewed files that the computer repair technician did not view in the initial search, violating the Fourth Amendment.[138]

One aspect of the file-based approach is that many computers and cell phones allow users to view thumbnail images of files before they are

131. *See id.*; Walter v. United States, 447 U.S. 649, 652 (1980).

132. Kerr, *Searches and Seizures*, *supra* note 3, at 554–55 (discussing the approach used in *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999) and noting that a similar approach was used in *United States v. Barth*, 26 F. Supp. 2d 929 (W.D. Tex. 1998)).

133. Holley, *supra* note 5, at 708–11.

134. *See Barth*, 26 F. Supp. 2d at 936–37. The language of the opinion focused on "files" as the unit of analysis, suggesting that a file-based approach was used. *Id.* However, this case was decided before any suggestion of an exposure-based approach and some of the language could be read to suggest that what the private party actually viewed determines the scope of the search. *Id.*

135. *Id.* at 932.

136. *Id.* at 932–33.

137. *Id.* at 936–37.

138. *Id.* at 937 ("Because the subsequent search in this case far exceeded [the computer technician's] viewings, Defendant's Fourth Amendment rights were implicated during the [government's] subsequent viewing of [the defendant's] hard drive.").

opened. This allows a private party to scroll through and "search" hundreds, if not thousands, of files in a short period of time, extinguishing any reasonable expectation of privacy in those files and potentially allowing the government to conduct an in-depth review of the files that contain contraband or evidence of wrongdoing.[139] Some courts hold that the government is simply conducting a more thorough search when it enlarges photos that were previously viewed in thumbnail size.[140] As I discuss in Part III.A, this is one of the many concerns that arise when courts apply the private-search doctrine to digital information.

D. PROFESSOR KERR'S EXPOSURE-BASED APPROACH

Privacy concerns have led courts and scholars, most notably Professor Orin S. Kerr, to advocate for an even narrower approach.[141] Under Professor Kerr's approach, which he refers to as the exposure-based approach, a private party must view the data in order to extinguish an individual's reasonable expectation of privacy in that data.[142] Thus, a government agent exceeds the scope of a private search when he or she views data that was not previously "exposed to human observation."[143] For instance, if a private individual opened a large document and only viewed the first page, the government would exceed the scope of the prior search if it viewed any other pages.[144] One of the main differences between this approach and the file-based approach, at least the one proposed by Benjamin Holley, is that the file-based approach allows law enforcement to view metadata[145] associated with a file even if it was not uncovered in the

139. *See* United States v. Sparks, 806 F.3d 1323, 1331 (11th Cir. 2015); United States v. Tosti, 733 F.3d 816, 819 (9th Cir. 2013).

140. *See Sparks*, 806 F.3d at 1335, 1336; *Tosti*, 733 F. 3d at 822. This may be a close call in cases where a private party is unable to determine the content of the thumbnail picture due to its small size.

141. Kerr, *Searches and Seizures*, *supra* note 3, at 547–48.

142. *Id.* at 548 ("[G]overnment agents may view only the information viewed by the private actor unless they first obtain a warrant."). As Professor Kerr notes, in some cases there is little difference between the exposure-based approach and the file-based approach because in most cases the contraband is the image itself. *Id.* at 556.

143. *See id.* at 547–48.

144. *See id.* at 556–57.

145. "[Metadata] provides information about a certain item's content. For example, an image may include metadata that describes how large the picture is, the color depth, the image resolution, when the image was created, and other data. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document." Per Christensson, *Metadata Definition*, TECHTERMS, http://techterms.com/definition/metadata (last visited Mar. 30, 2017).

private search.[146]

The Eleventh Circuit adopted the exposure-based approach in *United States v. Sparks* when it found that a police officer exceeded the scope of a private search when the officer viewed an entire video of which the private party only viewed the initial image.[147] In *Sparks*, a Walmart employee found a cell phone and viewed numerous images on the phone in thumbnail format.[148] A police officer later viewed the same images and a video stored in the same album as the photos, of which the Walmart employee had only viewed the initial frame of the video in thumbnail format.[149] The court held that the officer did not exceed the private search when he viewed the images that the Walmart employee viewed, but the officer did exceed the private search when he viewed the video that the Walmart employee did not watch.[150]

This helps illustrate the difference between the exposure- and file-based approaches. Under the file-based approach, the officer would not have exceeded the scope of the prior search by watching the video because the employee had already viewed the first frame of the video in thumbnail format, which would have frustrated the cell phone owner's expectation of privacy in the video. But because the court used the exposure-based approach, the officer exceeded the scope of the private search when he watched the video and saw data that the employee was not exposed to.

The Sixth Circuit also adopted what appears to be an exposure-based approach in *United States v. Lichtenberger*.[151] In *Lichtenberger*, the court held that a police officer exceeded the scope of a prior private search because he lacked "virtual certainty" that his search would reveal the same data that was exposed in the private search.[152] The court traced the virtual

146. Holley, *supra* note 5, at 710 ("[Under Professor Kerr's approach], metadata, such as access times and modification history, are generally not part of the private search and may not be viewed by law enforcement absent a warrant or other exception." (footnote omitted)).

