# IMPLICATIONS OF THE PRIVATE SEARCH DOCTRINE IN A DIGITAL AGE: ADVOCATING FOR LIMITATIONS ON WARRANTLESS SEARCHES THROUGH ADOPTION OF THE VIRTUAL FILE APPROACH

BRIANNA M. ESPELAND

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

# IMPLICATIONS OF THE PRIVATE SEARCH DOCTRINE IN A DIGITAL AGE: ADVOCATING FOR LIMITATIONS ON WARRANTLESS SEARCHES THROUGH ADOPTION OF THE VIRTUAL FILE APPROACH

BRIANNA M. ESPELAND*

TABLE OF CONTENTS



---

* University of Idaho College of Law, J.D., 2017. The author would like to express her sincerest gratitude for the love, support, and advice of her parents and family, without whom none of her success would be possible. Additionally, the author would like to thank Professor Aliza Cover for her guidance and encouragement.

## I. INTRODUCTION

As Justice Learned Hand once observed, it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him."[1] As Chief Justice Roberts explained in *Riley v. California*, that statement is no longer true, due to the advent of the digital age and the proliferation of electronic devices containing immense storage capabilities.[2] It is much more likely in the modern age that a man's person will contain everything which may incriminate him, simply by the man's possession of a modern digital storage device, such as a cell phone, computer, or external hard drive.[3] In 2015, a survey conducted by the PEW Research Center revealed that 92% of U.S. adults owned a cellphone, with 68% of U.S. adults owning a "smartphone."[4] The survey also concluded 73% of U.S. adults owned a desktop or laptop computer and 45% of U.S. adults

1. Riley v. California, 134 S. Ct. 2473, 2490–91 (2014) (citing United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926)).

2. *Id.* at 2491.

3. *See id.*

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

owned a tablet computer.[5] These digital devices store personal and private information in staggering amounts, a fact that has important consequences on a person's right to privacy under the Fourth Amendment.

The Fourth Amendment guarantees "a safeguard to the liberty of the individual,"[6] by "protect[ing] citizens against unreasonable governmental searches and seizures."[7] In defining what constitutes an unreasonable governmental search and seizure, the Supreme Court of the United States has identified several exceptions to the Fourth Amendment's broad protections. One of these exceptions to the Fourth Amendment is known as the private search doctrine, first highlighted in *Walter v. United States*,[8] and further elaborated in *United States v. Jacobsen*.[9]

The private search doctrine relies upon the premise that the Fourth Amendment only applies to *governmental* action, not action by private citizens.[10] Therefore, if a private citizen, acting upon his own volition and not at the behest of a governmental agent, searches another person's private personal property (in which the person possesses a reasonable expectation of privacy) and finds incriminating material, the private citizen is permitted to disclose that incriminating material to a government agent.[11] The government agent is then permitted to search and seize the incriminating material without first obtaining a warrant.[12]

The private search doctrine was initially introduced in relation to a private search of a physical container — a package

---

5. *Id.*

6. NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 9 (1937).

7. THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION xix (Carolina Academic Press, 2008).

8. Walter v. United States, 447 U.S. 649, 650 (1980).

9. United States v. Jacobsen, 466 U.S. 109, 112 (1984).

10. *Id.* at 113.

11. *Id.*

12. *Id.*

shipped through FedEx.[13] In the advent of the digital age, however, the private search doctrine has been routinely applied to searches of digital containers, such as computers, flash drives, cell phones, and CDs.[14] In applying the private search doctrine to digital containers, there has been some contention amongst the United States Circuit Courts of Appeals regarding the proper determination of permissible scope for the subsequent government search following the initial private search.[15] The specific issue of contention is how to define the scope of the search and what constitutes a "container" for purposes of determining what the government agent is permitted to search.[16] Three options for defining the container have been introduced amongst the various circuits, the district courts, and legal scholars: the device itself, the individual file or image originally searched, or the exposed data of the individual file or image (the data visible on the screen).[17]

The United States Circuit Courts of Appeals for the Fifth and Seventh Circuits hold that the proper limitation of scope is to the digital storage device itself.[18] The reason for this holding is the assumption that when a private person searches the digital device, by opening the device itself, the private person has frustrated any

---

13. *Id.* at 111.

14. United States v. Sparks, 806 F.3d 1323, 1330 (11th Cir. 2015) (cell phone); United States v. Lichtenberger, 786 F.3d 478, 479 (6th Cir. 2015) (computer); United States v. Tosti, 733 F.3d 816, 818 (9th Cir. 2013) (computer); Rann v. Atchison, 689 F.3d 832, 833 (7th Cir. 2012) (ZIP drive and camera memory card); United States v. Runyan, 275 F.3d 449, 451 (5th Cir. 2001) (ZIP disks).

15. *See* 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/.

16. *See id.*

17. *Sparks*, 806 F.3d 1323; *Lichtenberger*, 786 F.3d 478; *Tosti*, 733 F.3d 816; *Rann*, 689 F.3d 832; *Runyan*, 275 F.3d 449; Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 554 (Dec. 2005).

18. *See Rann*, 689 F.3d 832; *Runyan*, 275 F.3d 499.

remaining expectation of privacy in the device.[19] Therefore, any subsequent governmental action cannot be defined as a search for Fourth Amendment purposes.[20] The implication of this ruling is that even if the private person has only searched one file on the device, the entire device is open to the subsequent government investigation.[21] The government agent can view any file, image, or data on the device, without a warrant, even if it has not already been viewed by the private searcher.[22]

The United States Circuit Courts of Appeals for the Sixth and Eleventh Circuits, and the Ninth Circuit through dicta, hold the Fifth and Seventh Circuits's definition of container is too expansive and in violation of the purpose of the Fourth Amendment.[23] These circuits instead hold that the proper definition of "container" is limited to the individual file or image searched by the private person as part of the initial private search.[24] The Sixth and Eleventh Circuits maintain the expansive storage capacity of modern digital devices and the improbability of virtual certainty in what those devices may contain mandates a stricter definition of "container," particularly in light of the important policy considerations regarding modern digital devices highlighted by the Supreme Court in *Riley v. California*.[25]

As this article will make clear, the proper definition of "container" is the definition pronounced by the Sixth and Eleventh Circuits. This definition preserves and furthers the purpose of the Fourth Amendment, properly takes into account the unique characteristics and implications of modern digital devices, appropriately balances the competing interests of governmental autonomy and privacy protection, and befittingly incorporates the current

---

19. *See Rann*, 689 F.3d 832; *Runyan*, 275 F.3d 499.

20. *See Rann*, 689 F.3d 832; *Runyan*, 275 F.3d 499.

21. *See Rann*, 689 F.3d 832; *Runyan*, 275 F.3d 499.

22. *See Rann*, 689 F.3d 832; *Runyan*, 275 F.3d 499.

23. *See Sparks*, 806 F.3d at 1336; *Lichtenberger*, 786 F.3d at 491; *Tosti*, 733 F.3d at 821–22.

24. *See Sparks*, 806 F.3d at 1336; *Lichtenberger*, 786 F.3d at 491; *Tosti*, 733 F.3d at 821–22.

25. *See Riley v. California*, 134 S. Ct. at 2490–91; *Lichtenberger*, 786 F.3d at 491; *Sparks*, 806 F.3d at 1336.

stance of the Supreme Court regarding privacy interests in the modern digital age.

This comment will first briefly give background information on the current circuit split issue by introducing the Fourth Amendment and the private search doctrine in general. It will then explore what it means to "exceed the scope of the private search" under the private search doctrine, by discussing the physical container distinction and then the digital zone distinction highlighted by Orin S. Kerr. Next, this comment will examine how the various circuit courts of appeals have applied the container distinction to digital storage devices and advocate for the approach taken by the Sixth, Ninth, and Eleventh United States Circuit Courts of Appeals in limiting the digital container definition to an individual file or image on the digital device. In explaining how the proper definition of digital container is the individual file or image, this comment will conclude with a discussion of the important policy interests at stake on either side of the divide: the governmental interest in investigating and prosecuting criminal activity and preserving digital evidence on one side, and the personal privacy interests on the other side in limiting erosion of the Fourth Amendment and arbitrary governmental interference with important privacy rights.

## II. BACKGROUND

The Fourth Amendment to the United States Constitution was enacted on September 25th, 1789, as part of the Bill of Rights, and ratified on December 15th, 1791.[26] The text of the amendment states:

> 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,

---

26. Barry Friedman & Orin Kerr, *The Fourth Amendment*, NAT'L CONSTITUTION CTR., http://constitutioncenter.org/interactive-constitution/amendments/amendment-iv (last visited Nov. 9, 2016).

> and particularly describing the place to be searched, and the persons or things to be seized.[27]

The Fourth Amendment was placed in the Constitution by our Founding Fathers and the ratifying generation in response to colonial experiences with general warrants in an era of unchecked power of the British government to "enter private homes and conduct dragnet searches for evidence of any crime."[28] In drafting the Fourth Amendment, the Founding Fathers sought to ensure the federal government lacked the power to conduct general and unreasonable searches and seizures, and so prohibited general warrants, mandated that all searches and seizures had to be reasonable, and required that only specific warrants detailing the place to be searched and the persons or things to be seized would be permitted.[29]

Over the last 224 years, the Supreme Court has sought to develop "a comprehensive set of rules regulating law enforcement" to ensure the important policies of the Fourth Amendment are preserved in modern jurisprudence.[30] Despite this dedication to preserving privacy interests, the Supreme Court has allowed for certain exceptions to the Fourth Amendment's protections including the search-incident-to-lawful-arrest exception,[31] the plain view doctrine,[32] the exigent circumstances exception,[33] and the private search doctrine,[34] among others. This article specifically relates to the private search doctrine and the permissible scope of the exception as applied to digital containers. To determine the permissible scope, we need first to understand the private search doctrine in general.

---

27. U.S. CONST. amend. IV.

28. Kerr, *supra* note 17, at 536.

29. *Id.*

30. *Id.*

31. PHILLIP A. HUBBART, MAKING SENSE OF SEARCH & SEIZURE LAW: A FOURTH AMENDMENT HANDBOOK 268 (2015).

32. *Id.* at 293.

33. *Id.* at 294.

34. *Id.* at 119–20.

The private search doctrine is based on the premise that the Fourth Amendment does not apply to actions taken by private citizens.[35] It only applies to unreasonable *governmental* searches and seizures.[36] This principle was clearly shown in *United States v. Jacobsen*.[37] *Jacobsen* presented the following issue: Is a government agent permitted to search a person's private property, without a warrant, if the government agent is told by a private individual that the property contains illegal substances, and that property has already been inspected by the private individual?[38]

In *Jacobsen*, employees of a private freight carrier observed a white, powdery substance in a package, which originally had been wrapped in multiple layers, but which had become damaged and partially opened during transit.[39] The freight carrier supervisor and employees unwrapped this package, found a tube inside made of silver tape, cut open the tube, and found a series of Ziplock bags, which all contained a white, powdery substance.[40] The supervisor notified the Drug Enforcement Administration, who sent an agent to investigate the claim.[41] Upon viewing the package, the DEA agent removed the plastic bags from the tube, observed the white, powdery substance inside, opened each of the four bags, and removed some of the substance.[42] A field test on this substance revealed that the material was cocaine.[43] Results from the field test

---

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

36. *Id.*

37. *Id.* ("This Court has also consistently construed this protection as proscribing only governmental action; 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.'").

