Phone Sweet Phone: The Future of the Private Search Doctrine Following *Riley v. California*

Isabella Blizard[*]

TABLE OF CONTENTS

* J.D. Candidate, University of the Pacific, McGeorge School of Law, 2018; B.S., California State University, Sacramento, 2015. I would like to extend my profound thanks to Professor Stephen Cody, whose enthusiasm bolstered the creation of this Comment. I would also like to thank my Primary Editor Rosie Deck, and the *University of the Pacific Law Review* Volumes 48 and 49 Board of Editors. Especially, I would like to thank my dad, sister, and fiancé for their open ears and never-ending support.

I. INTRODUCTION

Two roommates, Geoffrey and Nicholas, rented property from their landlord, Theresa Smith.[1] One month, their landlord noticed the water bill was higher than usual, and so she went to investigate the properties she owned.[2] Theresa thought there was probably just a water leak.[3] She approached the property rented by Geoffrey and Nicholas and used her own key to enter their residence.[4] Theresa noticed contraband inside, so she decided to contact the authorities.[5] After that, she allowed a law enforcement officer to enter the residence without a warrant.[6] Neither Geoffrey nor Nicholas were home during either entry to protest.[7] If the officer viewed only what Theresa described, the search would likely be lawful under the private search doctrine.[8] This is an example of how the private search doctrine works.[9] Now imagine what someone could do with the password to another person's computer or cell phone.[10]

Under the private search doctrine, when a private party violates a person's privacy by conducting a search, a government official can follow-up that search and conduct one of their own without a warrant, so long as the second search

1. United States v. Williams, 354 F.3d 497, 499 (6th Cir. 2003).

2. *Id.* at 499–500.

3. *Id.* at 500.

4. *Id.*

5. *Id.*

6. *Id.* at 501, 510.

7. *Id.* at 500.

8. These facts are from United States v. Williams, 354 F.3d 497, 501, 510 (6th Cir. 2003). Although some circuits hold the private search doctrine applies to residences and some do not, *see infra* Part VIII, this particular case held the private search did not justify the warrantless entry because the officer's search exceeded the scope of the landlord's. *Id.* at 510.

9. *Infra* Part II.

10. *See, e.g.*, United States v. Sparks (Johnson), 806 F.3d 1323 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 2009, 195 L. Ed. 2d 222 (2016), *and cert. denied sub nom.* Johnson v. United States, 137 S. Ct. 34, 196 L. Ed. 2d 46 (2016) (law enforcement officer searched a cell phone under the private search doctrine). References to cell phones and modern cell phones in this Comment are references to "smart phones" specifically—smart phones are small, lightweight, minicomputers with many uses. *What Are the Different Types of Computer?*, REFERENCE.COM, https://www.reference.com/technology/different-types-computer-7c93526a14be5dcf (on file with *The University of the Pacific Law Review*).

does not exceed the scope of the first.[11] The Supreme Court of the United States created the private search doctrine in 1984 in *U.S. v. Jacobsen*, where it held that because a private party frustrated the privacy interests of the defendant, the government actor was free to view the contents because it no longer constituted an unreasonable search.[12] When applied to digital devices, the doctrine had been used broadly—allowing police to search any files on a zip drive, for example, simply because a private party knew what was on it.[13] But in recent years, courts have been in disagreement about the scope of this doctrine due to the influential decision *Riley v. California*.[14]

Riley explained that modern cell phones "hold for many Americans 'the privacies of life.'"[15] They have the capacity to store many different types of information, from photographs to Internet browsing history.[16] They can contain many sensitive records and even private information that cannot be found in a home.[17] The use of cell phones is now so pervasive that "the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[18] This concept has led recent courts to favor the individual's privacy interests in digital devices and narrow the scope of the private search doctrine when it comes to searching them.[19]

The Sixth Circuit adopted a narrow scope of the private search doctrine in *United States v. Lichtenberger*, following the Eleventh Circuit's decision in *Johnson v. United States*.[20] The policy under *Riley v. California* that cell phones are as private as the home under the Fourth Amendment shows that courts are not only correct in narrowing the doctrine, but that cell phones and similar digital devices should be exempt from the private search doctrine altogether.[21]

This Comment first explains the private search doctrine and its origins.[22] It then explains the two private search cases applying the doctrine to digital

---

11. Stephen LaBrecque, *"Virtual Certainty" in a Digital World: The Sixth Circuit's Application of the Private Search Doctrine to Digital Storage Devices in United States v. Lichtenberger*, 57 B.C. L. REV. E-SUPPLEMENT 177, 181 (2016).

12. 466 U.S. 109, 119 (1984).

13. *See* Rann v. Atchison, 689 F.3d 832 (7th Cir. 2012) (the mother brought a zip drive to the police, claiming she reviewed its contents and knew it contained child pornography).

14. *See* Riley v. California, 134 S. Ct. 2473 (2014); United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015).

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

16. *Id.* at 2489.

17. *Id.* at 2491.

18. *Id.* at 2484.

19. *See* United States v. Lichtenberger, 786 F.3d 478, 487–488 (6th Cir. 2015) (noting the *Riley* decision's analysis of phones adds weight to one side of the scale when balancing individual and state interests).

20. *Id.* at 488.

21. *See Riley*, 134 S. Ct. at 2491 (comparing privacy interests in phones to a home).

22. *See infra* Part II.

devices, *Rann* and *Runyan*.[23] Then, this Comment dives into the case *Riley v. California*, and explains the ripple effect *Riley* created on legal treatment of technology.[24] Next, this Comment shows the emerging circuit splits following the *Riley* decision, created by *Lichtenberger* and *Johnson* in their narrowing of the private search doctrine.[25] This Comment shows that the emerging policy protecting technology from government searches is likely to influence future courts in continuing to narrow the doctrine.[26] Finally, it argues that because of the high privacy interests in cellphones, as the *Riley* court explained, cellphones and similar technology should be exempt from the private search doctrine altogether.[27]

II. THE PRIVATE SEARCH DOCTRINE

The Fourth Amendment to the United States Constitution protects against unreasonable searches of peoples' "persons, houses, papers, and effects."[28] Under that amendment, the government may only search by first obtaining a warrant.[29] But government agents are able to avoid the warrant requirement in special cases through the "private search doctrine," as created by *U.S. v. Jacobsen*,[30] where, after a search by a private party, a replicated warrantless search by a government agent is not an unreasonable search under the Fourth Amendment.[31] This Part explains the *U.S. v. Jacobsen* decision, which is the basis for the private search doctrine.[32] Then, it describes the policies underlying the doctrine.[33]

In *U.S. v. Jacobsen*, the private freight carrier Federal Express had accidentally damaged a package with a forklift, and pursuant to company policy, employees opened the package to examine its contents.[34] Upon inspection, the Federal Express employees observed a series of zip-lock bags containing white powder and contacted the Drug Enforcement Administration.[35] The federal agent saw the same white powder in the package and opened the bags, identifying the substance as cocaine.[36] The agents rewrapped the package and obtained a warrant