147. United States v. Sparks, 806 F.3d 1323, 1335–36 (11th Cir. 2015); Orin S. Kerr, *11th Circuit Deepens the Circuit Split on Applying the Private Search Doctrine to Computers*, WASH. 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.

148. *Sparks*, 806 F.3d at 1329, 1331.

149. *Id.* at 1331–32. It is also important to note that during the police search, text-message notifications appeared on the screen, further exposing the officer to information that was unviewed by the Walmart employee. *Id.* at 1331. The court does not discuss the impact that exposure to this type of information could have on the private-search analysis.

150. *Id.* at 1336.

151. *See* United States v. Lichtenberger, 786 F.3d 478, 485, 488–89 (6th Cir. 2015).

152. *Id.* at 488. A student note criticizes the Sixth Circuit's decision in *Lichtenberger* for, among other things, (1) relying on *Riley v. California*, 134 S. Ct. 2473 (2014), and (2) not adopting the

certainty standard back to the language seen in *Jacobsen*.[153] The court did, however, reject Lichtenberger's argument that the private-search exception should not apply to digital searches.[154]

The Sixth Circuit had previously held that the private-search exception did not allow a warrantless search of a private dwelling,[155] but in *Lichtenberger*, it distinguished personal computers from homes, stating, "Homes are a uniquely protected space under the Fourth Amendment, and that protection 'has never been tied to measurement of the quality or quantity of information obtained.'"[156] If the court accepted Lichtenberger's argument, the police officer in the case would have needed a warrant before observing any of the images that the private party had previously seen.[157]

While the difference between the file-based approach and the exposure-based approach may seem academic, the two approaches can have very different real-world impact. Benjamin Holley suggests that the file-based approach is superior to the exposure-based approach because of the difficulties in determining retroactively what exactly was viewed during the private search and the difficulty that this would place on law enforcement.[158] This problem was illustrated in *Lichtenberger*, in which the private party could not recall what she actually viewed.[159] Holley admits that the distinction between the two approaches would have serious implications when it comes to searching metadata, especially in regard to investigating white-collar crimes.[160]

approach used in *Rann v. Atchison*, 689 F.3d 832 (7th Cir. 2012) and *United States v. Runyan*, 275 F.3d 449 (5th Cir. 2001). Katie Matejka, Note, United States v. Lichtenberger*: The Sixth Circuit Improperly Narrowed the Private Search Doctrine of the Fourth Amendment in a Case of Child Pornography on a Digital Device*, 49 CREIGHTON L. REV. 177, 189–97 (2015). I believe that this criticism is flawed. First, the fact that *Lichtenberger* involved a different exception to the warrant requirement does not render the Supreme Court's analysis in *Riley* irrelevant. Both the search-incident-to-arrest exception and the private-search exception involve balancing society's privacy interest with the government's interest in conducting a warrantless search. The heightened privacy interest in digital information that the Court recognized in *Riley* with regards to the search-incident-to-arrest exception would also need to be weighed in a court's analysis of the private-search exception as applied to digital-storage devices. Thus, the Sixth Circuit did not improperly rely on *Riley*—to the contrary, a court would have been remiss to not consider the impact of *Riley*'s holding on the private-search exception. Second, as discussed in Part II.A, the approaches in *Rann* and *Runyan* are inconsistent with *Jacobsen* and should not be followed.

153. *Lichtenberger*, 786 F.3d at 484, 485–86.

154. *Id.* at 483–84.

155. United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997).

156. *Lichtenberger*, 786 F.3d at 484 (quoting Kyllo v. United States, 533 U.S. 27, 37 (2001)).

157. *See id.* at 483–84.

158. Holley, *supra* note 5, at 710–11.

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

160. Holley, *supra* note 5, at 711 n.170 ("The distinction could be important, however, in certain

The main problem with Holley's proposed file-based approach is that it is inconsistent with the Court's holding in *Jacobsen* that a search exceeds the scope of a private search when the government learns information that was not discovered during the private search.[161] The previously uncovered metadata could provide law enforcement with a trove of deeply private information, such as who viewed a particular document, who authored the document, and where it was viewed.[162] In most cases, the private search would not have uncovered this information. In contrast, the exposure-based approach would require that the private searcher viewed this metadata in order for law enforcement to view it later without a warrant. For these reasons, the exposure-based approach better applies *Jacobsen*.

Further, while Holley is correct that there are difficulties in ascertaining the scope of a prior private search under the exposure-based approach that can hinder law enforcement,[163] even under the file-based approach there can be questions as to whether the private party actually viewed the file in question.[164] The difficulty in ascertaining the scope of a search under both the file- and exposure-based approaches favors a bright-line rule that will not leave law enforcement guessing as to what the private individual actually saw. Further, the warrant requirement is not "'an inconvenience to be somehow 'weighed' against the claims of police efficiency.'"[165] To conclude, the exposure-based approach better applies *Jacobsen*, but, as I will argue in the following section, it does not provide digital information the heightened protection that *Riley* requires.