38. *See id.* at 113.

39. *Id.* at 111.

40. *Id.*

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

42. *Id.* at 111–12.

43. *Id.* at 112.

were used to obtain a warrant to search the address where the cocaine was to be sent, and that search resulted in the arrest of the respondents on charges of possession of an illegal substance with intent to distribute.[44]

At trial, respondents moved to suppress the evidence discovered through the DEA field test and the subsequent search of the respondents's address, arguing that the DEA agent's search of the package violated the respondents's Fourth Amendment rights against unreasonable governmental search and seizure.[45] As such, any warrant obtained as a result of the initial search was "the product of an illegal search and seizure" and thus inadmissible at trial.[46] This motion was denied at the trial level but that decision was reversed on appeal.[47] The Supreme Court of the United States granted certiorari to resolve the issue and ruled in favor of the DEA, holding that "the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct."[48] The DEA search and field test was "constitutionally reasonable."[49]

*United States v. Jacobsen* was a landmark case for legal analysis under the Fourth Amendment because it conclusively established the private search doctrine.[50] The *Jacobsen* majority also defined a "search" as occurring when "an expectation of privacy that society is prepared to consider reasonable is infringed."[51] Relying on earlier precedent set in *Walter v. United States*, the majority conclusively decided that the Fourth Amendment does not apply to private action, whether or not that action is reasonable.[52] The importance of this ruling cannot be overstated; the *Jacobsen* majority

---

44. *Id.*

45. *Id.*

46. *Id.*

47. *Jacobsen*, 466 U.S. at 112.

48. *Id.* at 126.

49. *Id.*

50. *See id.* at 113; United States v. Lichtenberger, 786 F.3d 478, 481 (6th Cir. 2015).

51. *Jacobsen*, 466 U.S. at 113.

52. *Id.* (citing Walter v. United States, 447 U.S. 649, 662 (1980)).

opened the floodgates for admissibility of evidence obtained through private searches by definitively holding that such searches were not illegal.[53] To illustrate the gravity of this decision, consider the following hypothetical.

Johnny owns a computer which he regularly uses to view child pornography. One day, while Johnny is out, Jane, Johnny's girlfriend, takes his computer and discovers several files containing child pornography. Jane turns Johnny's computer into the police, who then search the files Jane discovered. Under the *Jacobsen* ruling, Johnny has no ability to argue that the government search was in violation of his Fourth Amendment rights, even though the government agents searched his personal property without first obtaining a warrant. The typical warrant requirement for government searches and seizures is extinguished in Johnny's case simply because his property was first searched by Jane. If Johnny's property had not first been searched by Jane, the government would have been required to obtain a search warrant before seizing and inspecting the computer.

What accounts for the different treatment? The *Jacobsen* majority, in defining a "search" as occurring when a person's reasonable expectation of privacy has been frustrated, by corollary, also determined when a search does not occur under the Fourth Amendment.[54] A "search," for purposes of the Fourth Amendment, does not occur when a person does not have a reasonable expectation of privacy in the property.[55] When a private individual searches a person's property, that private individual frustrates any remaining expectation of privacy in the property.[56] Therefore, any subsequent

53. *See id.*

54. *See id.* at 117.

55. *See id.*

56. *See id.*

governmental investigation of the property cannot possibly fall under the *Jacobsen* definition of a "search."[57]

Despite this permissive ruling, the *Jacobsen* majority did place restrictions on the admissibility of evidence obtained through private searches in two ways. First, the subsequent government search cannot exceed the scope of the original private search.[58] Additional invasions of a person's privacy will be tested "by the degree to which they exceed the scope of the private search."[59] Second, the private searcher cannot be an "agent" of the government nor acting at the behest of a government agent.[60] In other words, the private searcher must be truly private, and not influenced in any way by a government agent or coerced into searching the private property by a government agent or organization.[61]

These two caveats of the private search doctrine give rise to numerous qualifying questions, particularly in the advent of the digital age. It is the first caveat — the restriction that the subsequent government search cannot exceed the scope of the prior private search — that is under scrutiny in this article, and which gives rise to a current circuit split.[62] The question for consideration

---

57. *Jacobsen*, 466 U.S. at 117 ("The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated.").

58. *Id.* at 116 ("The Government may not exceed the scope of the private search unless it has the right to make an independent search.").

59. *Id.* at 115.

60. *Id.* at 113 ("This Court has also consistently construed this protection as proscribing only governmental action; 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.'" (citing Walter v. United States, 447 U.S. 649, 662 (1980)).

61. *See id.*

62. The current circuit split is between the United States Circuit Courts of Appeals for the Fifth and Seventh Circuits on the one hand, and the United States Circuit Courts of Appeals for the Sixth, Ninth (through dicta), and Eleventh Circuits on the other hand. Orin Kerr, *Sixth Circuit creates circuit split on private search doctrine for computers*, WASH. POST (May 20, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/20/sixth-circuit-creates-circuit-split-on-private-search-doctrine-for-computers/; Orin 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/.

is "What does it mean to exceed the scope of a private search of a digital device?"

## III. EXCEEDING THE SCOPE OF THE PRIVATE SEARCH: EXAMINING THE CONTAINER DISTINCTION

*United States v. Jacobsen* was decided in 1984, prior to the real emergence of the digital age.[63] In the 1980s and 1990s, cases involving the private search doctrine examined scope questions largely related to searches of physical, non-digital forms of property, not digital material.[64] Throughout these two decades, jurisprudence on the private search doctrine established the container distinction for determining when the government agent exceeded the scope of the initial private search.[65] While the container distinction is appropriate in limiting searches of physical property, its principles are unsuitable as applied to digital devices. This section will outline the container distinction as applied to traditional, non-digital forms of property and explain the suggested alternatives to applying the container distinction to digital devices, as created by Orin S. Kerr.

### A. Application of the Container Distinction to Traditional, Non-Digital Forms of Property

Traditionally, precedent regarding the Fourth Amendment has limited searches to discrete containers.[66] In the physical, non-

63. United States v. Jacobsen, 466 U.S. 109, 111 (1984).

64. *See Jacobsen*, 466 U.S. at 111 (1984) (search of wrapped package); State v. Dold, 44 Wash. App. 519, 521, 722 P.2d 1353, 1355 (Wash. Ct. App. 1986) (search of envelope); State v. Cline, 126 N.M. 77, 78, 966 P.2d 785, 786 (N.M. Ct. App. 1998) (search of zippered cosmetics pouch).

65. *See generally* HUBBART, *supra* note 31, at 340–46.

66. *See generally id.*

digital world, this distinction makes sense. A container is "an object (such as a box or can) that can hold something."[67] Courts have conclusively decided "that a person has a reasonable expectation of privacy in a container that he or she owns or possesses."[68]

As discussed in prior cases analyzing searches under the Fourth Amendment, "the opening of any closed containers . . . constitutes a separate search."[69] Traditionally, it has been very easy to determine when privacy in a physical container has been violated: if the container has been opened, with its contents laid bare for the world to see, the expectation of privacy in that container has been violated.[70] It is not until the container is opened that the person loses his or her expectation of privacy.[71]

To illustrate the physical container distinction under the private search doctrine, let's assume the private searcher comes across a metal box with a lid, opens that box, and discovers marijuana and drug paraphernalia, stacks of cash, various clothing items and a notebook containing a ledger of accounts. When the private searcher lifts the lid on the metal box, any expectation of privacy the owner possessed in that box has been extinguished. This is because simply by lifting the lid and viewing the contents of the box, it becomes clear what the box contains. The government agent can proceed to search the box with a virtual certainty of what the box will contain. The government agent knows the box will contain marijuana, drug paraphernalia, money, clothes, and a notebook, simply because that is what the private searcher informed the government agent the box would contain.

The government agent's search of the metal box does not violate the Fourth Amendment because the private searcher has already extinguished any expectation of privacy existing in the box and therefore, any subsequent search is not a "search" for purposes

---

67. *Container*, MERRIAM-WEBSTER DICTIONARY (2015), http://www.merriam-webster.com/dictionary/container.

68. HUBBART, *supra* note 31, at 341.

69. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 554 (citing United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978)).

70. *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984).

71. *See id.*

of the Fourth Amendment.[72] The reason the subsequent search is not a Fourth Amendment "search" turns on the reasoning in *Jacobsen* regarding the virtual certainty requirement. The physical container distinction works well for smaller containers, such as the metal box in the example above, because by opening the container, the private searcher and the subsequent government searcher know the contents of the container with virtual, if not absolute, certainty. However, as will be discussed in Part VI, *infra*, the physical container distinction does not apply well to larger spaces such as a shipping container or a house.[73] This has prompted the courts to apply limitations to the private search doctrine in those instances.

These limitations arguably should be applied to digital devices as well because the virtual certainty requirement cannot possibly be satisfied as applied to a digital container. It is not automatically obvious upon opening the device, what the device will contain. Therefore, the physical container distinction is inappropriate as applied to digital containers. The question then becomes what is the appropriate test in determining permissible scope of searching digital devices. Orin S. Kerr sought to create a workable standard for searching digital devices, and so created the three zone theories.[74] The rest of this section discusses the zone theories highlighted by Kerr.

### B. Application of the Container Distinction to Digital Devices: The Zone Theories

As discussed above, the container theory comports well when the property at issue is a physical, discrete receptacle; however,

---

72. *See id.*

73. *See infra* Part VI.

74. Kerr, *supra* note 17, at 554.

the container theory diverges in the digital world where the containers are not discrete objects but imaginary data.

Orin S. Kerr explains this deviation well in his article entitled *Searches and Seizures in a Digital World.*[75] Kerr suggests that applying traditional principles of searches in the physical world to the digital world can occur in accordance with three different options: (1) the zone of the initial search could be the physical storage device itself, (2) the zone of the initial search "could be defined by the contents of a virtual file," or (3) the zone of the initial search could be the exposed data.[76] Each of these individual search zones has singular implications on the scope of what a government agent is allowed to search following an initial private search under the private search doctrine. The zones will now be outlined in the order listed above.

1. The Zone is the Physical Storage Device.

The term physical storage device is somewhat confusing. It refers to a tangible storage device which stores digital data. This type of device includes, but is not limited to, computers, cell phones, SIM cards, flash drives, "floppy" disks, hard drives, and CDs. The device itself is tangible, but the data it contains is intangible.