23. *See infra* Part III.
24. *See infra* Part IV.
25. *See infra* Part V.
26. *See infra* Part VI.
27. *See infra* Part VII.
28. U.S. CONST. amend IV.
29. *Id.*
30. 466 U.S. 109, 117 (1984).
31. *Id.* at 117–19.
32. *Infra* Part II.
33. *Infra* Part II.
34. 466 U.S. 109, 111 (1984).
35. *Id.*
36. *Id.* at 111–12.

to search the place to which it was addressed, eventually arresting and charging the respondents in that case.[37] The issue before the court was whether the Fourth Amendment required the federal agent to obtain a warrant before he opened the bag and tested the cocaine.[38]

The *Jacobsen* Court held that the removal and inspection of the substance within the plastic bags in the damaged package infringed no legitimate expectation of privacy, and therefore did not constitute a "search" within the meaning of the Fourth Amendment.[39]

In its holding, the Court in *Jacobsen* reasoned that the Fourth Amendment is implicated only if the authorities use information that has not already frustrated the respondent's expectation of privacy.[40] However, the expectation of privacy in that case had already been frustrated by the Federal Express employees when they inspected the package, and so the court held the respondents had no privacy interest in the contents of the package once unsealed and examined by the employees.[41] "The agent's viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment."[42]

In assessing whether the actual testing of the cocaine was a search, the court reasoned that the suspicious nature of the material made it *virtually certain* the substance tested was in fact contraband.[43] Therefore, the Court reasoned, the safeguards of a warrant could at best only minimally advance Fourth Amendment interests because the trace amount of material lost to the drug test has a de minimis impact on any property interest.[44]

Since the search of a private party frustrated the expectation of privacy of the respondent, and the testing of the cocaine was such a minimal impact on any property interest, the agent's search did not infringe on Fourth Amendment protections.[45]

The policies underlying the private search doctrine originated both from *Jacobsen*, and from an earlier case, *Burdeau v. McDowell*.[46] Decided in the early 1900s, *Burdeau* analyzed what constitutional protections individuals are entitled to under the language of the Fourth Amendment.[47] The United States Supreme

37. *Id.* at 112.

38. *Id.* at 111.

39. *Id.* at 119.

40. *Id.* at 117.

41. *Id.* at 119, 121.

42. *Id.* at 119.

43. *Id.* at 125 (emphasis added).

44. *Id.*

45. *Id.* at 119, 125.

46. 256 U.S. 465 (1921); *After Riley, Circuits Narrow Private Search Doctrine*, LAW360 (Jan. 11, 2016, 11:15 AM), http://www.law360.com/articles/743564/after-riley-circuits-narrow-private-search-doctrine (on file with *The University of the Pacific Law Review*).

47. Burdeau v. McDowell, 256 U.S. 465, 474 (1921).

Court explained both the history and origin of the Fourth Amendment to show the framers created the Amendment as a restraint on sovereign authority.[48] Therefore, the Fourth Amendment protects against government action, not private action, even if the private action is unlawful.[49] Under this reasoning, once a party's expectation of privacy is frustrated by a private search, the government is not barred by the Fourth Amendment from using the then non-private information.[50] Together, *Burdeau v. McDowell*'s policy and the *U.S. v. Jacobsen* decision created the private search doctrine.[51]

III. THE PRIVATE SEARCH DOCTRINE AS APPLIED TO DIGITAL DEVICES

Within private search doctrine jurisprudence, there are two notable cases that applied the private search doctrine to digital devices, which provided an example for other courts on how the doctrine could be applied to these types of devices.[52] The first of these cases to apply the doctrine was in the Fifth Circuit,[53] and the second was in the Seventh Circuit, which adopted the approach used by the Fifth.[54] This Part illustrates these two cases.[55]

In *United States v. Runyan*, the defendant's wife turned over a complete collection of disks, alleging that she found child pornography on some of them.[56] The Fifth Circuit held that the police exceeded the scope of the initial search because they were not "substantially certain that all of the disks contained child pornography."[57] The Fifth Circuit created its "substantial certainty" guideline, analogizing electronic devices to physical containers, in hopes that police will not engage in "'fishing expeditions' by opening closed containers."[58] Notably, the Fifth Circuit also held that the government was able to search the contents of an electronic device once a private party viewed at least one file.[59] The Court

48. *Id.* at 475.

49. *Id.*; *see also* Walter v. United States, 447 U.S. 649, 656 (1980) ("a wrongful search or seizure conducted by a private party does not violate the Fourth Amendment and . . . such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully").

50. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

51. *Burdeau*, 256 U.S. at 475; United States v. Jacobsen, 466 U.S. 109, 125 (1984).

52. *See infra* Part III (discussing the two notable cases that applied the private search doctrine to digital devices).

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

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

55. *Infra* Part III.

56. *Runyan*, 275 F.3d at 453–54 (5th Cir. 2001); *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

57. *Runyan*, 275 F.3d at 464.

58. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

59. *Id.*

reasoned that holding otherwise might over-deter police from thorough searches of containers where the owners had diminished expectations of privacy.[60]

In *Rann v. Atchison*,[61] the Seventh Circuit adopted the Fifth Circuit's reasoning.[62] There, a daughter and her mother brought the father's zip drive to the police, and claimed the drive contained child pornography.[63] Because the mother and daughter knew what was on the device, the Court reasoned, the police officers were "substantially certain" the zip drive contained child pornography.[64] The Fifth Circuit held that the search, therefore, did not exceed the scope of the private search, and the officers were able to search the entire zip drive.[65] Before *Riley v. California*, both of these cases demonstrated how courts applied the private search doctrine to electronic devices.[66]

IV. THE *RILEY V. CALIFORNIA* RIPPLE EFFECT

The United States Supreme Court took a new turn when it announced in the precedential case *Riley v. California* that individuals have a high privacy interest in their cell phones.[67] This Part first explains the decision,[68] and then explains its potential legal impact.[69]

A. Riley v. California

The court in *Riley v. California* handled the issue of whether the digital information on a cell phone may be searched incident to arrest.[70] There, petitioner David Riley was pulled over for driving without proper registration stickers.[71] During that stop, the officer learned Riley also had a suspended license, and impounded the car—finding handguns under the car's hood.[72] While arresting Riley, the officer seized his cell phone from his pocket and discovered evidence associating Riley with the "Bloods" street gang.[73]

---

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

61. 689 F.3d 832 (7th Cir. 2012).

62. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

63. *Id.*

64. *Rann*, 689 F.3d at 838.

65. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

66. *See Rann*, 689 F.3d at 838; *and* United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001) (applying the private search doctrine to an electronic device).

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

68. *Infra* Part IV.A.

69. *Infra* Part IV.B.

70. *Riley*, 134 S. Ct. at 2480.