III. ARGUMENT

A. BRIGHT-LINE RULE: GET A WARRANT

Riley signals that the traditional Fourth Amendment exceptions are ill-suited to the realities of digital-storage devices.[166] Instead of trying to fit

cases. Metadata information—such as who viewed a document and when—may be vital in determining culpability in insider trading and other white collar crimes, for example.").

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

162. *See Riley v. California*, 134 S. Ct. 2473, 2490 (2014).

163. *See* Holley, *supra* note 5, at 710–11; *Lichtenberger*, 786 F.3d at 488.

164. *See Lichtenberger*, 786 F.3d at 488 ("[The private party] admitted during testimony that she could not recall if these were among the same photographs she had seen earlier because there were hundreds of photographs in the folders she had accessed."). One way for law enforcement to ensure that they stay within the scope of the private search would be for an officer to document what the private party saw first and then only replicate this. Having this record would likely provide "virtual certainty" that the officer stayed within the scope of the private search.

165. *Riley*, 134 S. Ct. at 2493 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

166. *Id.* at 2489 ("[A] search of a person was limited by physical realities and tended as a general

digital searches into the existing private-search framework, which the Supreme Court established in a 1984 case dealing with a cardboard package sent via FedEx that contained cocaine,[167] courts should adopt a rule like the one seen in *Riley*—a bright-line rule that exempts digital searches from the private-search exception.[168]

The need for this distinction is based on (1) the differences in privacy interests that exist between digital information and the physical containers that the private-search doctrine was built around; (2) society's treatment of cell phones and personal computers as extensions of an individual's home, using them to store sensitive and personal documents; (3) the ability of a private searcher to use search functions to uncover large amounts of data in a short period of time, unlike physical searches that are limited by physical realities; and (4) the lack of strong policy reasons justifying a warrantless search of a personal computer.

First, increased privacy interests make the privacy implications in digital searches distinguishable from the search of a cardboard box in *Jacobsen*.[169] Unlike *Jacobsen*, in which the package contained contraband and little else, "[a] laptop is 'likely to contain . . . non-contraband information of exceptional value to its owner.'"[170] "[O]wners often have more interest in their computers than they have in traditional closed containers like suitcases or trunks."[171] A great deal of this valuable, personal information is likely to be intermingled with evidence of wrongdoing.[172]

matter to constitute only a narrow intrusion on privacy."). *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (claiming that the existing Fourth Amendment rule that individuals have no reasonable expectation of privacy in information voluntarily disclosed to third parties is "ill suited to the digital age"); Gershman, *supra* note 76 ("Alito moved onto privacy and the Fourth Amendment . . . 'During the past ten years, the Court has applied the Fourth amendment's prohibition against unreasonable search and seizure to modern technology. I think this is going to be a very big issue moving forward.'").

167. *See generally* United States v. Jacobsen, 466 U.S. 109 (1984) (holding that a search exceeds the scope of a private search when the government learns information not discovered during the private search).

168. *Riley*, 134 S. Ct. at 2496–97 (Alito, J., concurring) ("[W]e should not mechanically apply the rule used in the predigital era to the search of a cell phone. . . . This calls for a new balancing of law enforcement and privacy interests.").

169. Brief of Appellee Aron Lichtenberger at 22, United States v. Lichtenberger, 786 F.3d 678 (6th Cir. 2015) (No. 14-3540).

170. United States v. Bradley, 488 F. App'x 99, 104 (6th Cir. 2012) (quoting United States v. Mitchell, 565 F.3d 1347, 1351 (11th Cir. 2009) (per curiam)).

171. *Bradley*, 488 F. App'x at 104.

172. *See* United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011) ("[T]here is a far greater

The ability of computers and cell phones to store large quantities of metadata also raises concerns. As one article notes, "NSA [National Security Agency] General Counsel Stewart Baker has said, 'metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.'"[173] Many electronic devices contain "[a]n internet search and browsing history" that "could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."[174] Under the exposure-based approach, an individual's search history could easily become exposed to a warrantless search so long as the private searcher exposed this data.[175] In some cases, search history information may pre-date the purchase of the digital device.[176] Because of the differences in privacy concerns, courts should not treat personal computers in the same way as the cardboard box in *Jacobsen* and other physical containers.

Second, computers and cell phones are more like homes than the physical containers that the private-search doctrine was built around. Many of us use our cell phones or laptops as an extension of our homes, storing collections of movies, music, and sensitive documents on these devices. In terms of storage capacity, a computer is actually able to store more information than a private residence.[177] In *Riley*, the Supreme Court recognized this, stating that the search of a cell phone "would typically expose to the government far *more* than the most exhaustive search of a house."[178] Like the search of a home, a computer search is likely to uncover a great deal of private, unrelated evidence.[179] Often cell phones

potential 'for the "intermingling" of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.'" (citation omitted)).

173. David Cole, *'We Kill People Based on Metadata'*, N.Y. REVIEW OF BOOKS (May 10, 2014, 10:12 AM), http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata.