Under the "zone is the device" theory, the digital search is not limited to files, folders, or exposed data.[77] The physical storage device is the container, and the search of any information stored upon the device is permissible so long as the device itself has already been opened.[78] For purposes of the private search doctrine this means if the private actor simply opened the device, even if he or she only viewed a single unit of data on the device, any subsequent search of the device's entire data does not constitute an impermissible search under the Fourth Amendment.[79] If the physical storage device is a computer, all the private searcher need do is open

---

75. *Id.*

76. *Id.*

77. *See id.* at 554–55.

78. *See id.* at 555 (citing United States v. Runyan, 275 F.3d 449, 452–53 (5th Cir. 2001)).

79. *See id.*

and turn on the computer and view any file on the device.[80] If the physical storage device is a SIM card, flash drive, "floppy disk," hard drive, or CD, all the private searcher need do is insert that device into a computer (or other instrument capable of reading the contents of the storage device), open it so that its contents are capable of being viewed, and view a single unit of data on the device.[81]

If the search zone is defined as the device itself, opening the device and accessing just one file means the private searcher has searched the entire contents of the device and frustrated any privacy expectation of the device itself.[82] This means any subsequent searches, even if not of the specific images or files originally searched by the private actor, do not exceed the scope of the private search doctrine.[83] This zone definition is clearly the most permissive of the three. The next most permissive zone definition is the "zone is the virtual folder" distinction.

### 2. The Zone is the Virtual File

Under the "zone is the virtual file" distinction, the digital search is limited to a virtual file, and only that virtual file.[84] This file could be a document, image, or PDF for example. The file is the container for all intents and purposes. Opening the file means you have frustrated any expectation of privacy that existed within the file.[85]

A good example of the virtual file approach exists in *United States v. Lichtenberger*. As will be discussed *infra*, *Lichtenberger*

---

80. *See* Kerr, *supra note* 17, at 555.

81. *See id.*

82. *See id.*

83. *See id.*

84. *See id.* at 554–55.

85. *See id.*

involved a private search of the suspect's computer, which was determined to contain images of child pornography.[86] Although the private searcher, in this case the suspect's girlfriend, viewed images of child pornography on the device, upon turning the device over to law enforcement, the girlfriend was unable to say with certainty that the specific images she showed to the law enforcement agent were the same images she viewed during her private search.[87] As a result, the Sixth Circuit determined the subsequent government search exceeded the scope of the private search.[88] The court reasoned the agent's viewing of additional files than those viewed during the private search was an impermissible extension of the private search because the suspect retained an expectation of privacy in the images not searched by the girlfriend.[89] In so holding, the court created precedent for later courts to apply the "zone is the virtual file" distinction.

The "zone is the virtual file" distinction is more restrictive than the "zone is the digital device" approach because it does not allow the government agent to search the entire device; rather, this approach limits the government agent to only searching the specific images or files already viewed by the private searcher.[90] The virtual file distinction is, however, less restrictive than the "zone is the exposed data" approach because it allows the government agent to search the entire file or image and does not require the agent to limit his search to only the data shown on the output screen.[91]

### 3. The Zone is the Exposed Data

The last zone theory is the most restrictive of the three, and has not been adopted in any court to date. The "zone is the exposed data" theory limits the scope of the search to the information appearing on the output device (computer screen, cell phone screen,

---

86. 86 F.3d 478, 480–81 (6th Cir. 2015).

87. *Id.* at 481.

88. *Id.* at 485.

89. *Id.*

90. *See* Kerr, *supra* note 17, at 554–56.

91. *See id.* at 555–57.

printer, etc.).[92] The exposed data could be an individual image, an individual document, or even smaller subsets of these items such as a single page or part of a page within a document.[93] The officers conducting the subsequent search of the device are limited to viewing specifically what the private searcher viewed down to the minute details of the data.[94]

For example, if Sally views a document on Jeff's computer that she believes contains evidence of Jeff's fraudulent business transactions, but Sally only views the first page of that document before handing the computer in to the FBI, the FBI agents investigating her tip are limited to viewing only the first page of the document Sally opened. These agents may not view any other page in this document, nor can they view any other image, document, file, or folder stored on the device itself. Under the "zone is the exposed data" approach, even scrolling down to see a different part of the same word processing file searched by the private actor constitutes a separate search under the Fourth Amendment, and if the officers did not first obtain a search warrant to do so, the search is in violation of the device owner's Fourth Amendment rights.[95]

The "zone is the virtual file" approach does not require this limitation and permits the agent to search the entire document. The "zone is the virtual file" approach, therefore, is a happy medium between the three approaches outlined by Orin S. Kerr. As will be discussed *infra*, the virtual file approach is the approach that should be adopted in every private search doctrine case involving searches of digital containers. This approach adequately balances the competing policy interests at stake and ensures the unwavering protection of Fourth Amendment rights.

---

92. *Id.* at 556–57.

93. *Id.*

94. *Id.*

95. *Id.* at 557.

Although Kerr, the creator of the zone approaches, advocates for the exposed data approach,[96] no court to date has adopted such a restrictive distinction. The courts that have addressed this issue are instead in contention over the first two approaches: the digital device approach and the virtual file approach.[97] The next section of this comment will discuss the differing opinions regarding the proper approach to take in limiting the government search, specifically discussing the major cases on each side of the divide.

## IV. APPLYING THE CONTAINER DISTINCTION IN THE DIGITAL WORLD: EXPLAINING THE CIRCUIT SPLIT

As mentioned above, the various United States Circuit Courts of Appeals are split on the issue of limiting the scope of the subsequent government search following the initial private search.[98] The United States Circuit Courts of Appeals for the Fifth and Seventh Circuits hold with the "zone is the device" theory and define the container as the physical storage device itself.[99] For these two circuits, as long as the subsequent governmental search is confined to only the digital devices already opened by the private searcher, the governmental search is permissible.[100]

The United States Circuit Courts of Appeals for the Sixth and Eleventh Circuits, on the other hand, hold with a theory limiting the search to the virtual file.[101] The United States Circuit Court of Appeals for the Ninth Circuit arguably aligns with this approach

---

96. Kerr, *supra* note 17, at 556 ("the better answer is to use the exposed information as the common denominator. The scope of a computer search should be whatever information appears on the output device . . .").

97. United States v. Sparks, 806 F.3d 1323, 1330 (11th Cir. 2015) (cell phone); United States v. Lichtenberger, 786 F.3d 478, 479 (6th Cir. 2015) (computer); United States v. Tosti, 733 F.3d 816, 818 (9th Cir. 2013) (computer); Rann v. Atchison, 689 F.3d 832, 833 (7th Cir. 2012) (ZIP drive and camera memory card); United States v. Runyan, 275 F.3d 449, 452 (5th Cir. 2001) (ZIP disks).

98. *See Sparks*, 806 F.3d at 1330; *Lichtenberger*, 786 F.3d at 479; *Tosti*, 733 F.3d at 818; *Rann*, 689 F.3d at 833; *Runyan*, 275 F.3d at 452.

99. *See Runyan*, 275 F.3d at 452; *Rann*, 689 F.3d at 837.

100. *See Runyan*, 275 F.3d at 452; *Rann*, 689 F.3d at 837.

101. *See Lichtenberger*, 786 F.3d at 488; *Sparks*, 806 F.3d at 1336.

as well, as discussed in dicta in *United States v. Tosti*.[102] These circuits hold that the permissible container is the individual image, document, file, etc.[103] Within this restriction, the government agent is allowed to open and view the document, image, or file already seen by the private searcher, but is not allowed to open or view any other document, image, or file not already seen.[104] These circuits adopt a middle-ground approach to defining the scope and adequately balance the competing interests of furthering governmental investigation and protecting the privacy interests of citizens. As will become clear *infra*, this approach is the correct approach.

The leading cases holding for the "zone is the virtual file" approach are *United States v. Lichtenberger* and *United States v. Sparks*, and through dicta, *United States v. Tosti*. The leading cases holding for the "zone is the digital device" approach are *United States v. Runyan*, and *Rann v. Atchison*. The latter cases will be discussed first.

### A. The View of the Fifth and Seventh Circuits: The Container Should be the Physical Storage Device

The Fifth and Seventh Circuits hold in favor of limiting the scope of the government search, following the private search, to the physical storage device itself.[105] This means that if the private searcher views even one image or file on the digital storage device, the device owner's privacy interest in that device is frustrated.[106] Therefore, any subsequent search of the device does not exceed the scope of the private search, even if the subsequent search views additional, unviewed files and images.[107] The first case to hold in favor of this approach was *United States v. Runyan*, a 2001 case

---

102. *See Tosti*, 733 F.3d at 822.

103. *See Runyan*, 275 F.3d at 452; *Rann*, 689 F.3d at 837.

104. *See Runyan*, 275 F.3d at 452; *Rann*, 689 F.3d at 837.

105. *Runyan*, 275 F.3d at 452; *Rann*, 689 F.3d at 833.

106. *See Runyan*, 275 F.3d at 452; *Rann*, 689 F.3d at 833.

107. *See Runyan*, 275 F.3d at 452; *Rann*, 689 F.3d at 833.

published long before the Supreme Court addressed the unique privacy interests at stake in digital devices in *Riley v. California*.[108]

### 1. *United States v. Runyan*

*United States v. Runyan* established the "zone is the digital device" approach.[109] The situation giving rise to the Fifth Circuit's adoption of this approach was as follows: the defendant's ex-wife confiscated a desktop computer and several floppy disks, ZIP disks, and CDS.[110] After discovering that these devices contained images of child pornography, she turned the evidence over to the police.[111] The ex-wife only viewed some of the floppy disks and CDS, but did not view any of the ZIP disks.[112] Law enforcement agents "examined several images from each disk and CD, including the ZIP disks."[113] Based on the results of this investigation "Runyan was indicted on six counts of child pornography charges."[114]

Following his arrest, Runyan moved to suppress all of the evidence obtained against him, arguing that the warrantless searches of the disks were conducted in violation of the Fourth Amendment and therefore, any evidence obtained through these illegal searches had to be suppressed.[115] Runyan argued the government search exceeded the private search because state and federal officials examined the ZIP disks, even though Runyan's ex-wife had not.[116] He also argued that agents "examined more images in reviewing each of these disks than did the private searchers."[117]

---

108. *Runyan*, 275 F.3d at 452.

109. *See id.*

110. *Id.* at 453.

111. *Id.*

112. *Id.*

113. *Id.* at 454

114. *Runyan*, 275 F.3d at 455.

115. *Id.*

116. *Id.* at 460.

117. *Id.*

The issue before the Fifth Circuit was whether a police search exceeds the scope of the private search when the police examine more items within a particular container than did the private searchers.[118] In answering this question, the Fifth Circuit highlighted key language in *United States v. Jacobsen* — "the critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which the defendant's expectation of privacy has not already been frustrated."[119] The Court relied on the reasoning in *Jacobsen* which concluded that a police search is not problematic under the Fourth Amendment if the police "actions 'enabled . . . [them] to learn nothing that had not previously been learned during the private search.'"[120] The police had to be substantially certain of what the container would hold.[121] The police could become substantially certain of the container's contents "based on the statements of the private searchers, their replication of the private search, and their expertise."[122] Based on this reasoning, the Fifth Circuit determined that the police search did, in fact, exceed the scope of the private search because the defendant's ex-wife did not search the ZIP disks at all.[123] Runyan's reasonable expectation of privacy in the ZIP disks, therefore, still existed.[124]

The pertinent part of *Runyan*, for purposes of investigating the digital container distinction, concerns the second argument given by the defendant — that the government search exceeded the scope of the private search doctrine because the police "examined

---

118. *Id.* at 456.