71. *Id.*

72. *Id.*

73. *Id.*

In holding that the officer could not search the contents of the smart phone incident to arrest,[74] the *Riley* court balanced the degree to which the search intrudes upon a person's privacy against the degree to which it is needed for the promotion of legitimate governmental interests.[75] The governmental interests furthered from a search incident to arrest—protecting the officer's safety and preventing destruction of evidence—do not apply to the search of digital information on a cell phone, according to the *Riley* court.[76] Digital data cannot be used by itself as a weapon to harm an officer making an arrest, and any concern of destruction of evidence for a digital device is not enough because it is unlikely to occur.[77]

In weighing the privacy interests of the individual, the *Riley* court noted how smart phones are highly distinguishable from their older telephone counterparts.[78] "Modern cell phones implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[79] The devices are in fact minicomputers with enormous storage space capable of storing the equivalent of millions of pages of text, thousands of pictures, or hundreds of videos.[80] Therefore, the Court decided, the storage capacity of modern cell phones has large consequences for privacy.[81] *Riley* then ruled that the information contained on a cell phone, because of these high privacy interests, could not be searched incident to arrest without a warrant.[82]

The *Riley v. California* decision did not implicate the private search doctrine directly, rather the holding was directed only at searches incident to arrest.[83] However, the analysis in *Riley* has impacted courts and scholars citing the decision.[84]

B. Phone Sweet Phone: The Impacts of Riley

Riley v. California contained deep analysis on the individual privacy interests implicated by searching cellphones.[85] First, the court compared cell phones to a home.[86] The Court explained that modern phones not only contain very sensitive

74. *Id.* at 2485.
75. *Id.* at 2478.
76. *Id.* at 2484–85.
77. *Id.* at 2485.
78. *Id.* at 2488–89.
79. *Id.*
80. *Id.* at 2489.
81. *Id.*
82. *Id.* at 2493.
83. *Id.*
84. *Infra* Part IV.B.
85. *Riley*, 134 S. Ct. at 2493.
86. *Id.* at 2491.

personal information that was previously found in the home, but also personal information that is never found in a home; cell phones therefore expose to the government even more than what can be found in an exhaustive search of a house.[87] The Court held that not only was the officer in *Riley* not able search the phone incident to arrest, but generally that a warrant is required before a search of a cell phone.[88] The following subpart analyzes how *Riley* has affected reasoning in other areas of law,[89] and how that reasoning affects the private search doctrine.[90]

1. The Potential Effects on a Different Doctrine: The Third-Party Doctrine

Following *Riley*'s analysis on the privacy interests involved with the modern cell phone, many scholars have alluded to advancements in the law based on *Riley*'s analysis, such as extending protections to the third-party doctrine—where privacy interests in information are forfeited at the moment of conveyance to a third party—or even removing the third-party doctrine altogether.[91]

The *Riley* Court explained that much of the important data viewed or used on cell phones is not actually stored on the device itself, which further complicates the privacy interests at stake.[92] Instead, modern phones access data contained elsewhere, known as "cloud computing."[93] Scholars have explained that the third-party doctrine still applies to cell phones despite the *Riley* decision, because *Riley* did not address implications on the third-party doctrine.[94] One scholar, Joshua Vittor, urged that Fourth Amendment protections be expanded in the face of rapidly expanding technology.[95] For example, in *United States v. Warshak*, the Sixth Circuit limited the scope of the third-party doctrine as applied to emails

87. *Id.*

88. *Id.* at 2493.

89. *Infra* Part III.B.1.

90. *Infra* Part III.B.2.

91. The third-party doctrine holds that a person has no legitimate expectation of privacy in, and no Fourth Amendment protection of, information that is given to third parties. Ryan Watzel, *Riley's Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J. FORUM 73, 74 (2014). *See also* Joshua Vittor, *What Would a Martian Think of Cell Phones? The Third-Party Doctrine and Technological Extensions of the Human Self*, 10 HARV. L. & POL'Y REV. 255 (2016); Laurie Buchan Serafino, *"I Know My Rights, So You Go'n Need a Warrant for That": The Fourth Amendment,* Riley*'s Impact, and Warrantless Searches of Third-Party Clouds*, 19 BERKELEY J. CRIM. L. 154 (2014); George M. Dery III & Kevin Meehan, *A New Digital Divide? Considering the Implications of* Riley v. California*'s Warrant Mandate for Cell Phone Searches*, 18 U. PA. J.L. & SOC. CHANGE 311 (2015).

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

93. *Id.* Cloud computing is when data is stored and accessed over the internet, instead of being stored on a device's own hard drive. Eric Griffith, *What is Cloud Computing?*, PC MAG (May 3, 2016), http://www.pcmag.com/article2/0,2817,2372163,00.asp (on file with *The University of the Pacific Law Review*).

94. Vittor, *supra* note 91, at 258.

95. *Id.* at 272.

because emails have become an essential form of communication; the Fourth Amendment must keep pace with ever-evolving technologies.[96] This is why, Vittor explained, the third-party doctrine is perhaps not suitable for a growing digital age.[97] Thus, following *Riley v. California*, there are potential implications to expand this other doctrine—the third-party doctrine.[98]

2. The Reasoning for Expanding the Third-Party Doctrine After Riley*, Applied to the Private Search Doctrine*

Since scholars like Vittor urge that the third-party doctrine is inappropriate in a digital age where technologies are ever changing, it is equally important to consider how the digital age impacts the private search doctrine.[99] *United States v. Warshak* limited the third-party doctrine because emails have become essential communication; therefore, as people become dependent on their modern phones, courts could follow this same line of reasoning and limit the private search doctrine because phones are essential methods of communication.[100] The *Riley* analysis has not only urged that police cannot search cell phones incident to arrest, but it has apparently shown that the high privacy expectations in modern phones created a new policy for technology.[101] The policy is that cell phones are not simply physical objects, they are provided a high expectation of privacy in *Riley* because they "hold for many Americans 'the privacies of life.'"[102] This is the theory used by scholars in advocating for a revised third-party doctrine,[103] and it applies similarly to the private search doctrine.

V. THE CIRCUIT SPLIT

Following *Riley*, two recent decisions have joined together in narrowing the private search doctrine.[104] These two new cases created a circuit split with the pre-*Riley* cases.[105] One of these recent decisions, *United States v. Lichtenberger*,

96. *Id.* at 265.

97. *Id.* at 266.

98. *Id.*

99. *See id.* (mentioning that the third-party doctrine is inappropriate in a digital age).

100. *See id.* at 265 (explaining the reasoning in *Warshak*).

101. *See id.* at 258–59 (explaining how the deep concerns emphasized in *Riley* offered a theoretical solution to revise the third-party doctrine).

102. Riley v. California, 134 S. Ct. 2473, 2495 (2014).

103. *See* Vittor, *supra* note 91, at 258-259 (explaining how the deep concerns emphasized in Riley offered a theoretical solution to revise the third-party doctrine); Watzel, *supra* note 92, at 76 (noting how *Riley* suggested that cloud-based data may nevertheless be afforded Fourth Amendment protection).

104. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

105. *Compare* United States v. Lichtenberger, 786 F.3d 478, 487 (6th Cir. 2015); *and* United States v. Sparks (Johnson), 806 F.3d 1323, 1336 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 2009, 195 L. Ed. 2d 222

cited *Riley* and claimed that "the nature of the searched device greatly increased the potential privacy interests at stake."[106] This came shortly after another post-*Riley* case that applied the private search doctrine narrowly, *Johnson v. United States*.[107] Both of these post-*Riley* decisions stress the intrusiveness of police searching personal electronics.[108] This Part first explains what happened in these two cases,[109] and then examines the circuit split between them and the two notable pre-*Riley* cases.[110] Lastly, this Part examines whether the Sixth Circuit decided the *Lichtenberger* case properly, ultimately concluding that the Sixth Circuit was moving in the right direction.[111]

A. The New Decisions

In *Johnson v. United States*,[112] the Eleventh Circuit considered the issue of whether the warrantless search of a cell phone following a private search exceeded the scope of the private search doctrine.[113] In that case, two defendants, Alan Johnson and Jennifer Sparks, unwittingly left their cell phone in a Walmart.[114] One of the store's employees found the phone and agreed to return it to the defendants.[115] However, the employee decided to peek at the contents of the phone, and upon discovering child pornography, instead decided to turn it over to the police.[116] Both defendants were indicted for possession and production of child pornography.[117]

On the private search doctrine issue, the *Johnson* court held the police officer's search of the cell phone exceeded the scope of the Walmart employee's private search.[118] This was because the officer viewed one video on the phone the employee had not previously watched, meaning the governmental search did not

(2016), *and cert. denied sub nom.* Johnson v. United States, 137 S. Ct. 34, 196 L. Ed. 2d 46 (2016); *with* Rann v. Atchison, 689 F.3d 832 (7th Cir. 2012); *and* United States v. Runyan, 275 F.3d 449 (5th Cir. 2001) (the Sixth and 11th Circuits disagree with the Fifth and Seventh over how narrowly to apply the private search doctrine).

106. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

107. United States v. Sparks (Johnson), 806 F.3d 1323 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 2009, 195 L. Ed. 2d 222 (2016), *and cert. denied sub nom.* Johnson v. United States, 137 S. Ct. 34, 196 L. Ed. 2d 46 (2016).

108. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

109. *Infra* Part V.A.

110. *Infra* Part V.B.

111. *Infra* Part V.C.

112. *Johnson*, 806 F.3d 1323.

113. *Id.* at 1335.

114. *Id.* at 1329.

115. *Id.*

116. *Id.*

117. *Id.* at 1330.

118. *Id.* at 1335. Even though the court still held the subsequent search warrant valid and affirmed the district court's denial of the Defendants' motion to suppress the child pornography. *Id.*

replicate the private search and went beyond the scope of the private search doctrine.[119] In its analysis, the *Johnson* court noted that approving of the search would be inconsistent with *Riley* because cell phones hold "the privacies of life," and the storage capacities of phones suggest that a search warrant must specify what part of its contents may be searched.[120] Because the employee's search did not expose every part of information contained in the cell phone, no exception to the warrant requirement could have excused the officer's viewing of that particular video on the phone.[121]

Just a couple months following *Johnson* in early 2015, the Sixth Circuit decided *Lichtenberger*.[122] *Lichtenberger* is similar to *Johnson*, but the device searched was a laptop computer rather than a cell phone.[123] In that case the court decided whether an officer's search of a laptop exceeded the scope of the private search, where the defendant's girlfriend had found child pornography.[124] The police arrested the defendant for failing to register as a sex offender.[125] After his arrest, his girlfriend Karley Holmes looked through his computer and discovered numerous images of child pornography.[126] Holmes then contacted the police.[127] When officers arrived at the house Holmes showed them some of the images on the laptop.[128] Holmes could not recall if these were the same images she had viewed previously, and the officer testified he might have had Holmes open files "other than those she had previously opened."[129]

The *Lichtenberger* court held the warrantless search of the defendant's laptop exceeded the scope of the private search.[130] The court emphasized the "virtual certainty" requirement from the *Jacobsen* case,[131] and found the officer's lack of "virtual certainty" when he viewed the images dispositive.[132] The court refused to apply the private search doctrine where the search exceeded the scope of the initial private search.[133] Just like in *Johnson*, the *Lichtenberger* court cited *Riley* as instructive.[134] The court decided that under *Riley*, "the nature of the electronic

119. *Id.* at 1336.
120. *Id.*
121. *Id.*
122. United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015).
123. *Id.* at 479.
124. *Id.* at 491.
125. *Id.* at 479.
126. *Id.*
127. *Id.*
128. *Id.*
129. *Id.* at 488.
130. United States v. Lichtenberger, 786 F.3d 478, 491 (6th Cir. 2015).
131. *Id.* at 488.
132. *Id.* at 490.
133. *Id.* at 486.
134. *See id.* at 487 (discussing Riley v. California); *and see* United States v. Sparks (Johnson), 806 F.3d

device greatly increases the potential privacy interests at stake, adding weight to one side of the scale while the other remains the same."[135] Applying this concept to the private search doctrine, the court noted that this "shift" of the scale manifested itself in the "virtual certainty" requirement from *Jacobsen*.[136] The officer in that case needed to search the laptop with "virtual certainty" that his search would not show him any more than what Holmes had already described to him.[137] When the officer was uncertain that Holmes had opened the same files from the initial search, there was plainly no virtual certainty in that case.[138]

Both post-*Riley* cases emphasized the importance of "virtual certainty," and treated each individual file on the devices as their own container, not allowing the government search to exceed the specific files viewed in the initial private search.[139] The way these two cases treated files stored on an electronic device differed greatly from the two notable pre-*Riley* cases—*United States v. Runyan*[140] and *Rann v. Atchison*.[141]

B. The Circuit Split with United States v. Runyan *and* Rann v. Atchison

Runyan and *Rann* can be distinguished from the post-*Riley* cases in the sense that the objects searched were disks and a zip drive rather than a personal cellular phone and laptop computer.[142] But all of these cases are similar because the government searched personal electronic files.[143]

Even though *Runyan* and *Rann* applied a "substantial certainty" test, and *Lichtenberger* applied a "virtual certainty" test, there is little functional difference, if any, between the two.[144] *Runyan* read *Jacobsen* in combination with other precedential cases, declaring that searching a privately-searched container is not necessarily problematic if the police have *substantial certainty* of what they would find.[145] *Lichtenberger*, in interpreting *Jacobsen*, decided the officer had to be *virtually certain* his search would not uncover any more than the private party had told him.[146] *Jacobsen* provided both of these standards, and

---

1323, 1336 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 2009, 195 L. Ed. 2d 222 (2016), *and cert. denied sub nom.* Johnson v. United States, 137 S. Ct. 34, 196 L. Ed. 2d 46 (2016) (discussing Riley v. California).