174. United States v. Riley, 134 S. Ct. 2473, 2490 (2014). *See also* United States v. Lichtenberger, 786 F.3d 478, 489 (6th Cir. 2015) ("Other documents, such as bank statements or personal communications, could also have been discovered among the photographs. So, too, could internet search histories containing anything from Lichtenberger's medical history to his choice of restaurant. *The reality of modern data storage is that the possibilities are expansive*." (emphasis added)).

175. Kerr, *Searches and Seizures*, *supra* note 3, at 547–48.

176. *See id.* at 543.

177. *Riley*, 134 S. Ct. at 2491.

178. *Id.* (emphasis in original).

179. United States v. Mitchell, 565 F.3d 1347, 1352 (11th Cir. 2009) ("[T]he hard drive of a computer . . . 'is the digital equivalent of its owner's home, capable of holding a universe of private information.'" (citation omitted)); Kerr, *Searches and Seizures*, *supra* note 3, at 569 ("[C]omputer searches tend to be unusually invasive. A search for one type of digital evidence often reveals a tremendous amount of other evidence: a great deal comes into plain view. Of course, this can be true of many types of searches, including searches of homes.").

and computers contain intimate details that would generally have been stored in an individual's home and subject to heightened protection.[180]

Although the Supreme Court has not ruled that the private-search doctrine does not apply to homes and other residences, a number of lower courts have adopted this rule.[181] In *United States v. Allen*, the Sixth Circuit held that the private-search exception did not apply "to cases involving private searches of residences."[182] Thus, a private search of a hotel room did not allow the police to conduct a subsequent warrantless search of the room.[183] The court focused on the difference in the amount of personal possessions that law enforcement would discover in the search of a home as opposed to a package.[184] While *Jacobsen* involved the search of a mail package, "*the entire contents of which were obvious*,"[185] a residence is likely to contain personal items that would go unseen by the private searcher, but that would likely be seen by law enforcement in a more thorough examination of the residence.[186] Central to the court's decision was the fact that the defendant's hotel room contained a number of "personal possessions," some of which were not obvious at first glance, and thus the private search of the room "did not extinguish [the defendant's] privacy interest in the room's contents."[187]

In a similar case, *State v. Wright*, the Supreme Court of New Jersey held that both the State and Federal Constitutions prevent the application of

180. *See* Kyllo v. United States, 533 U.S. 27, 37 (2001) ("[A]ny physical invasion of the structure of the home, 'by even a fraction of an inch,' [is] too much . . . ." (citation omitted)); United States v. United States District Court, 407 U.S. 297, 313 (1972) ("[P]hysical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed . . . .").

181. United States v. Young, 573 F.3d 711, 721 (9th Cir. 2009) ("A guest has a legitimate and significant privacy interest in [a] room's contents, and does not lose his expectation of privacy against unlawful government intrusions into his closed briefcase or the contents of his computer hard drive when hotel staff sees the briefcase, laptop, or other belongings while cleaning the room or changing a light bulb."); United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997); State v. Wright, 114 A.3d 340, 352 (N.J. 2015) ("[W]e conclude that the private search doctrine cannot apply to private dwellings."); State v. Eisfeldt, 185 P.3d 580, 585 (Wash. 2008) (holding that the private-search doctrine is contrary to the Washington Constitution).

182. *Allen*, 106 F.3d at 699.

183. *Id.*

184. *Id.*

185. *Id.* (emphasis added).

186. *See id.*

187. *Id. See also* United States v. Williams, 354 F.3d 497, 510 (6th Cir. 2003) (suggesting that *Jacobsen* should not apply when the subject of the search is "entitled to significantly more protection" than the FedEx package in *Jacobsen*); Brief of Appellee Aron Lichtenberger, *supra* note 169, at 23 (arguing that the private-search doctrine should not apply to "places or things likely to contain highly sensitive personal possessions or information").

the private-search exception to homes.[188] The court distinguished *Jacobsen*, noting that when police officers reconstruct the search of a home "[they are] no longer simply . . . asked to view a discrete set of items turned over to them. Instead, they would walk through a private residence and observe far more."[189] The court then laid out a bright-line rule: "The proper course under the State and Federal Constitutions is the simplest and most direct one. If private parties tell the police about unlawful activities inside a person's home, the police can use that information to establish probable cause and seek a search warrant."[190] By basing its opinion on both the State and Federal Constitutions, the court immunized its decision from federal review.[191] Even if federal courts refuse to adopt a rule that exempts digital information from the private-search doctrine, state courts are free to interpret their state constitutions to provide this protection.[192]

In the absence of action by state and federal courts, a statutory remedy requiring a warrant before reconstruction of a digital search would also protect these important privacy interests from government invasion.[193] For instance, in *Smith v. Maryland*, the Supreme Court found that the use of a pen register to record the numbers dialed on a telephone did not infringe on a legitimate expectation of privacy, and thus it was not a search under the Fourth Amendment.[194] In response, Congress passed legislation requiring a warrant to obtain this data.[195] Congress and state legislatures can take the same action in regards to the application of the private-search doctrine to

188. State v. Wright, 114 A.3d 340, 353 (N.J. 2015).

189. *Id.* at 349.

190. *Id.* at 353.