119. *Id.* at 461.

120. *Runyan*, 275 F.3d at 463 (quoting United States v. Jacobsen, 446 U.S. 109, 120 (1984)).

121. *Id.*

122. *Id.*

123. *Id.* at 464 ("Indeed, [Judith] could not have known the contents of any of the ZIP disks, as she and Brandie did not use hardware capable of reading these disks in their private search.").

124. *Id.*

more files on each of the disks than did the private searchers."[125] In response, the Fifth Circuit held that there was no constitutional issue when police examined more files than did the private searcher.[126] The Fifth Circuit followed precedent established by *United States v. Simpson*[127] which held law enforcement agents "do not exceed the scope of a prior private search when they examine the same materials that were examined by the private searchers, but they examine these materials more thoroughly than did the private parties."[128] The reason for this exception is the simple fact that the individual's expectation of privacy in his property has already been frustrated by the private searcher; therefore, any subsequent viewing of the container's contents by the police does not constitute a "new 'search' for Fourth Amendment purposes."[129]

In essence, although not explicitly stated, the *Runyan* court viewed the "container," for purposes of the private search doctrine, as the physical storage device itself, in this case CDs and a computer.[130] Once the defendant's privacy interest has been frustrated in the container, anything on the device is fair game for police investigation and can be used as evidence to obtain a warrant or to arrest the defendant.[131]

The Fifth Circuit identified the following policy reasons for its liberal definition of "container." Using a "zone is the exposed data" or "zone is the file" approach would prevent the police from "engaging in lawful investigation of containers where any reasonable expectation of privacy has already been eroded."[132] This would be a waste of time and resources.[133] Also, police would waste time and resources attempting to obtain warrants based on the testimony of

---

125. *Id.*

126. *Runyan*, 275 F.3d at 465.

127. United States v. Simpson, 904 F.2d 607, 610 (11th Cir. 1990).

128. *Runyan*, 275 F.3d at 464 (citing *Simpson*, 904 F.2d at 610).

129. *Id.* at 465.

130. *See id.* at 463–65.

131. *See id.*

132. *Id.* at 465.

133. *Id.*

private searchers, which may or may not be reliable.[134] An approach that does not allow the police to search the whole container following the private searcher's opening of that container might:

> . . . lead police to waste valuable time and resources obtaining warrants based on intentionally false or misleading testimony of private searchers, for fear that, in confirming the private testimony before obtaining a warrant, they would inadvertently violate the Fourth Amendment if they happened upon additional contraband that the private searchers did not see.[135]

The key takeaway from the Fifth Circuit's reasoning in *Runyan* is, for the sake of judicial expediency and conservation of law enforcement resources, police should be able to examine containers already searched by private individuals, even to a greater degree and intensity than previously executed.[136] After all, the property owner's expectation of privacy has already been frustrated anyway.[137] Government agents do not exceed the scope of the private search when they view additional files on a device that has already been searched by the private individual, but they do exceed the scope of the private search if they view additional devices not viewed by the private individual prior to the government search.[138] This train of reasoning can also be found in a 7th Circuit case, *Rann v. Atchison*.[139]

### 2. *Rann v. Atchison*

*Rann v. Atchison* is the most recent case holding in favor of the "zone is the digital device" approach. The Seventh Circuit was

---

134. *Runyan*, 275 F.3d at 465.

135. *Id.*

136. *See id.*

137. *Id.*

138. *Id.*

139. Rann v. Atchison, 689 F.3d 832, 833 (7th Cir. 2012).

called upon to decide if the police's viewing of images not viewed by the private searcher was a "significant expansion of a private search such that a warrant was required to permit police to view the images."[140] The court ultimately concluded, following the Fifth Circuit's reasoning in *Runyan*, the government search did not exceed the private search.[141]

Steven Rann was convicted, in November 2006, of criminal sexual assault and possession of child pornography.[142] Rann's daughter reported him for sexual assault and turned in to the police, a digital camera memory card and a computer zip drive.[143] Rann argued that when police searched the submitted devices and viewed images stored upon them, they exceeded the scope of any private search previously conducted by the private party.[144] Rann based this argument on the fact that no evidence was submitted showing that the private party had previously viewed the devices, nor that she "knew the digital storage devices contained images of child pornography prior to the police viewing."[145] Without this certainty, Rann contended, "police needed a warrant to 'open' the digital storage devices and search them . . .."[146] Without a warrant, the police search violated Rann's Fourth Amendment rights and any evidence obtained through the illegal search should be suppressed.[147]

Citing *Jacobsen* and *Runyan*, the court in *Rann* held police did not exceed the scope of the private search when they searched the disks.[148] The officers in charge of this case could have been substantially certain, based on statements made by the private

---

140. *Id.* at 835.

141. *Id.* at 838.

142. *Id.* at 833.

143. *Id.* at 834.

144. *Id.* at 836.

145. *Rann*, 689 F.3d at 836.

146. *Id.*

147. *Id.*

148. *Id.* at 837.

searcher, what the disks contained.[149] Additionally, the *Rann* court commented that "even if the police more thoroughly searched the digital media devices . . . the police search did not exceed or expand the scope of the initial private searches."[150] Once it could be determined that the reasonable expectation of privacy in the devices was frustrated by the private party, any evidence contained within the device was fair game for investigation.[151]

Again, the *Rann* court viewed the "zone is the device" theory as the sensible approach when determining what it means to exceed the scope of the private search because the approach allegedly "preserves the competing objectives underlying the Fourth Amendment's protections against warrantless police searches."[152] The "zone is the device" theory keeps intact the defendant's reasonably legitimate expectation of privacy until such time as that expectation of privacy is frustrated by the private search.[153] When the frustration occurs, the additional invasions of privacy are still tested in regards to the degree by which they exceed the scope of the private search.[154] However, the "zone is the device" theory also proceeds from the assumption that warrants are costly and time consuming for police to obtain.[155] If the police are reasonably certain of what information the device will contain, based on the private search and their own expertise, and the suspect's privacy has already been violated, what is the harm in viewing additional files?[156]

As will be discussed in Part VI, *infra*, the reasoning supporting the *Rann* court's decision to support the "zone is the digital device" approach is flawed.[157] Warrants are not that costly and they are

149. *Id.*

150. *Id.* at 838.

151. *See Rann*, 689 F.3d at 838.

152. *Id.* at 837.

153. *Id.*

154. *Id.*

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

156. *See id.*

157. *See infra* Part VI.

much easier to obtain in the digital age. Additionally, the unique characteristics of digital devices, specifically the immense storage capabilities and the discrete types of information contained on these devices, requires a much more restrictive approach to defining the permissible scope of the government search. This restrictive approach can be seen in the post-*Riley* cases of *United States v. Lichtenberger* and *United States v. Sparks* in the Sixth and Eleventh Circuits, respectively, and the pre-*Riley* case of *United States v. Tosti* in the Ninth Circuit. The next section of this comment will discuss these cases in depth.

### B. The View of the Sixth, Ninth, and Eleventh Circuits: The Container Should be the Virtual File

The position of the Fifth and Seventh Circuits described above is flatly rejected by the United States Circuit Courts of Appeals for the Sixth and Eleventh Circuits.[158] These courts believe the "zone is the device" theory exposes criminal defendants to too much arbitrary governmental intrusion.[159] Instead, these circuits believe the proper theory defining the scope of the private search should be the "zone is the virtual file" approach.[160] The first circuit to hold in favor of the "zone is the virtual file" approach was the Sixth Circuit in *United States v. Lichtenberger*.[161]

#### 1. *United States v. Lichtenberger*

In *United States v. Lichtenberger*, the United States Circuit Court of Appeals for the Sixth Circuit decided against the persuasive trend set by the Fifth and Seventh Circuits, holding that individual files and images are separate "containers" and therefore, a subsequent government search of a digital storage device is limited to the individual files and images viewed by the private searcher.[162] Authorities arrested Aron Lichtenberger after his girlfriend discovered images of child pornography on his laptop and showed

158. *See* United States v. Lichtenberger, 786 F.3d 478, 479 (6th Cir. 2015); United States v. Sparks, 806 F.3d 1323, 1333 (11th Cir. 2015).

159. *See Lichtenberger*, 786 F.3d at 479; *Sparks*, 806 F.3d at 1333.

160. *See Lichtenberger*, 786 F.3d at 479; *Sparks*, 806 F.3d at 1333.

161. *Lichtenberger*, 786 F.3d at 485.

162. *Id.* at 490–91.

some of the images to the police.[163] Lichtenberger was charged with possession of child pornography; "before trial, Lichtenberger filed a motion to suppress the laptop evidence, which the district court granted."[164]

The district court granted Lichtenberger's motion to suppress based on testimony from his girlfriend in which she admitted to viewing "approximately 100 images of child pornography saved in several subfolders inside a folder entitled 'private.'"[165] Lichtenberger's girlfriend could not identify which photographs she eventually presented to authorities, and could not say with certainty whether the images she presented to authorities were the exact images she viewed during her private search of Lichtenberger's computer.[166] The district court ruled authorities exceeded the scope of the private search because they viewed additional images not already seen through the private search.[167] The Sixth Circuit rejected the government's appeal.[168]

Relying on *United States v. Jacobsen*, the court determined that a government actor exceeds the scope of the private search when he or she frustrates an expectation of privacy within the property that had not already been frustrated by the private actor.[169] Pronouncing a largely political argument for its decision, the Sixth Circuit held the scope of the authorities' "search of Lichtenberger's laptop exceeded that of Holmes' private search conducted

---

163. *Id.* at 479.

164. *Id.* at 480.

165. *Id.* at 481.

166. *Id.*

167. *See Lichtenberger*, 786 F.3d at 481.

168. *Id.*

169. *Id.* at 485 (citing United States v. Jacobsen, 446 U.S. 109, 117–18 (1984)) ("The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated. In such a case the authorities have not relied on what is in effect a private search, and therefore presumptively violate the Fourth Amendment if they act without a warrant.").

earlier that day."[170] The court discussed what it termed the "critical measures" under the private search doctrine in regards to the scope of a permissible government search.[171] These "critical measures" were: (1) how much information authorities were exposed to upon re-examination of the device and (2) the certainty of the authorities regarding what they would likely find upon the device.[172]

Adopting reasoning from the Supreme Court's recent decision in *Riley v. California*, the court determined it would be inappropriate to rely upon the traditional principles regarding searches of physical spaces and the items they contained in the context of digital spaces.[173] The Sixth Circuit's main reasoning for breaking from tradition was due to the immense storage capacity of modern digital devices.[174] As the court noted, "the likelihood that an electronic device will contain 1) many kinds of data, 2) in vast amounts, and 3) corresponding to a long swath of time, convinced the *Riley* court that officers must obtain a warrant before searching such a device incident to arrest."[175] That reasoning, in the eyes of the Sixth Circuit, applied just as convincingly to the private search doctrine as it did to the search incident to arrest exception.[176]

The privacy interest in Lichtenberger's property greatly outweighed any governmental interest in conducting the search.[177] The fundamental reason for this tip in the balance came down to virtual certainty, or lack thereof.[178] As required by *Jacobsen*, in order to stay within the scope of the private search, local authorities have to proceed with virtual certainty that they would not learn

---

170. *Id.* at 485.