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

136. *Id.*

137. *Id.*

138. *Id.*

139. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

140. 275 F.3d 449 (5th Cir. 2001).

141. 689 F.3d 832 (7th Cir. 2012).

142. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

143. *Id.*

144. LaBrecque, *supra* note 11, at 185.

145. *Runyan*, 275 F.3d at 463.

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

although these tests are worded differently, they are functionally equivalent.[147] Both the pre-*Riley* and post-*Riley* cases were applying the same test.[148]

What created the different results between the pre-*Riley* and post-*Riley* cases was which specific container the police needed virtual certainty in.[149] What is the right measuring unit: the file, the folder, or the physical device?[150] There was one main shift in applying the private search doctrine—allowing police to search only each individual file the private party searched as opposed to the entire device.[151] The post-*Riley* cases have thus narrowed the scope of the private search doctrine, holding a warrantless search by police cannot go beyond those electronic files viewed by the private party during the prior search.[152] In essence, the post-*Riley* cases treated each individual file on the devices as their own "container" for purposes of the private search doctrine.[153]

C. Were Lichtenberger *and* Johnson *Decided Properly?*

Are *Lichtenberger* and *Johnson* correct in narrowly applying the private search doctrine?[154] One scholar, for example, believes the the heavy focus on individuals' privacy was inappropriate in *Lichtenberger*, and that the Sixth Circuit improperly ignored the balanced approach of precedent in other circuits while citing a case unrelated to the private search doctrine.[155] This subpart considers whether the approach taken by *Lichtenberger* and *Johnson* was an appropriate change to the private search doctrine, considering their large focus on *Riley*, concluding the shift was well warranted.[156]

147. LaBrecque, *supra* note 11, at 185.

148. Orin Kerr, *Sixth Circuit Creates Circuit Split on Private Search Doctrine for Computers*, THE WASH. POST (May 20, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/20/sixth-circuit-creates-circuit-split-on-private-search-doctrine-for-computers/ (on file with *The University of the Pacific Law Review*).

149. Jeffrey Koelemay, *Laptop Search for Child Porn Suppressed; Officer Lacked 'Virtual Certainty' of Contents*, BLOOMBERG BNA (May 26, 2015), https://www.bloomberglaw.com/document/XBGSG59K000000?jcsearch=dk%253Abna%2520a0g6z7e5y5#jcite (on file with *The University of the Pacific Law Review*).

150. Kerr, *supra* note 148.

151. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

152. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

153. Koelemay, *supra* note 149.

154. *Infra* Part V.C.

155. Katie Matejka, *United States v. Lichtenberger: The Sixth Circuit Improperly Narrowed the Private Search Doctrine of the Fourth Amendment in a Case of Child Pornography on a Digital Device*, 49 CREIGHTON L. REV. 177, 198 (2015).

156. *Infra* Part IV.C.

*1. Were the Post-*Riley *Cases Correct in Narrowing the Private Search Doctrine?*

One scholar who wrote on the issue, Katie Matejka, argued the *Lichtenberger* court improperly focused on protecting data privacy.[157] This scholar contended the use of *Riley* in the court's analysis was inappropriate because it is not a private search case.[158] This subpart considers whether the case was decided properly.[159]

Matejka argued the *Lichtenberger* court ignored the balanced approach of other circuits and ignored its own precedent.[160] In 2010, before *Riley* was decided, the Sixth Circuit held that officers who looked through a photo album of pornographic images of children did not exceed the scope of the private search because they had been told of the album's contents.[161] Similarly, only a couple years prior, the Sixth Circuit also held that a government search of a storage locker containing pornographic images of children did not exceed the scope of the initial private search by a storage facility employee.[162] Both of these pre-*Riley* private search cases can be distinguished from *Lichtenberger* because *Lichtenberger* was about data on a digital device while the prior cases were not.[163] However, Matejka drew an analogy between a digital file and a physical one, "the rationale extending the private search doctrine . . . to digital items is very clear because the folder containing all of the images of child pornography on Lichtenberger's laptop is comparable to the album of photos in *Bowers* and the storage unit in *Richards*."[164] In all of these cases, Matejka urged, the officers were certain the container in question contained child pornography, but could have also incidentally contained something other than child pornography.[165] Therefore, Matejka argued, the *Lichtenberger* court should not have treated the laptop differently, and erred when it applied the private search doctrine narrowly to each individual file of child pornography viewed by the private party.[166]

Although it is true the Sixth Circuit applied the private search doctrine in a way that appeared inconsistent with its precedent, it correctly cited and applied *Riley* because *Riley* contains influential analysis of a new policy that the United States Supreme Court intended to adopt.[167] *Riley* is not a private search case,

157. Matejka, *supra* note 155, at 178.

158. *Id.* at 196.

159. *Infra* Part V.C.1.

160. Matejka, *supra* note 155, at 196.

161. United States v. Bowers, 594 F.3d 522, 527 (6th Cir. 2010); Matejka, *supra* note 155, at 185–86.

162. United States v. Richards, 301 F. App'x 480, 483 (6th Cir. 2008); Matejka, *supra* note 155, at 186.

163. Matejka, *supra* note 155, at 194.

164. *Id.*

165. *Id.* at 194–95.

166. *Id.* at 195.

167. *See* Riley v. California, 134 S. Ct. 2473, 2488–89 (2014) (examining the privacy interests in cell

meaning it is not dispositive as to how broadly a search can occur under the private search doctrine.[168] Regardless, *Riley* thoroughly explained the importance cellular phones hold in the lives of Americans, and emphasized this heightened privacy interest.[169] The holding of *Riley* was centered not on the fact that the cell phone was searched incident to arrest, but on weighing the privacy interests in phones—they contain a broad array of sensitive records and information.[170] "Our holding . . . is not that the information on a cell phone is immune from a search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest."[171]

Therefore, the Court based the holding of *Riley v. California* not on the mechanics of a search incident to arrest, but on a broader policy—that modern cell phones deserve special protection because of the increasingly private nature of information contained within.[172] Additionally, the Court in *Riley* specifically rejected the analogy between the kinds of data found on a modern cell phone and information contained in physical places: "[Saying this kind of data is materially indistinguishable from physical items] is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[173]

Consequently, the Sixth Circuit's use of *Riley* as instructive was not improper because the United States Supreme Court applied not a rigid rule about the search incident to arrest doctrine, but a policy about the privacy interests in modern cell phones.[174] The Sixth Circuit in *Lichtenberger* did not cite a search incident to arrest case on accident.[175] Instead, *Lichtenberger* took careful note of the qualities in these electronic devices that implicate privacy interests,[176] and balancing the shift in the scale of personal interests versus governmental interests by using its more stringent threshold.[177] The Sixth Circuit in *Lichtenberger* merely followed *Riley*'s example of protecting the privacy of information contained in a personal digital device after weighing the interests of both sides.[178]

---

phones).

168. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

169. *Riley*, 134 S. Ct. at 2488–95 (analyzing the privacy interests in modern cell phones).