191. *See* Michigan v. Long, 463 U.S. 1032, 1041 (1983) ("If the state court decision indicates clearly and expressly that it is alternatively based on bona fide separate, adequate, and independent grounds, we, of course, will not undertake to review the decision.").

192. *See* State v. Eisfeldt, 185 P.3d 580, 585–86 (Wash. 2008) ("The individual's privacy interest protected by article I, section 7 [of the Washington Constitution] survives the exposure that occurs when it is intruded upon by a private actor. Unlike the reasonable expectation of privacy protected by the Fourth Amendment, the individual's privacy interest is not extinguished simply because a private actor has actually intruded upon, or is likely to intrude upon, the interest. . . . We therefore reject the private search doctrine and adopt a bright line rule holding it inapplicable under article I, section 7 of the Washington Constitution." (footnotes omitted)). *See also* Goodridge v. Dep't of Pub. Health, 798 N.E.2d 941, 959 (Mass. 2003) ("The Massachusetts Constitution protects matters of personal liberty against government incursion as zealously, and often more so, than does the Federal Constitution, even where both Constitutions employ essentially the same language.").

193. *See* 18 U.S.C. § 2518(10)(a) (2012). *See also* Jordan Miller, *New Age Tracking Technologies in the Post-*United States v. Jones *Environment: The Need for Model Legislation*, 48 CREIGHTON L. REV. 553, 591–93 (2015) (advocating for a statutory scheme that restricts the government's ability to use GPS tracking).

194. Smith v. Maryland, 442 U.S. 735, 742 (1979).

195. 18 U.S.C. § 2518.

digital information by requiring a warrant before reconstruction of a private search. Law enforcement agencies are free to, and should, adopt a policy requiring a warrant before replicating a private search of digital information.

Third, even under the exposure-based approach, digital search features allow private parties to expose large amounts of sensitive information in a short period of time, thus favoring a bright-line approach.[196] In both *Wright* and *Allen*, the courts distinguished *Jacobsen* not only because of sensitive information that individuals store in homes, but also because of the quantity of this information, which may go unseen during a private party's cursory inspection.[197] Digital searches raise the same concern because a private party can expose large amounts of data, even under the exposure-based approach, without fully recognizing the scope of what is uncovered. A brief search of an individual's computer can be unusually intrusive, especially when the government later replicates it, reexamining each file thoroughly.[198]

The notion that a cursory viewing of digital information justifies an unlimited, warrantless government inspection of that information is at odds with the immense privacy interests in digital data, as seen in *Riley*.[199] As one article puts it, "[G]ateways to the most intimate components of one's life must be evaluated with a greater emphasis on retaining that privacy, even at the expense of the ability of law enforcement to combat crime."[200]

196. *See* United States v. Sparks, 806 F.3d 1323, 1331 (11th Cir. 2015) ("In the phone's photo-album application, [the private party] accessed a screen that displayed several smaller 'thumbnail' images.").

197. *See* United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997); State v. Wright, 114 A.3d 340, 352 (N.J. 2015) ("In short, a private home is not like a package in transit.").

198. The Supreme Court of Idaho described the invasion that takes place when the private-search doctrine is applied to homes as follows:

> If the state were to have its way on this point, it would apparently argue that the following scenario is outside constitutional protection: A private citizen ransacks a home, claiming to be in search of contraband. Upon discovering the alleged contraband, the citizen calls in the police who conduct a second ransacking of the home, looking and searching everywhere and inspecting everything as did the citizen. According to the state, because the officer is only "viewing" the citizen's efforts—"merely" retracing the citizen's footsteps—such government activity is outside the purview of federal and state constitutional protections. Such an aberrational view is not harmonious with what the framers of our federal and state constitutions intended when they put these protections into our constitutions, and we so hold.

State v. Johnson, 716 P.2d 1288, 1293 (Idaho 1986). In most cases, a search of a personal computer is just as intrusive, if not more so, as the search described by the Idaho Supreme Court.

199. Riley v. California, 134 S. Ct. 2473, 2490 (2014).

200. Raysman, *supra* note 77.

Accordingly, courts should provide digital-storage devices the same status as homes for private-search analysis—a requirement that law enforcement obtain a warrant before reconstructing a prior search.

Fourth, a bright-line rule, unlike many of the existing approaches, gives law enforcement clear guidance on when they need a warrant. As discussed in Part II.D, the exposure- and file-based approaches force courts to engage in a difficult factual inquiry as to the scope of the prior search. In *Lichtenberger*, the police officer did what he should have done under the exposure-based approach when he "asked [the private party] if she could boot up the laptop to show him *what she had discovered*."[201] Despite the officer's attempt to stay within the scope of the private search, the court found that there was no virtual certainty that the officer did so.[202] Requiring a warrant provides law enforcement with a clear rule on what they must do before searching a computer, and it prevents courts from wading into the difficult factual inquiry of what files, and how much of those files, the private party saw.