171. *Id.*

172. *Id.* at 485–86.

173. *Lichtenberger*, 786 F.3d at 487.

174. *Id.*

175. *Id.* at 488 (citing Riley v. California, 134 S. Ct. 2473, 2489 (2014)).

176. *Id.* at 488.

177. *Id.*

178. *Id.*

any new, private information from their subsequent search.[179] Virtual certainty is an impossibility with digital devices due to their unique capabilities.[180]

As the court discussed, the government's search of Lichtenberger's laptop could have revealed staggering amounts of Lichtenberger's private information "unrelated to the allegations prompting the search."[181] For example, the folders containing the images of child pornography just as easily could have contained "explicit photos of Lichtenberger himself," "bank statements or personal communications," "Lichtenberger's medical history," or even "his choice of restaurant."[182] These potential intrusions into Lichtenberger's private life could not possibly be justified, especially considering the governmental search lacked any of the "risks that support an immediate search."[183] The authorities' safety was not threatened, Lichtenberger had already been arrested so "the images were not in danger of erasure, deterioration, or tampering," and "the need to confirm the laptop's contents on-site was not immediate."[184] Due to "the strong privacy interests at stake, and the absence of threat to government interests," the Sixth Circuit concluded that the authorities' search of Lichtenberger's laptop did, in fact, violate Lichtenberger's Fourth Amendment rights against warrantless searches.[185] In doing so, the Sixth Circuit established conclusively that a government search which follows a private

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

180. *See id.* at 488–89.

181. *Id.* at 489.

182. *Id.*

183. *Id.* at 491.

184. *Id.*

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

search exceeds the scope of the private search when the government searcher views additional files or images not viewed by the private actor.[186]

In reaching its conclusion, the Sixth Circuit relied in part on reasoning established by the United States Court of Appeals for the Ninth Circuit in *United States v. Tosti*.[187]

### 2. *United States v. Tosti*

Although *United States v. Tosti* did not conclusively decide that the "zone is the virtual file" approach is the correct approach when determining permissible scope, the court in this case did, through dicta, give the impression that it determined the proper approach is the virtual file approach.[188] The police arrested the defendant, Donald Thomas Tosti, after a computer technician at a CompUSA store discovered child pornography in a sub-folder on Tosti's computer.[189] At trial, Tosti moved to suppress the evidence obtained through the government's search of his computer at the CompUSA store,[190] arguing the search exceeded the scope of the private search because detectives viewed enlarged photographs in a slideshow format and scrolled through the thumbnail images, whereas the computer technician who conducted the initial search only viewed the thumbnail versions of the photos.[191] The district court and the Ninth Circuit agreed that Tosti was not entitled to suppression on either of these bases.[192]

The Ninth Circuit reasoned that pursuant to *Jacobsen* precedent, the government search does not constitute a "search" for Fourth Amendment purposes if the reasonable expectation of privacy in the property has already been extinguished by a private

---

186. *Id.*

187. United States v. Tosti, 733 F.3d 816, 821 (9th Cir. 2013).

188. *Id.* at 818.

189. *Id.* at 818–19.

190. *Id.* at 820.

191. *Id.* at 821–22.

192. *Id.* at 822.

party.[193] Scrolling through thumbnail photographs, which have already been exposed in their thumbnail form to a private actor, and enlarging those photographs does not constitute an additional invasion of privacy.[194] Even though he only viewed the photos in thumbnail form, the computer technician extinguished any reasonable expectation of privacy Tosti had in the images.[195]

Central to our discussion on the permissible scope of subsequent government searches of digital storage devices is the Ninth Circuit's reasoning in relation to what the government agents did not do when they searched Tosti's computer. As the court noted in *Tosti*, detectives did not view photos not already seen by the computer technician.[196] Likewise, "there was 'no evidence in the record to suggest that either [d]etective . . . viewed any file folder or images other than the file folder and images opened by [the technician]." [197] This explicit statement by the court in support of its finding that the detectives did not exceed the scope of the private search in this case seems to indicate that had the detectives viewed additional files on the device, the government search would have exceeded the private search. Additional support for this analysis comes from the fact that the Sixth Circuit, in deciding *United States v. Lichtenberger*, supported its decision by reference to the reasoning pronounced above by the Ninth Circuit in *Tosti*.[198] Therefore, it is reasonable to conclude that on the issue of permissible scope in warrantless searches of digital storage devices, the Ninth Circuit holds in favor of the virtual file theory.

193. *Tosti*, 733 F.3d at 821.

194. *Id.* at 822.

195. *Id.*

196. *Id.*

197. *Id.*

198. *Lichtenberger*, 786 F.3d at 490 (citing *Tosti*, 733 F.3d at 822).

The most recent decision weighing on this issue at the circuit court level is *United States v. Sparks*,[199] an Eleventh Circuit case decided December 1, 2015.[200]

### 3. *United States v. Sparks*

*United States v. Sparks* tasked the Eleventh Circuit with deciding what was a permissible warrantless search of a cell phone under the private search doctrine.[201] Similar to the cases coming before it, *United States v. Sparks* was an appeal from convictions for possession and production of child pornography.[202] Defendants Alan Robert Johnson and Jennifer A. Sparks left a cell phone containing hundreds of images and videos of child pornography at a Walmart in Cape Coral, Florida.[203] A Walmart employee showed the images on the cell phone to her husband, Widner, who brought the phone to the local authorities.[204] Upon searching the phone, the local authorities viewed several images and two videos, one which was previously watched by Widner and one that had not been viewed during the private search.[205]

Johnson and Sparks argued, in their respective motions to suppress, that the authorities's viewing of the second unwatched video constituted an expansion of Widner's private search; and therefore, a violation of their Fourth Amendment rights against unreasonable governmental search and seizure.[206] The Eleventh Circuit agreed on this point.[207] The court expressed "serious doubts that approving of the viewing of the second video when no private

199. United States v. Sparks, 806 F.3d 1323, 1330 (11th Cir. 2015).

200. *Id.*

201. *Id.*

202. *Id.* at 1330–31.

203. *Id.* at 1329.

204. *Id.* at 1331.

205. *Sparks*, 806 F.3d at 1332.

206. *Id.* at 1333.

207. *See id.* at 1335.

party had first watched it would be consistent with the reasoning in *Riley v. California*."[208]

In light of the privacy concerns unique to digital devices, Widner's private search of the cell phone could not possibly have extinguished all reasonable expectation of privacy in the device itself.[209] The court stated:

> While Widner's private search of the cell phone might have removed certain information from the Fourth Amendment's protections, it did not expose every part of the information contained in the cell phone. Here, no search warrant was obtained, and no exception to the search-warrant requirement excused [the detective's] viewing of the second video.[210]

Hence, the Eleventh Circuit in *United States v. Sparks*, further strengthened the support for a determination of permissible scope based on the actual images and files viewed by the private actor.[211] In doing so, the court relied significantly on the reasoning espoused in *Riley v. California*.[212] The Supreme Court's reasoning in *Riley* lays the foundation for limiting searches of digital devices. The next part of this article discusses the *Riley* decision, highlighting Chief Justice Roberts's analysis regarding the unique peculiarities of digital devices and the importance of protecting personal privacy.

## V. THE LEGACY OF *RILEY V. CALIFORNIA*: ADVOCATING FOR LIMITED GOVERNMENT INTRUSION ON PERSONAL PRIVACY RIGHTS IN DIGITAL DEVICES

---

208. *Id.* at 1336.

209. *See id.*

210. *Id.*

211. *See Sparks*, 806 F.3d at 1336.

212. *Id.*

*Riley v. California* was not a case involving the private search doctrine; rather, it dealt with the application of the Fourth Amendment to digital devices through the search-incident-to-arrest exception.[213] Despite the fact that *Riley* concerned a different Fourth Amendment exception, the policy reasoning encouraging digital device search limitations and the Court's discussion of the privacy interests at stake informs our current issue. For that reason, this section will give an overview of the discussion in *Riley*, highlighting specific points discussed by Chief Justice Roberts concerning the proliferation and unique attributes of digital devices and the importance of limiting warrantless access to these devices.

The search-incident-to-arrest exception essentially allows "the Government . . . to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crimes."[214] This exception is certainly different from the private search doctrine because it involves actions initiated by government agents, not private individuals, and it exists primarily to recognize "concerns for officer safety and evidence preservation."[215] However, the two exceptions are similar in that they concern the reasonableness of warrantless searches. It is the reasonableness point that was at issue in *Riley*[216] and that is at issue in our discussion of private search doctrine cases. Therefore, the Court's reasoning in *Riley* is informative of how the Court likely would and should define the scope of a permissible subsequent search of a digital device by a government agent in private search doctrine cases.

Chief Justice Roberts began by examining the singular characteristics of modern digital devices (particularly cellular "smart" phones).[217] In the words of Chief Justice Roberts, "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[218] Roberts noted that even

---

213. Riley v. California, 134 S. Ct. 2473, 2482 (2014).

214. *Id.*

215. *Id.* at 2484.

216. *Id.* at 2482.

217 . *Id.* at 2484.

218. *Id.*

less sophisticated phones, which are increasingly becoming obsolete, are "based on technology nearly inconceivable just a few decades ago."[219] Denouncing the United States's argument "that a search of all data stored on a cell phone is 'materially indistinguishable' from searches of these sorts of physical items." Roberts pronounced that modern devices, as a whole, "implicate privacy concerns far beyond those implicated by the search of [a physical container]."[220]

Cell phones contain immense storage capacity.[221] The standard model of the top-selling smart phone, at the time of the *Riley* decision, was sixteen (16) gigabytes.[222] "Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos."[223] Additionally, cell phones have the capability of storing many distinct types of information, such as "photographs, picture messages, text messages, internet browsing history, a calendar, a thousand-entry phone book, and so on."[224]

Chief Justice Roberts highlighted four interrelated consequences on personal privacy as a result of the increasing storage capacity of cell phones (as well as other digital devices).[225] First, a cell phone is a repository for numerous distinct forms of information, including but not limited to notes, addresses, prescriptions, videos, and bank or credit statements, which may "reveal much more in combination than any isolated record."[226] Second:

> A cell phone's capacity allows even just one type of information to convey far more than previously possible. The

---

219. *Riley*, 134 S. Ct. at 2484.