170. *Id.* at 2491.

171. *Id.* at 2493.

172. *See id.* at 2495 (holding cell phones exempt from the search incident to arrest exception to the warrant requirement).

173. *Id.* at 2488.

174. *See id.* at 2495 (because phones "are not just another technological convenience," holding the privacies of life, they are worthy of the protections the founders fought for).

175. *See* United States v. Lichtenberger, 786 F.3d 478, 487 (6th Cir. 2015) (citing *Riley* as instructive, and fully illustrating the holding in that case, including that it related to searches incident to arrest).

176. *Id.* at 487–88.

177. *Id.* at 488.

178. *See id.* at 487–88 (applying the virtual certainty threshold after agreeing with the *Riley* court that privacy-related concerns in electronic devices are weighty because they contain "1) many kinds of data, 2) in

Lichtenberger and *Johnson* are not coincidences; the courts intended to apply *Riley's* policy.[179] With technology continuously developing, with new phones, computers, and tablets being released every few months, the decision to agree with the *Riley* Court about the privacy interests that digital devices implicate is not only warranted, but vitally important.[180]

*2. Did the Post-*Riley *Cases Correctly Apply the Narrowed Private Search Doctrine?*

Another legal researcher who wrote on the private search doctrine, Stephen LaBrecque, argued the *Lichtenberger* court may have misapplied the private search doctrine, even though it correctly narrowed the scope of it.[181] This subpart considers the issue of how the post-*Riley* cases should have applied the doctrine.[182]

LaBrecque asserts that, although the Sixth Circuit correctly identified the proper scope for the private search doctrine in *Lichtenberger*, it failed in applying the test to the facts of the case.[183] LaBrecque explained that the officers in *Lichtenberger* had virtual certainty they would not reveal anything else of significance because they were viewing multiple files displayed as thumbnail images.[184] He urged the *Lichtenberger* court was mainly concerned with accidental discovery of medical records, bank statements, or other personal documents—but because the officer viewed the files as thumbnails, the officer could not have seen any text-based documents.[185] Therefore, LaBrecque stated, there was no risk the officer would accidentally discover other documents.[186]

When applying the private search doctrine to see if the governmental search exceeded the scope of the private search, courts measure how much information the government stands to gain, in relation to how certain the government is that it will find such information.[187] This measure considers the circumstances surrounding the governmental search, and so LaBrecque properly noted that the

---

vast amounts, 3) corresponding to a long swath of time").

179. *Id.* at 487; United States v. Sparks (Johnson), 806 F.3d 1323, 1336 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 2009, 195 L. Ed. 2d 222 (2016), *and cert. denied sub nom.* Johnson v. United States, 137 S. Ct. 34, 196 L. Ed. 2d 46 (2016).

180. *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014) (phones are used so much that an outsider would think they are part of human anatomy).

181. LaBrecque, *supra* note 11, at 189.

182. *Infra* Part V.C.2.

183. LaBrecque, *supra* note 11, at 189.

184. *Id.* at 191. "A thumbnail is a small image that represents a larger one . . . often used to provide snapshots of several images in a single space." *Thumbnail Definition*, TECHTERMS, https://techterms.com/definition/thumbnail (last visited Feb. 25, 2017) (on file with *The University of the Pacific Law Review*).

185. LaBrecque, *supra* note 11, at 191.

186. *Id.*

187. United States v. Lichtenberger, 786 F.3d 478, 485–86 (6th Cir. 2015).

small size and nature of thumbnail images affect what information officers learn during a search.[188]

However, the mere existence of thumbnail images should not be dispositive on this issue because what information they display is unknown to the officer before the search.[189] A disorganized person can intermingle different types of documents together in a single folder, and thumbnails can appear larger or smaller, showing more or less information.[190] Therefore, the mere nature of thumbnails is not enough to conclude that the officer in *Lichtenberger* had sufficient "virtual certainty" the laptop's contents would not tell him any more than he was told by the private party.[191]

In fact, the *Lichtenberger* court emphasized that the private party was just not sure if she showed the officer the same images she had seen in her original search.[192] This significantly influenced the court to conclude that the officer had no virtual certainty he would not discover anything new.[193] The officer may have seen images the private party simply did not see in the initial search.[194] Therefore, although the consideration of thumbnail images had an effect on what information the officer actually learned during a search, the *Lichtenberger* decision seems appropriate considering the circumstances.[195]

After *Johnson* and *Lichtenberger* applied the private search doctrine narrowly to digital devices, they created a circuit split with the pre-*Riley* private search cases *Rann* and *Runyan*.[196] Although their decisions contrasted prior cases that applied the private search doctrine to digital devices, the result is likely appropriate because the cases applied a new policy from *Riley v. California* meant to protect privacy interests in electronic devices.[197]

VI. SHIFTING PERSPECTIVES ON TECHNOLOGY: PREDICTIONS FOR THE FUTURE

With the new *Lichtenberger* and *Johnson* decisions in such stark contrast to the pre-*Riley* private search cases *Rann* and *Runyan*, other circuits that have yet

188. *See id.* at 485 (courts evaluate the reasonableness of an invasion with the facts as they existed at the time the invasion occurred).

189. *See, e.g.*, *id.* at 486 (noting that police must search with a particular amount of certainty as to what they will find).

190. *See Thumbnail Definition*, *supra* note 185 (thumbnails can vary in size);

191. *Lichtenberger*, 786 F.3d at 488 (explaining virtual certainty).

192. *Id.*

193. *Id.*

194. *Id.*

195. *Id.* at 488–89.

196. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

197. *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014) (phones are worthy of the protections the founders fought for).

to decide the issue will have decisions to make.[198] This Part considers what direction future circuits will take in deciding private search cases.[199] Then, this Part predicts that future cases will be decided in accordance with the Sixth and Eleventh Circuits and use the narrower threshold, treating each file like its own "container."[200] With *Lichtenberger* and *Johnson* in contrast with *Runyan* and *Rann*, future courts will need to decide the proper scope of the private search doctrine—whether they choose to apply the broader or narrower approach.[201] This Part considers which approach is likely to be applied in the future,[202] and how that standard will likely be applied to other devices.[203]

A. The Right Legal Standard for the Private Search Doctrine

What is the right scope for the private search doctrine?[204] *Runyan* treated computer disks as their own "containers," claiming that its analysis using substantial certainty was the most sensible result because it discouraged police from conducting "fishing expeditions" while simultaneously avoiding over-deterrence of police searches.[205] Similarly, *Rann* treated the zip drive as its own "container" when searched by a private party, instead of the files within.[206] Both of these cases held that police did not exceed the scope of the first search, when they treated the entire digital device as the "container."[207] In both *Runyan* and *Rann*, the privacy interests in all of the files were frustrated by a private party viewing only some of the files.[208] But *Runyan* and *Rann*'s application of the private search doctrine analogized digital files to physical containers in an effort to harmonize an issue around container searches.[209] "In the context of a search involving a number of closed containers . . . opening a container that was not

198. *Compare Lichtenberger*, 786 F.3d at 487; *and* United States v. Sparks (Johnson), 806 F.3d 1323, 1336 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 2009, 195 L. Ed. 2d 222 (2016), *and cert. denied sub nom.* Johnson v. United States, 137 S. Ct. 34, 196 L. Ed. 2d 46 (2016); *with* Rann v. Atchison, 689 F.3d 832 (7th Cir. 2012); *and* United States v. Runyan, 275 F.3d 449 (5th Cir. 2001) (the Sixth and 11th Circuits disagree with the Fifth and Seventh over how narrowly to apply the private search doctrine).