Even under the exposure-based approach, there is also a risk that law enforcement will unwillingly discover data that was unseen in the private search, such as text messages, emails, or other notifications that appear on screen without any action by the government.[203] An officer may be in the process of viewing what was uncovered in the private search when a notification exposes the officer to information that the private searcher was unaware of, such as the phone's owner and people with whom the owner associated.[204] This information is clearly outside the scope of the private search, and the owner of the phone would presumably have a reasonable expectation of privacy with regard to these messages. Accordingly, the text message or email evidence would likely be suppressed even though there is little to no fault on the officer's part.[205] The officer could have easily avoided this situation by obtaining a warrant before the search.

201. United States v. Lichtenberger, 786 F.3d 478, 480 (2015) (emphasis added).

202. *Id.* at 488–89.

203. *See, e.g.*, United States v. Sparks, 806 F.3d 1323, 1331 (11th Cir. 2015) ("While [the private searcher] displayed the images to [law enforcement], text-message notifications appeared on the screen.").

204. *See id.*

205. One could argue that an officer can avoid this type of unwilling disclosure by disconnecting the phone or computer from whatever network it is connected to. *See* Riley v. California, 134 S. Ct. 2473, 2487 (2014) (noting that law enforcement can turn off a device or place it in an "enclosure that isolates [it] from radio waves" to disconnect it from the network). While turning off the device or isolating it from radio waves would prevent unwilling disclosure, I think these solutions may be impractical in reality. Simply getting a warrant likely places less of a burden on the government than requiring it to go through these steps to carry out a warrantless search.

The bright-line rule also promotes responsible investigative techniques. Requiring a warrant before a digital search can prevent law enforcement from contaminating or damaging evidence in certain situations.[206] Some private-search cases involve law enforcement conducting an on-site search.[207] These on-site manual searches in which law enforcement simply turns on the computer and searches for incriminating files can lead to destruction of evidence.[208] As G. Robert McClain, Jr. aptly puts it, "The physical world equivalent of the [manual on-site search] . . . might be an officer walking into a murder scene with muddy boots, removing, bare-handed, a knife from the victim, dropping it in his coat pocket and returning to the office."[209] One solution to this problem is to create a bitstream copy, which law enforcement can search later without damaging or destroying the original evidence.[210] Requiring a warrant is one step toward making sure that law enforcement uses approved search protocols that preserve the chain of custody.

B. POTENTIAL CRITICISM

Some may argue that a bright-line rule will hinder law enforcement investigations.[211] Professor Kerr touched on the possible constraints of this approach in a *Washington Post* article:

> [Y]ou might be asking, can't the government just get a warrant based on the private party report? It depends. Sometimes the private report will provide probable cause and sometimes it won't. The officers may want

206. *See* McClain, Jr., *supra* note 71, at 1083 ("On-site searching can result in destroying or altering evidence, and can easily take so long to perform that it would place undue burdens on both the police and the suspect whose premises are being searched."); Robinton, *supra* note 6, at 324–25 ("Simply opening a file or turning on a computer can overwrite deleted data, and may alter time stamps on the data, which investigators might need to show the time the suspect created or last accessed a file.").

207. *See, e.g.*, United States v. Lichtenberger, 786 F.3d 478, 480–81 (2015) (describing an on-site search carried out by a police officer and the defendant's girlfriend).

208. *See* McClain, Jr., *supra* note 71, at 1081 ("[O]n-site computer searches risk damage or alteration to the evidence. . . .").

209. McClain, Jr., *supra* note 71, at 1094. The author also notes, "[D]igital evidence on computer storage media is almost always better suited to an off-site search by an expert in a controlled environment." *Id.* at 1084.

210. *Id.* at 1083; United States v. Grimmett, 439 F.3d 1263, 1269 (10th Cir. 2006) ("It is only with careful laboratory examination of electronic storage devices that it is possible to recreate the evidence trail." (internal quotation marks omitted)).

211. *See* Kerr, *Sixth Circuit Creates Split*, *supra* note 5; Holley, *supra* note 5, at 712 ("One objection to the [file-based approach] is that narrow exceptions to the warrant requirement hinder police investigation, making it more difficult to find and arrest criminals.").

> to check to make sure there is probable cause, making reconstruction of what the private party saw helpful to getting a later warrant.[212]

While there may be situations in which law enforcement is unable to obtain a warrant based on the private report, these situations would be extremely rare and provide little justification for the privacy invasions that follow.

Probable cause for a search warrant exists when there is a "'substantial basis for . . . conclud[ing]' that a search would uncover evidence of wrongdoing."[213]

> The task of the issuing magistrate is simply to make a practical, common-sense decision whether, *given all the circumstances* set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.[214]

A warrant may be based on "hearsay" so long as the information is "reasonably corroborated by other matters within the officer's knowledge."[215]

In the context of private-search cases, an officer's affidavit will be based, at least in part, on a private party's statement that the defendant's computer contains evidence of wrongdoing. Courts have frequently found that a statement from an identified informant who meets with the police in person and provides information of wrongdoing based on firsthand knowledge is enough to establish probable cause.[216] Police can often