220. *Id.* at 2488–89.

221. *Id.* at 2489.

222. *Id.*

223. *Id.*

224. *Id.*

225. *Riley*, 134 S. Ct. at 2489–90.

226. *Id.* at 2489.

> sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.[227]

Third, unless the device's owner sets the device to automatically delete information after a certain period of time, devices accumulate unending stores of information, which "can date back to the purchase of the [device], or even earlier."[228] It is not uncommon for individuals to retain the same device for years at a time before upgrading to a new model, which means that a person's communication with people in his life can be recorded and stored for weeks, months, or years.[229] In contrast, a person is very unlikely to record all the face-to-face conversations he has with others and take those communications with him wherever he goes.[230] Finally, cell phone use is exceedingly pervasive.[231] "Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day."[232] "Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception."[233] Roberts highlighted a further complication on the scope of the privacy interests at stake by noting the existence of cloud computing, "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself."[234] The existence of cloud computing creates the issue that the government agent's search is not limited to just what is on the device.[235]

The above policy implications convinced the Supreme Court to significantly limit warrantless searches of digital devices, even if

---

227. *Id.*

228. *Id.*

229. *See id.* at 2489–91

230. *Id.*

231. *Riley*, 134 S. Ct. at 2490.

232. *Id.*

233. *Id.*

234. *Id.* at 2491.

235. *Id.*

conducted through a legitimate exception to the Fourth Amendment.[236] Chief Justice Roberts concluded his opinion with the recognition that the Court's decision would have a great "impact on the ability of law enforcement to combat crime."[237] Roberts recognized that cell phones (and other digital devices) "have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals."[238] Roberts noted, however, that "[p]rivacy comes at a cost,"[239] and if the police want to search the digital device, they can, but first, they *must* obtain a warrant.[240]

The conclusion that police should be able to search an entire digital device following the private search is quite clearly at odds with the Supreme Court's current view of privacy rights in digital devices. As the following section will make clear, it is the virtual file approach, not the digital device approach, that preserves the privacy protections our Founders fought so hard to obtain, and for that reason, it is the correct approach for all courts in this nation to adopt.

## VI. WHY LIMITING THE SCOPE OF THE PERMISSIBLE GOVERNMENTAL SEARCH TO THE INDIVIDUAL IMAGE OR FILE IS THE CORRECT APPROACH: ANALYZING THE POLICY INTERESTS AT STAKE

As *Lichtenberger*, *Tosti*, and *Sparks* make clear, applying the traditional test for determining what it means to exceed the scope of a private search, as applied to physical, tangible containers, is inappropriate for outlining a permissible search of a digital container. Digital containers differ from physical containers in marked ways. This point was evidenced in the Supreme Court's decision in *Riley v. California*, discussed in the previous section. Although the government has expressed some important policy

236. *See id.* at 2492–95.

237. *Riley*, 134 S. Ct. at 2493.

238. *Id.*

239. *Id.*

240. *Id.*

reasons, such as the danger of evidence destruction and the considerable resources expended to obtain search warrants, these reasons are substantially outweighed by: (1) the intent of the Founding Fathers and the ratifying generation in passing the Fourth Amendment, (2) the nature and pervasive use of digital devices themselves, and (3) the impossibility of virtual certainty regarding the contents of digital containers. This section will consider the main arguments posed by the Fifth and Seventh Circuits in support of the digital device approach and explain why these arguments are flawed. Then, this section will discuss the main arguments in favor of the virtual file approach, and ultimately conclude that these arguments prevail.

### A. The Arguments for Adopting the Digital Device Approach & Why Such a Permissive Approach is Unwarranted

As outlined above, the primary reasons extended by the Fifth Circuit in *United States v. Runyan* to support it's holding in favor of the "zone is the digital device" approach included the unnecessary and significant judicial costs in obtaining warrants and the fact that the government agent could already be virtually certain of what the device contained due to the description of the contents by the private searcher.[241] Another argument that could arguably be extended in favor of adopting the "zone is the digital device" approach is to prevent destruction of evidence through modern data destruction techniques. These arguments will be discussed in this section, and ultimately rejected.

#### 1. Preventing Destruction of Evidence

One argument that could be extended in support of allowing the government agent to search the entire digital device, even if the private searcher did not do so, is the danger that, through modern data destruction technologies, the pertinent evidence of criminal activity might be deleted from the device prior to the government agent's being able to obtain a warrant. This is a potential problem because in many of the cases involving the private search doctrine, the private searcher personally knows the owner of the property.[242] The personal relationship between the private

241. *See supra* Part IV.A.1.

242. United States v. Runyan, 275 F.3d 449, 452 (5th Cir. 2001) (private searcher was the defendant's ex-wife); United States v. Lichtenberger, 786 F.3d 478, 480 (6th Cir. 2015) (private searcher was defendant's girlfriend); Rann v. Atchison, 689 F.3d 832, 834 (7th Cir.

searcher and the alleged criminal/owner of the property can have problematic consequences on the government's search of the property. If the private searcher tips off the suspect, even unintentionally, as to the government confiscation of property, prior to the government agent being able to obtain a warrant to search the rest of the device, the suspect could wipe the device or encrypt it so the data cannot be accessed.[243] This is a process known as remote wiping.[244]

Remote wiping is "a security feature that allows a network administrator or device owner to send a command to a computing device and delete data."[245] If a computer or other device is connected to the Internet and the device's owner is sophisticated enough in computer technology, the owner could remotely access the computer with the object of removing any incriminating data upon the device before that data could be used against the owner.[246] "A remote wipe may delete data in selected folders, repeatedly overwrite stored data to prevent forensic recovery, return the device to factory settings or remove all programming on the device, essentially turning it into a brick, meaning that it is no longer of any use to anyone."[247]

According to an article published by CNN, remote wiping technology will become a standard addition to all phones produced by

---

2012) (private searcher was defendant's biological daughter and the daughter's mother); United States v. Tosti, 733 F.3d 816, 819 (9th Cir. 2013) (additional documents, hard drives, a computer, and DVDs were turned over to police by defendant's estranged wife); United States v. Wicks, 73 MJ 93, 96 (C.A.A.F. 2014) (private searcher was a former friend of the defendant with whom he had a "personal relationship"); People v. Wilkinson, 78 Cal. Rptr. 3d 501, 505–06 (Cal. Ct. App. 2008) (private searcher was a friend and housemate of defendant).

243. Zack Whittaker, *Smartphones 'remotely wiped' in police custody, as encryption vs. law enforcement heats up*, ZD NET (Oct. 9, 2014), http://www.zdnet.com/article/smartphones-remotely-wiped-in-police-custody-as-encryption-vs-law-enforcement-heats-up/.

244. *Id.*

245. Margaret Rouse, *Remote Wipe*, TECHTARGET (last visited Oct. 26, 2016), http://searchmobilecomputing.techtarget.com/definition/remote-wipe.

246. *See id.*

247. *Id.*

major players in the mobile phone world.[248] "Apple, Google, Samsung and Microsoft, along with the five biggest cellular carriers in the United States, are among those that have signed on to a voluntary program."[249] This voluntary program requires all smartphones manufactured in the United States after July 2015 to have remote wiping technology.[250] The feature is designed to deter smartphone theft, a growing problem in the United States, but it has the added consequence of allowing users to remotely wipe their digital devices should those devices fall into the wrong hands, even the hands of law enforcement.[251] The "kill switch" would allow device owners to "erase contacts, photos, e-mail and other information, and lock the phone so it can't be used without a password."[252]

Remote wiping is a particular problem in the time period after the private actor has turned the device into the police and the police have verified that the device contains criminal material but before the police are able to obtain a search warrant to view the rest of the device's contents. During that limbo period, the device owner could, theoretically, remotely wipe the device and destroy any evidence of criminal or illegal activity. This exact problem has occurred in the United Kingdom.[253]

In 2014, British police forces encountered at least six individual instances of smartphones being remotely wiped after being seized by police.[254] This remote wiping activity purportedly destroyed "vital evidence as part of ongoing investigations."[255] It does not take a long amount of time to send a signal to the mobile device so "even that short period of time after a device has been seized can

---

248. Doug Gross, *'Kill Switch' may be standard on U.S. phones in 2015*, CNN (Apr. 16, 2014), http://www.cnn.com/2014/04/16/tech/mobile/ctia-phone-kill-switch/.

249. *Id.*

250. *Id.*

251. *Id.*

252. *Id.*

253. Whittaker, *supra* note 243.

254. *Id.*

255. *Id.*

be enough to send through a remotely-activated data kill switch."[256] There does not seem to be any evidence of police forces in the United States encountering the same issues as British police forces, but as time goes on, the potential problems created by remote wiping technology could increase as people, especially those with something to hide, become more aware of the technology and well versed in its applications.

Another potential technological advancement that could contribute to the destruction of evidence in pre-warrant situations is a process known as geofencing. Geofencing is a subset of remote wiping; it is a process by which a device is "configured to automatically wipe all data when the GPS in the device determines that it has left (or entered) a specific predetermined geographic area. This method may also employ WiFi towers for location determination as well."[257] Theoretically, geofencing technology could be used by criminals to lock down and/or remotely wipe digital devices that come within a certain distance to a police station. In that sense, if the police confiscate the device from the private searcher and take that device to their headquarters, the act of entering the predetermined GPS coordinates could trigger the digital device to destroy its contents.

The technologies of remote wiping and geofencing could lend support to the "zone is the physical device" theory supported by the Fifth and Seventh Circuits. One could argue that the government should be able to view the entire contents of a digital device for evidence of criminal activity if there is a substantial risk of those contents being erased before the government can obtain a search warrant. If the device is erased before the search warrant is granted, the government is effectively unable to prosecute individuals for criminal activity, despite strong evidence of illegal actions.[258]

---

256. *Id.*

257. RICK AYERS, SAM BROTHERS, & WAYNE JANSEN, NAT'L INST. OF STANDARDS & TECH, GUIDELINES ON MOBILE DEVICE FORENSICS 30 (2014), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.

258. *See generally* Riley v. California, 134 S. Ct. 2473, 2486 (2014).

This argument is almost flatly rejected by the Supreme Court in *Riley v. California*.[259] As Chief Justice Roberts pointed out, in his *Riley* opinion, law enforcement has means to address the problem of remote wiping.[260] For example, officers could simply turn the phone or other device off or remove the device's battery so it cannot connect to a network.[261] Additionally, David Bennett suggests two other ways officers could ensure the device is unable to be remotely accessed: use of a Faraday bag and use of a radio frequency shielded test enclosure box.[262]

A Faraday bag is a plastic-coated, radio frequency (RF) shielded bag "used to shield a mobile device from external contact."[263] If the device is placed in a Faraday bag, it cannot reach a wireless signal, thereby making remote wiping or geofencing an impossibility as long as the device remains in the bag.[264] A radio frequency shielded test enclosure box is similar to the Faraday bag in that it isolates the device from the cellular network.[265] This prevents communication with the device, including GPS communication.[266]

In addition to the use of practical, network limiting technologies, there exists a judicial remedy to allow government agents to conduct searches if they have a reasonable fear of destruction of

---

259. *Id.* at 2487.