199. *Infra* Part VI.

200. *Infra* Part VI.

201. *Compare Lichtenberger*, 786 F.3d at 487; *and Johnson*, 806 F.3d at 1336; *with Rann*, 689 F.3d 832; *and Runyan*, 275 F.3d 449 (the Sixth and 11th Circuits disagree with the Fifth and Seventh over how narrowly to apply the private search doctrine).

202. *Infra* Part VI.A.

203. *Infra* Part VI.B.

204. *Infra* Part VI.A.

205. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46; *Runyan*, 275 F.3d at 465.

206. *Rann*, 689 F.3d at 838.

207. *Runyan*, 275 F.3d at 462; *Rann*, 689 F.3d at 838.

208. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

209. *Id.*

opened by private searchers would not necessarily be problematic if the police knew with substantial certainty . . . what they would find inside."[210]

However, the analogy between electronic devices and physical containers falls flat after the United States Supreme Court explained in *Riley v. California* that the type of data contained in cell phones and stored in physical places is, in fact, very different.[211] The Court stated that cell phones by their very nature implicate privacy concerns "far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[212] Therefore, the pre-*Riley* applications of the private search doctrine to digital devices were based on an analogy that was, in essence, disapproved of by the Supreme Court.[213]

The more narrow approach to the doctrine applied by *Lichtenberger* and *Johnson* treats each individual file as a "container," as opposed to the entire device.[214] This means when a private party views only some of the files, it does not frustrate the expectation of privacy in the other, non-viewed files.[215]

Because the United States Supreme Court has held that individuals have a heightened expectation of privacy for data stored on cell phones as compared to physical containers, the way *Runyan* and *Rann* applied the private search doctrine to digital devices is now outdated.[216] Therefore, in applying the private search doctrine, future courts are more likely to treat each digital file as its own container when searched by the government.[217]

B. How the New Standard Applies to Other Containers

Courts can apply the doctrine's narrower approach to digital devices other than cell phones so long as a court can draw an analogy from modern cell phones (in *Riley*'s analysis) to other personal digital devices, like the laptop in *Lichtenberger*.[218] The Sixth Circuit in *Lichtenberger* had no problem relating *Riley*'s analysis to laptop computers, because it was the qualities of cell phones that were of particular importance to the United States Supreme Court when it

210. *Runyan*, 275 F.3d at 463.

211. Riley v. California, 134 S. Ct. 2473, 2488 (2014).

212. *Id.* at 2488–89.

213. *Id.*

214. *See* United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015) (applying the private search doctrine narrowly to a personal digital device with similar characteristics with a cell phone).

215. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46 (in both *Lichtenberger* and *Johnson*, the government could not "exceed the specific files viewed in a prior private search").

216. *See Lichtenberger*, 786 F.3d at 488 (applying the private search doctrine narrowly to a personal digital device with similar characteristics with a cell phone).

217. *See id.* (treating the individual files on the laptop as their own containers for purposes of the private search doctrine).

218. *See id.* at 487 (using *Riley* as instructive for the search of a laptop computer).

decided *Riley*.[219] The Sixth Circuit used the reasoning behind the *Riley* Court's decision, noting that cell phones are in fact just "minicomputers that also happen to have the capacity to be used as a telephone."[220] This fact, combined with the idea that cell phones have immense storage capacity capable of keeping data over long periods of time, is what the *Lichtenberger* court found particularly instructive.[221] Thus, the application of a narrower private search doctrine to personal digital devices other than cell phones seems appropriate if the devices have these qualities.[222]

Following that reasoning, courts could likely apply the private search doctrine to tablets and desktop computers.[223] These two types of computers are very similar to both cell phones and laptops because they are computers with immense storage capacity.[224] But it is questionable whether courts could similarly apply the doctrine to netbooks[225] or smart watches.[226] Netbooks have considerably less storage capacity,[227] which was important to the *Riley* court in distinguishing cell phones.[228] Smart watches are somewhat similar to modern phones because they run applications and show media.[229] However, they are not stand-alone devices like a computer.[230] They are instead designed to link with a modern phone, and without such a link, their capabilities are very limited.[231] Thus, for smart watches that have little storage capacity, and are used mainly as an easier way to receive information from a person's phone, there are not many privacy interests at stake.[232]

Therefore, because the broader private search doctrine standards for digital devices are outdated, and because future courts will likely be able to relate other personal digital devices to *Riley*'s analysis, future courts will probably apply the

---

219. *Id.; see also Riley* v. California, 134 S. Ct. 2473, 2489 (2014) (discussing qualities of cell phones).

220. *Lichtenberger*, 786 F.3d at 487 (quoting *Riley v. California*).

221. *Id.* at 488.

222. *C.f. id.* (narrowing the private search doctrine for the search of a laptop computer because laptops share similar qualities with cell phones under Riley v. California's analysis that cell phones implicate heightened privacy interests).

223. *What Are the Different Types of Computer?*, *supra* note 10.

224. *Id.*

225. Net books are smaller and lighter versions of laptops, with much less storage capacity. *Id.*

226. A smart watch is a personal digital device that links to smart phones and shows information. Robert Valdes & Nathan Chandler, *How Smart Watches Work*, HOWSTUFFWORKS, http://electronics.howstuffworks.com/gadgets/clocks-watches/smart-watch.htm (last visited Feb 11, 2017) (on file with *The University of the Pacific Law Review*).

227. *What Are the Different Types of Computer?*, *supra* note 10.

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

229. Valdes & Chandler, *supra* note 226.

230. *Id.*

231. *Id.*

232. *See Riley*, 134 S. Ct. at 2489 (discussing qualities of cell phones while noting the heightened privacy interests involved).

narrower private search doctrine to searches of both cell phones and similar devices like desktop computers, laptops, and tablets.[233]

VII. ADVOCATING A NEW EXCEPTION TO THE PRIVATE SEARCH DOCTRINE—A CELL PHONE IS AS PRIVATE AS THE HOME

Cell phones are a growing necessity in the lives of every day Americans—so much that they appear as part of human anatomy.[234] The rationale underlying *Riley*—especially the comparison between phones and the privacy interests in homes—brings up a new question: are phones as private as the home?[235] And if so, should the private search doctrine be used to search them?[236] This Part considers first how the private search doctrine affects government searches of homes,[237] and then compares the application of the private search doctrine to phones.[238] This Part argues cell phones, and similar electronic devices, should be exempt from the private search doctrine altogether.[239]

A. The Doctrine's Application to the Home

The United States Supreme Court has yet to rule on whether the private search doctrine allows a warrantless search of a home, and circuits are divided on the issue.[240] However, the private search doctrine has long-standing roots in the Court's authority.[241] This fact has been troubling to courts considering the issue, despite the doctrine's solid foundation in the Fourth Amendment, since the warrant requirement applies only to government actors.[242]

The Supreme Court of New Jersey considered the issue most recently, claiming serious reservations about allowing the private search doctrine to apply to the search of a home.[243] In holding that the doctrine could not be used for a warrantless search of a home, the New Jersey Supreme Court cited its State Constitution and the general notion that the "chief evil" the Fourth Amendment

233. *See supra* Part VI (illustrating these concepts).