212. Kerr, *Sixth Circuit Creates Split*, *supra* note 5.

213. Illinois v. Gates, 462 U.S. 213, 236 (1983).

214. *Id.* at 238 (emphasis added). In rejecting the more rigid *Aguilar-Spinelli* two-prong test for probable cause, the Court stressed its desire to encourage law enforcement to get a warrant before a search as opposed to trying to use an exception to the warrant requirement. *Id.* at 236, 238. The Court notes that "'[a]lthough in a particular case it may not be easy to determine when an affidavit demonstrates the existence of probable cause, the resolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants.'" *Id.* at 237 n.10 (citation omitted). By lowering the threshold for probable cause, the Court hoped to "encourage use of the warrant process" in recognition that "once a warrant has been obtained, intrusion upon interests protected by the Fourth Amendment is less severe than otherwise may be the case." *Id.* A bright-line rule would reduce the number of warrantless searches that rely on the private-search doctrine, thereby reducing the intrusion on Fourth Amendment interests. This is certainly one consideration for a magistrate who receives an affidavit that alleges evidence of wrongdoing stored in digital form.

215. Jones v. United States, 362 U.S. 257, 269 (1960).

216. United States v. Kinison, 710 F.3d 678, 682–83 (6th Cir. 2013) ("[W]e have clearly held that a known informant's statement can support probable cause even though the affidavit fails to provide any additional basis for the known informant's credibility and the informant has never provided information to the police in the past."). *See, e.g.*, United States v. Ruth, 489 F. App'x. 941, 943 (6th Cir.

corroborate the informant's basis through their own investigation, further supporting a finding of probable cause.[217] The low threshold for establishing probable cause makes it such that an officer can easily obtain a warrant by interviewing the private party and conducting a minimal level of corroboration. In fact, it is troubling that law enforcement would rely on the private-search exception to conduct a search of digital information when probable cause is lacking.

If an officer needs to corroborate evidence or question an informant to establish probable cause for a warrant, the officer should be allowed to temporarily seize the electronic device so long as the seizure is properly limited in scope. This approach is supported by the need to prevent destruction of evidence and the Court's holding in *United States v. Place*.[218] Under *Place*, certain situations allow law enforcement to seize an item when they have reasonable suspicion that it contains contraband or evidence of a crime.[219] In *Place*, the investigatory seizure based on reasonable suspicion was supported by the "inherently transient nature of drug courier activity at airports."[220] Similarly, in the context of computer crimes, the government has a substantial interest in temporarily seizing a device to prevent destruction of evidence because of the threat of remote wiping.[221] Law enforcement's interest in preventing destruction of evidence justifies a temporary seizure of an electronic device, during which time law enforcement must carry out their investigation in a reasonable and diligent manner.[222]

2012).

217. *See, e.g.*, United States v. Potts, 586 F.3d 823, 830 (10th Cir. 2009) ("We conclude that the warrant was supported by an adequate showing of probable cause. [The officer's] affidavit recited the information she had obtained from the complaining witness, information [that] was plausible on its face. [The officer] investigated some of the details that the witness had reported, and her investigation verified what the witness had reported. [The officer] did not investigate every part of the witness's account, but the law has never required an officer to conduct a perfect investigation."); United States v. Gitarts, 341 F. App'x. 935, 938 (4th Cir. 2009); United States v. McGaughey, 200 F. App'x. 305, 306 (5th Cir. 2006) ("The informants independently provided the police with firsthand knowledge of [defendant's] name, address, and place of work, and the police verified the accuracy of this information before seeking [a] warrant.").

218. *See* United States v. Place, 462 U.S. 696, 706 (1983). In many cases, the temporary seizure may be unnecessary if the officer is able to obtain a bitstream copy of the device.

219. *Id.* at 702–04, 706.

220. *Id.* at 704.

221. *See* Riley v. California, 134 S. Ct. 2473, 2487 (2014). Once the item is seized, the officer would be able to take measures to prevent remote wiping of the device. *Id.*

222. *See* House v. Napolitano, No. 11-10852-DJC, 2012 U.S. Dist. LEXIS 42297, at *28–29 (D. Mass., March 28, 2012).

Law enforcement could still rely on other exceptions to the warrant requirement. In situations where an officer is unable to obtain a bitstream copy, which would be rare, the officer could rely on the exigent-circumstances exception to search a computer or cell phone without a warrant.[223] "In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that [would be] suggested. . . ."[224]

The plain-view exception would also still apply. When a police officer acts "'merely as a witness'" and sees something that a private party shows to him without prompting, the plain-view exception would apply and the evidence would be admissible.[225] For instance, if a private party presented an officer with a cell phone or laptop that displayed incriminating evidence in plain view, there would be no need for a warrant. On the other hand, the plain-view doctrine should not allow an officer to direct a private party to reconstruct their prior search while the officer watches. Under these circumstances, the private party would be acting as an agent of the government, and the officer would need a warrant. The availability of the exigent-circumstances and plain-view exceptions leaves law enforcement with many of its familiar tools.