260. *Id.*

261. *Id.*

262. David W. Bennett, *The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations*, FORENSIC FOCUS (Aug. 22, 2011), https://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/.

263. *Id.*

264. *Id.*

265. *Id.*

266. *Id.*

evidence.[267] This remedy is known as a search under exigent circumstances, also known as the exigency doctrine.[268] The exigency doctrine, as applied to Fourth Amendment searches and seizures, allows the needs of law enforcement to compel a warrantless search based on objectively reasonable determinations.[269] An objectively reasonable determination could be found in cases where there is a need to prevent the imminent destruction of evidence.[270] Government agents, in such a situation, are justified in circumventing the Fourth Amendment "by the existence of exigent circumstances [requiring] the officer to act immediately without [a] warrant or consent."[271]

The exigency doctrine is not a savings provision; it is very much the exception to the general rule.[272] In the typical case, government agents will not be justified by the exigency doctrine in searching the entire device. Government agents should only be permitted to invoke the exigency doctrine when there is a real danger that the evidence contained on the device will be imminently destroyed before the agents can obtain a warrant to search the entire device. Only in these situations will it be objectively reasonable for the government agents to be permitted to violate the suspect's Fourth Amendment rights. While destruction of evidence in specific cases may support a finding of exigency, it should not do so categorically, and the prevailing test for determining permissible scope should be the "zone is the virtual file" approach.

Even though it is important for government agents to be permitted to search devices for incriminating material, government agents should not be permitted to circumvent well-established Fourth Amendment jurisprudence to do so. With the use of technologies such as the Faraday bag, increased governmental intrusion in regards to permitting law enforcement to search an entire

---

267. 68 AM. JUR. 2D *Searches and Seizures* § 133 (2016).

268. *Id.*

269. *See* Missouri v. McNeely, 133 S. Ct. 1552 (2013).

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

271. State v. David, 269 Ga. 533, 535, 501 S.E.2d 494, 497 (1998).

272. *See McNeely*, 133 S. Ct. at 1556.

digital device in excess of a private search is not justified. Law enforcement agencies have the capabilities to preserve digital evidence until warrants can be obtained; therefore, these agencies should not be permitted to trample upon defendants' Fourth Amendment rights. Even in situations where law enforcement agencies may lack such technologies as Faraday bags or radio frequency shielded test enclosure boxes, they can always simply power down the device so it cannot connect to a WiFi or cellular network. Additionally, in very rare circumstances, the exigency doctrine exists to save vital evidence from the risk of true destruction. With these alternatives, adoption of the "zone is the digital device" theory is unnecessary.

2. Avoiding Unnecessary Judicial and Law Enforcement Costs

Another argument in support of allowing government law enforcement agencies to search the whole digital device as permitted by the Fifth and Seventh Circuits is the idea that requiring a warrant to search devices for which the expectation of privacy has arguably already been frustrated by the private actor and which contain criminal activity is a waste of judicial time and resources.[273] In essence, this argument pronounces that law enforcement agents should be able to view the entire contents of the device because they can be virtually certain that the device contains criminal activity. This virtual certainty is accomplished by the fact that the law enforcement agents have already viewed illegal activity on the device, the evidence offered by the private actor.

This argument is flawed for the following reasons. First, as will be discussed in the next section, the unique characteristics of digital devices make the virtual certainty requirement of *Jacobsen* a pragmatic impossibility. Even if agents could be certain that the device contains images of child pornography or evidence of financial fraud, for example, the agents could not be certain of what else the device could contain. Digital devices have immense storage capacity and the capability of holding numerous discrete forms of information. The only virtual certainty an agent could possibly have in the digital device is that the specific file or image viewed contains illegal activity. This virtual certainty only exists in the specific file or image viewed. It does not exist for the rest of the device.

---

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

Second, while the resources of law enforcement agencies and the judiciary are of important consideration, concerns of depleting resources should not be enough to overcome the strong constitutional protections of the Fourth Amendment. The Fifth Circuit reasons, in *United States v. Runyan*, that warrants are costly and time consuming to obtain.[274] While this may have been true when *Runyan* was decided in 2001, the Supreme Court case of *Missouri v. McNeely*,[275] makes clear that technological advancements in the warrant application process have made obtaining warrants quicker and much less costly.[276] As amended, the Federal Rules of Criminal Procedure allow warrants to be issued by telephone or other electronic means.[277] Additionally, "well over a majority of States allow police officers or prosecutors to apply for search warrants remotely through various means, including telephonic or radio communication, electronic communication such as e-mail, and video conferencing."[278] States have also streamlined the warrant process by using standard forms for certain applications.[279]

While telecommunications innovations have not, by any means, "eliminate[d] all delay from the warrant-application process,"[280] they have enabled law enforcement agents to obtain warrants through a quicker and more streamlined process.[281] For that reason, the argument in favor of allowing law enforcement agents the ability to search the whole device fails. The unique characteristics of digital devices and the inherent potential for abuse in allowing law enforcement wide discretion and latitude counsel against the adoption of the "zone is the digital device" theory. Only the "zone is the virtual file" approach accurately and adequately

---

274. *See id.*

275. Missouri v. McNeely, 133 S. Ct. 1552 (2013).

276. *Id.* at 1561–62.

277. *Id.* at 1562.

278. *Id.*

279. *Id.*

280. *Id.*

281. *McNeely*, 133 S. Ct. at 1562.

takes into account the competing interests at stake in digital device searches.

### B. The Arguments for Adopting the Virtual File Approach & Why Such a Limited Approach is Desirable

The virtual file theory acknowledges technological advancements in digital devices, advancements in the jurisprudential system and the unwavering intent of the Founding Fathers in passing the Fourth Amendment. For that reason, it is the proper approach to be taken in determining permissible scope. This section will discuss the important policy arguments in support of the virtual file approach.

#### 1. The Intent of the Founding Fathers and the Ratifying Generation in the Passage of the Fourth Amendment

The "zone is the virtual file" approach adopted by the Sixth and Eleventh Circuits comports most accurately and completely with the intent of the Founding Fathers in the passage of the Fourth Amendment. This section will give some historical background on the passage of the Fourth Amendment, specifically showing how the Fourth Amendment was passed to ensure adequate safeguards were implemented to prevent the creation of a police state. It will also discuss how allowing the "zone is the digital device" approach is contrary to the intentions of the Founding Fathers, which were to require specificity and concrete limitations to unchecked and arbitrary governmental intrusion on private citizen life.

The Fourth Amendment was placed in the Constitution by our Founding Fathers and the ratifying generation in response to the fear of allowing searches and seizures of a person's property and home without probable cause.[282] In Great Britain, in the early to mid 1700s, searches without probable cause were commonplace, and "general warrants allowed the Crown's messengers to search without any cause to believe someone had committed an offense."[283] Perhaps the most prolific example of the unchecked power of the British government to invade the privacy of its citizens through general warrants was the case of John Wilkes, a member of the

---

282. Friedman & Kerr, *supra* note 26.

283. *Id.*

British Parliament and staunch critic of the expansive and unbridled policies of the government.[284]

In 1762, Wilkes published an anonymous series of pamphlets which criticized the search and seizure policies of the British government.[285] Embittered with the constant and increasingly adverse critique of its administration, the British government launched an attack against the authors of these pamphlets, the identities of whom were unknown by the government at the time.[286] The Secretary of State, Lord Halifax, issued a general warrant of arrest to four individuals, "ordering them to make strict and diligent search for the authors, printers, and publishers of a seditious and treasonable paper . . . and them, or any of them, having found, to apprehend and seize, together with their papers."[287]

The problem with this warrant was its lack of specificity.[288] As discussed by Nelson B. Lasson in his book examining the early background development of the Fourth Amendment, Halifax's warrant was so general "as to the persons to be arrested and the places to be searched and the papers to be seized" that "probable cause upon oath could necessarily have no place in it since the very questions as to whom the messengers should arrest, where they should search, and what they should seize, were given over into their absolute discretion."[289]

Imbued with the authority of the general warrant, the four messengers proceeded to arrest forty-nine individuals in three days upon simple suspicion of seditious activity, oftentimes taking individuals from their beds during the night.[290] After apprehending

---

284. LASSON, *supra* note 6, at 43.

285. *Id.* at 43 n.108.

286. *Id.* at 43.

287. *Id.*

288. *Id.*

289. *Id.*

290. LASSON, *supra* note 6, at 43.

the actual printer of the pamphlets, the messengers learned that Wilkes was the author, arrested him, and removed all of Wilkes's private papers from his home.[291] Wilkes and the other printers arrested brought suit against the British government for false imprisonment.[292] Chief Justice Pratt declared the general warrant to be illegal and a gross abuse of power by the Secretary of State.[293] The Chief Justice stated:

> The defendants claimed a right under precedents to force persons' houses, break open escritoires, seize their papers, upon a general warrant, where no inventory is made of the things taken away, and where no offenders' names are specified in the warrant, and therefore a discretionary power given to messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in a secretary of state, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject.[294]

In the aftermath of the American revolution, the newly independent Americans decided to break from British tradition and placed "the right against unreasonable search and seizure on a constitutional footing."[295] The many state constitutions in the emerging United States of America not only disallowed general warrants; "they also elevated specific warrants, probable cause, and the idea of unreasonable search and seizure to the position of higher law."[296] With the memory of the *Wilkes* case and the language of thirteen state constitutions in mind, Congress passed the Fourth Amendment as part of the Bill of Rights on September 25th, 1789.[297] The

---

291. *Id.* at 44.

292. *Id.*

293. *Id.* at 44–45.

294. *Id.* at 45.

295. WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING 603 (Oxford University Press, 2009).

296. *Id.*

297. Friedman & Kerr, *supra* note 26.

ultimate goal of the Fourth Amendment is to "protect people's right to privacy and freedom from arbitrary governmental intrusions."[298] This goal reflects the familiar maxim that "a man's home is his castle," and "makes plain . . . that the Constitution does not tolerate the tactics of a police state."[299]

The history and jurisprudence of the Fourth Amendment inform this issue of permissible scope of the subsequent government search in at least a couple ways. First, connections can be made between a digital storage device and a house, such that the special protections regarding "a man's castle" and the unique limitations of the private search doctrine as applied to residences work to limit the permissible scope of the subsequent government search to the virtual files searched by the private actor. Second, the prohibition against general warrants discussed above and the unwavering desire for specificity in Fourth Amendment applications mandate a virtual file approach and reject the digital device approach.

a. Similarities Between Digital Devices and Houses

A digital storage device is not unlike a house. In essence, a digital storage device contains many of the same things as a house might contain – photos, cameras, videos, video players, libraries, diaries, albums, televisions, maps, newspapers, etc. A digital storage device is essentially a house for your consciousness; it stores many of your thoughts, your concerns, your dreams, and your doubts. It can very well be described as a "sanctuary" for those thoughts, and as such is deserving of special protection.