Similarly, critics may argue that digital information should not receive the same protections as homes because of a home's unique status under the Fourth Amendment.[226] This was the reason the *Lichtenberger* court gave when it refused to exempt cell phones from the private-search doctrine.[227] However, the Supreme Court has stated that digital information "implicate[s] privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[228] These privacy concerns prevented law enforcement from carrying out a search incident to arrest of an arrestee's cell phone, despite the arrestee's reduced expectation of privacy

223. James M. Rosenbaum, *In Defense of the Sugar Bowl*, 9 THE GREEN BAG 2d 55, 57 (2005) ("[I]f immediate access is needed – when exigent circumstances are present – the investigator can demonstrate the need and be granted immediate access."). *See also Riley*, 134 S. Ct. at 2494 (discussing the applicability of the exigent circumstances exception to "prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury").

224. *Riley*, 134 S. Ct. at 2494.

225. *See* United States v. Benoit, 713 F.3d 1, 9–12 (10th Cir. 2013).

226. Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) ("[W]hen it comes to the Fourth Amendment, the home is first among equals.").

227. United States v. Lichtenberger, 786 F.3d 478, 484 (6th Cir. 2015).

228. *Riley*, 134 S. Ct. at 2488–89.

flowing from the arrest.[229] This suggests that an individual's reasonable expectation of privacy in digital information could survive a private search, unlike the defendant's reasonable expectation of privacy as to the contents of the package in *Jacobsen*.

The *Lichtenberger* court also attempted to distinguish homes from computers stating "all details in a home 'are intimate details, because the entire area is held safe from prying government eyes.'" [230] Why would the same not be true for someone who password protects their computer or cell phone? In the case of someone who uses a computer that is not connected to the Internet or simply has a storage drive, all of that information is "held safe from prying government eyes."[231] And even when an individual chooses to broadcast information from his or her phone or cell phone, all other information stored on their device is kept safe from prying government eyes. An analogy between digital devices and homes is much stronger than to traditional physical containers for the purposes of the private-search exception, and thus digital information should receive the same protection that most courts have applied to homes: exemption from the private-search exception.

Another potential criticism of the bright-line approach that exempts digital information from the private-search exception is that it provides heightened protection to information that is in digital form. For instance, law enforcement can rely on the private-search exception to conduct a search of physical documents that were previously searched by a private individual, but the rule would prevent an officer from executing the same search if the files were in digital format. Counsel for Lichtenberger pointed out that a bright-line rule for digital information can lead to inconsistent results, noting that "had [the private party] printed an image during her initial search, there would have been no Fourth Amendment violation had [the officer] subsequently directed her to show him the printout."[232]

While the bright-line rule can lead to inconsistent results, the Supreme Court has accepted inconsistencies when it comes to protecting digital information.[233] In *Riley*, Justice Alito questioned the Court's decision to exempt digital information from the search-incident-to-arrest exception,

229. *Id.* at 2493–95.
230. *Lichtenberger*, 786 F.3d at 484 (citation omitted).
231. *Id.*
232. Brief of Appellee Aron Lichtenberger, *supra* note 169, at 26.
233. *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring).

pointing out that doing so provides heightened protection to information in digital form.[234] In Justice Alito's words,

> While the Court's approach [in *Riley*] leads to anomalies, I do not see a workable alternative. *Law enforcement officers need clear rules* . . . and it would take many cases and many years for the courts to develop more nuanced rules. And during that time, the nature of the electronic devices that ordinary Americans carry on their persons would continue to change.[235]

In addition to the need for providing law enforcement with a clear rule, inconsistent results under the private-search exception are justified by the sensitive nature of digital data, the ease with which it can be exposed, and the difficulties in confining a subsequent search.[236] These same concerns are prominent when the private-search exception is used to conduct a warrantless search of digital information, and they justify a bright-line rule that exempts digital information from the private-search exception, despite the heightened protection it provides to digital information.

CONCLUSION

Riley recognizes society's heightened privacy interest in digital data stored on personal computers and requires that courts balance these heightened interests with the government's interest in conducting a warrantless search.[237] "[W]hen 'privacy-related concerns are weighty enough' a 'search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee.'"[238] Like *Riley*, the diminished expectations of privacy that result from a private search are insufficient to outweigh the privacy interests that individuals have in digital information. This leaves law enforcement with a bright-rule for reconstructing private searches of digital data—"get a warrant."[239]

234. *Id.* at 2497 (Alito, J., concurring) ("[T]he Court's broad holding favors information in digital form over information in hard-copy form.").

235. *Id.* at 2497 (Alito, J., concurring) (emphasis added).

236. *See supra* Part III.A. *See also Riley*, 134 S. Ct. at 2497 (Alito, J., concurring) ("[B]ecause of the role that [cell phones] have come to play in contemporary life, searching their contents implicates very sensitive privacy interests that this Court is poorly positioned to understand and evaluate. Many forms of modern technology are making it easier and easier for both government and private entities to amass a wealth of information about the lives of ordinary Americans, and at the same time, many ordinary Americans are choosing to make public much information that was seldom revealed to outsiders just a few decades ago.").

237. *See Riley*, 134 S. Ct. at 2493–95.

238. *Id.* at 2488 (quoting Maryland v. King, 133 S. Ct. 1958, 1979 (2013)).

239. *Id.* at 2495.