In Fourth Amendment jurisprudence, the house has received such special protection.[300] "Indeed, the physical entry into the home has been described as the 'chief evil against which the wording of

298. *Fourth Amendment: An Overview*, L.L.I., https://www.law.cornell.edu/wex/Fourth_amendment (last visited Nov. 9, 2016).

299. Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 197 (1993).

300. THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATIONS 122–23 (Carolina Academic Press 2008).

the Fourth Amendment is directed.'"[301] It has been pronounced that "a sane, decent, civilized society must provide some such oasis, some shelter from public scrutiny, some insulated enclosure, some enclave, some inviolate place which is a man's castle."[302]

The home receives special protection as well under the private search doctrine. As the Sixth Circuit decided in *United States v. Allen*,[303] the private search doctrine does not apply to searches of residences.[304] A person's expectation of privacy is not extinguished if a private actor searches the person's residence.[305] The person still has an expectation of privacy in the *contents* of his residence.[306] If a government agent, upon information from the private searcher, opens containers within the home not opened by the private searcher, the government agent has violated the person's Fourth Amendment rights.[307] Simply by searching the house generally, the private actor does not destroy the expectation of privacy specifically.[308]

The residence protection applies well to the subject of digital storage devices. As discussed above, digital storage devices are sufficiently similar to houses to be subject to the same Fourth Amendment policy protections. In fact, Chief Justice Roberts in his *Riley* opinion noted this very problem and said:

> Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[309]

---

301. *Id.* at 123.

302. *Id.* at 122.

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

304. *Id.* at 699.

305. *Id.*

306. *Id.*

307. *See id.*

308. *See id.*

309. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

In applying the principles regarding physical searches of residences to digital containers, it becomes clear that the proper approach to determining the scope of a permissible governmental search is the virtual file approach. In essence, the digital device is the home and any file, image, or document contained upon the device can be analogized to a box or container within the home. In order to open additional files, images, or documents on the device, those files, images, or documents must first have been opened by the private actor. As the world becomes increasingly digital, with more and more activity done online rather than in reality, this comparison only becomes more concrete.

b. The Prohibition Against Lack of Specificity Mandates a Virtual File Approach.

As the *Wilkes* case, discussed *supra*, makes clear, specificity in warrant applications and in searches and seizures is a must, not a suggestion. The Supreme Court in *Jacobsen* picked up on this mandate of specificity in its requirement of virtual certainty in application of the private search doctrine. But, as will be discussed *infra*, is it even possible to have virtual certainty regarding the contents of a digital device, without first searching every last piece of data on the device?

Digital devices have an inherent lack of specificity in regards to knowing the contents of the device and being able to pinpoint with virtual certainty the allegedly criminal material. It is very improbable that a person's entire digital device will only contain criminal material. It is much more likely that the device will contain anything and everything from pictures to e-books, videos to addresses, medical records to diary entries. As *Jacobsen* pronounced, the critical measures in determining whether the government search exceeds the scope of the private search are how much private information the government stands to gain when it re-examines the evidence and how certain it is regarding what it will find.[310]

If the government agent is permitted to use the "zone is the digital device" approach, the agent stands to gain every piece of

310. United States v. Jacobsen, 466 U.S. 109, 119–20 (1984).

information ever viewed or downloaded on the device. The government agent cannot possibly be certain that every piece of information on the device will contain criminal material. The government agent cannot even be *virtually* certain that every piece of information on the device will contain criminal material. For that reason, the "zone is the digital device" theory goes against every limitation in *Jacobsen* and against everything the Fourth Amendment was passed to prevent. Permitting the government agent to search every file, image, or document on a suspect's private device, without first obtaining a warrant, is akin to allowing government agents to ransack every container within a person's home for evidence of alleged criminal activity, an action clearly outlawed by the *Wilkes* decision and numerous decisions following.

Chief Justice Pratt, in the quoted language discussed *supra*, established that to allow a government agent to search wherever his "suspicions may chance to fall" would be to allow an act so subversive to liberty that it would go against every protection we have against unreasonable search and seizure.[311] The digital device approach allows the government agent to search the entire device, wherever his suspicions may chance to fall. Only the virtual file approach and the exposed data approach impose limitations on this broad and virtually unchecked power. Of course, it becomes a different question when the government agent has obtained a warrant and is searching a digital device upon the authority of that warrant. In that case, as long as the warrant is specific and lawful, the reasons for limiting government searches of digital devices become less convincing. In private search doctrine cases, however, the government agents are proceeding without a warrant; as such, their actions in searching digital devices should be limited.

Warrants present limitations on the power of law enforcement. When abolishing the warrant requirement, the judiciary should be very careful to preserve the important privacy interests of citizens. To allow the agents to search the whole device, without a warrant, simply because a private actor viewed one, single file on the device is to provide too broad a license of investigation and suspicion. The virtual file approach presents a needed limitation on the powers of law enforcement, and thus should be the approach adopted in private search doctrine cases where the evidence at issue is a digital device.

---

311. *See* LASSON, *supra* note 6, at 45.

### 2. The Nature and Pervasive Use of Digital Devices

Digital devices present unique attributes that distinguish them from physical containers. Cell phones (and other digital devices) have immense storage capacity. Cell phones, alone, can act as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[312] Before the advent of modern digital devices, a search was limited by the fact that most people couldn't, and even if they could likely wouldn't, carry "every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read . . . ."[313] Digital devices make this physical impossibility not only possible but also quite probable and make prior search limitations inapplicable. The resulting possible intrusion on privacy interests for digital devices is not physically limited in the same way a possible intrusion on privacy interests for physical devices is.

As Chief Justice Roberts pointed out in *Riley*, "the current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos."[314] Even basic phones without such capacity have the ability to hold text and picture messages, a person's calendar and schedule, thousands of personal contacts, photographs, and for those phones with network capabilities, an Internet browsing history.[315]

In the short time since *Riley* was passed, the computer technology market has expanded even further than sixteen gigabyte standard models. In fact, Samsung is introducing a sixteen *terabyte*

---

312. *Riley v. California*, 134 S. Ct. at 2489.

313. *Id.*

314. *Id.*

315. *Id.*

model to the consumer hard drive market sometime in 2016.[316] Sixteen terabytes translates to roughly 272,000 hours of music, 16,000 hours of video, or 4,960,000 photos.[317] With the constantly changing nature of the digital technology market, it is not inconceivable to conclude that this storage capacity will continue to increase for years to come.

The problem is compounded when you consider the pervasiveness of digital devices. Cell phones, and other devices "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy. A smart phone . . . was unheard of ten years ago; a significant majority . . . now own such phones."[318] In fact, a study conducted in 2015 regarding smartphone usage in the United States revealed that "64% of American adults own a smartphone of some kind."[319] The percentage increases to 85% among young adults.[320]

Especially concerning for our purposes is the quality of the information accessed on digital devices. Smartphones are much more than the typical telephone of yesteryear in that they are used for more than just to call and text people.[321] According to the PEW Research Center survey, a significant number of adult smartphone owners used their phones during the year to "look up information about a health condition" (62%), participate in online banking (57%), "look up real estate listings" (44%), search for job information (43%), search for government services (40%), "take a class or get educational content" (30%), and submit job applications

316. Will Nicol, *Expand Your Digital Vault With These 5 High-Capacity Hard Drives*, DIGITAL TRENDS (Sept. 27, 2015), http://www.digitaltrends.com/computing/highest-capacity-hard-drives.

317. *See* Melvin Foo, *How much can a 1 TB external hard drive hold?*, PC NINJA (Feb. 8, 2012), http://www.pcninja.us/how-much-can-a-1-tb-external-hard-drive-hold.

318. *Riley v. California*, 134 S. Ct. at 2484.

319. Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RESEARCH CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015.

320. *Id.*

321. *Id.*

(18%).[322] These percentages increase among young adult smartphone owners.[323]

If the pervasiveness and quality of usage regarding digital storage devices is not enough to convince of the need to limit governmental power to search digital devices, it is worth noting that digital devices present the added problem of connectivity to the cloud, as noted *infra* in our discussion of *Riley v. California*. As the Ninth Circuit noted in *United States v. Cotterman*, digital devices are "conduit[s] to retrieving information from the cloud, akin to the key to a safe deposit box."[324] Just by having access to the digital device itself, a person has access to every account and offsite store of information a person possesses. With that in mind it is difficult to argue that allowing law enforcement access to the whole digital device is not an abuse of discretion and in direct violation of everything for which the Fourth Amendment stands.

### 3. The Impossibility of "Virtual Certainty" Regarding the Contents of Digital Containers

Due to the unique characteristics of digital devices, it is virtually impossible for law enforcement to be sufficiently certain of what they will find upon the digital device. For that reason, searches of the whole digital device cannot satisfy the "virtual certainty" requirement of *Jacobsen*. Digital device searches "tend to be unusually invasive."[325] Digital evidence, likewise, often can reveal so much more evidence, in both quality and quantity, than physical evidence.[326] When one opens a physical container, the contents inside are fixed, meaning just by viewing the inside of the container, you can know with "virtual certainty" what that container will hold. The same cannot be said of a digital container.

When one opens a digital folder on a computer, it is not immediately obvious what that folder contains. A private actor could

---

322. *Id.*

323. *Id.*

324. United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013).

325. Kerr, *supra* note 15, at 569.

326. *Id.*

open the folder and find evidence of child pornography through images and videos. However, unless the private actor views every single data file in that folder, the folder's contents are still a mystery. The only thing the private actor knows with certainty is that the opened images and videos contain child pornography.

When the private actor then replicates the search for the government agent, the government agent is limited to the level of certainty the private actor had. The agent does not gain additional certainty regarding the contents of the container just by his or her expertise. The risk that the government agent, if allowed to search the whole folder, or the whole device, will find private information for which the expectation of privacy has not been frustrated is too great to allow such latitude. The subsequent government search cannot possibly satisfy the "virtual certainty" requirement of *Jacobsen*, and therefore, the subsequent search exceeds the scope of the private search and is impermissible without a warrant.

The foregoing policy discussion strongly mandates a finding that the only permissible search technique to be used in private search doctrine cases of digital devices is the virtual file approach. In this sense, the Sixth, Ninth, and Eleventh Circuits have it correct. These circuits see that the virtual file approach is the only approach that adequately and unwaveringly preserves the purpose of the Fourth Amendment and ensures we, as a nation, remain free from arbitrary governmental intrusion.

## VII. CONCLUSION

As this comment makes evident, there are many dangers in allowing a subsequent government search, following a private search, to view the whole contents of a digital storage device. For that reason, the proper approach to determining the scope of the subsequent government search should be that of the Sixth, Ninth, and Eleventh Circuits, finding that the government search is limited in scope to the individual images or files viewed by the private actor. This approach preserves the reasonable expectation of privacy that device owners have in their property, furthers the goals of the Fourth Amendment, and prevents abuse of discretion by law enforcement officers.