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

235. *See id.* at 2491 (discussing the privacy interests surrounding phones).

236. *Infra* Part VII.

237. *Infra* Part VII.A.

238. *Infra* Part VII.B, VII.C.

239. *Infra* Part VII.

240. Eric Breslin, *Can the "Private Search" Doctrine Serve as an Exception to the Federal and State of New Jersey Constitutional Requirement That a Warrant Issued in Advance of a Search of a Private Home?*, MONDAQ (May 19, 2015), http://www.mondaq.com/unitedstates/ (on file with *The University of the Pacific Law Review*) (search "private search doctrine" and select first result).

241. *Id.*

242. *Id.*

243. State v. Wright, 221 N.J. 456, 476 (2015).

sought to protect against was physical entry of the home.[244] That court reasoned that the interests a person has in their home are entitled to the utmost respect from unreasonable searches.[245] The court noted how careful scrutiny always follows the search of a private and intimate residence, because courts have recognized homes as unique for centuries.[246] "When it comes to the Fourth Amendment, the home is first among equals," and stands "at the Amendment's very core."[247]

Regardless, not all courts have followed this same line of reasoning.[248] There are multiple cases that have once held that a warrantless search of a home, following a private search, was justifiable under a private search theory.[249] In *United States v. Jones*, for example, the Fifth Circuit quickly concluded the Fourth Amendment did not apply.[250] Citing *Runyan*, the Fifth Circuit Court of Appeals held that as long as the "police view" is within the scope of the initial private search, Fourth Amendment protections are not implicated.[251]

But there are still many courts that have refused to extend the private search doctrine to residences, and for good reason.[252] *United States v. Allen*, for example, distinguishes *Jacobsen*.[253] The package in *Jacobsen* contained only contraband, the court explained.[254] But the defendant's motel was his temporary abode, containing intimate and personal items.[255] The defendant *Allen* had a significant privacy interest in where he was living, when the private search did not completely frustrate that interest because the motel manager viewed only

244. *Id.* at 466–67.

245. *Id.* at 467.

246. Breslin, *supra* note 240.

247. Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013).

248. WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.8(b) n.95 (5th ed. 2012).

249. *See* United States v. Bomengo, 580 F.2d 173 (5th Cir.1978) (officer called into apartment after a search by chief engineer); Lucas v. State, 381 So.2d 140 (Miss.1980) (neighbor invited officer to search apartment); United States v. Jones, 421 F.3d 359 (5th Cir.2005) (manager asked police to join her upon reentry of apartment); United States v. Miller, 152 F.3d 813 (8th Cir.1998) (police entry proper after manager entered apartment and saw drugs); United States v. Paige, 136 F.3d 1012 (5th Cir.1998) (holding that a subsequent police entry is no search if the prior private person entry was "reasonably foreseeable"); United States v. Clutter, 914 F.2d 775 (6th Cir.1990) (police search was no search under Jacobsen because the officer learned nothing on his own that he had not already learned from the private search); State v. Miller, 110 Nev. 690, 877 P.2d 1044 (1994) (police invited by babysitter); Peters v. State, 302 S.C. 59, 393 S.E.2d 387 (1990) (person found LSD in sibling's home, invited police on reentry).

250. *Jones*, 421 F.3d at 361–62.

251. *Id.*

252. *See* LAFAVE, *supra* note 248 (listing cases that have held that a private search does not allow government entry of a residence).

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

254. *Id.*

255. *Id.*

some of his possessions.[256] Therefore, although many courts have upheld searches of residences based on a private search theory, there remains good reason to doubt that the Supreme Court of the United States will allow police to make a warrantless entry of a premises simply because it was previously viewed by a private party.[257]

B. Applying the Doctrine to Electronic Devices: Riley's *Policy Rationale*

Despite courts' disagreement on whether the private search doctrine extends to homes because of the large privacy interests involved, *Riley*'s analysis provides huge implications to the effect of the doctrine on phones and similar devices.[258] As *Riley* stated, phones often contain far more information than what can be found in a house.[259] This means that, given the growing importance and widespread dependence on cell phones, warrantless searches that implicate the privacy interests in these devices should be taken seriously.[260]

There is little question that courts afford the greatest protection to the home under the Fourth Amendment, but this protection can arguably be extended to modern cell phones, considering their unique qualities.[261] A cell phone search shows to the government "far *more* [information] than the most exhaustive search of a house."[262] This fact alone creates huge implications for the future of privacy in cell phones—if a cell phone can contain documents more personal and private than what is stored away in a person's home, yet the home is the most protected place under the Fourth Amendment, then courts should afford similar protections to the data stored on cell phones.[263]

Compared to the papers and effects inside a residence, *Riley* explained that phones contain vast amounts of information that are far more private in nature.[264] For example, modern cell phones store enormous amounts of location data: the phone's location where each call was made and received, the location of every Wi-Fi network joined, and even photos taken with the camera contain "geo-tag[s]."[265] Applications intended for chatting with friends, even when supposedly

256. *Id.*

257. LAFAVE, *supra* note 248.

258. *See* Riley v. California, 134 S. Ct. 2473, 2491 (2014) (explaining the privacy interests in cell phones).

259. *Id.*

260. *See Riley*, 134 S. Ct. at 2493 (holding that, generally, officers should get a warrant before searching cell phones).

261. *See id.* at 2491 (a phone contains sensitive records).

262. *Id.*

263. *C.f. id.* (stating that phones contain more information than a house, opening an opportunity to analogize the privacy interests in cell phones to those interests in the private home).

264. *Id.*

265. Rob Lekowski, *What Lawyers Need to Know About Data Stored on Mobile Devices*, LAW TECH.

secure, store records on the phone.[266] People can always retrieve messages, with their respective time stamps.[267] Someone searching for data can restore full browsing history even when the phone's owner deletes it.[268] Certain applications that use images, like Snapchat, store images on the phone even when the user does not intentionally save them via screen shot.[269]

It is important to consider the large amount of the data stored on a modern phone, in addition to people are using them more often—becoming increasingly dependent on their functionalities.[270] For heavy users, the amount of data stored on these devices is staggering.[271] Because of this, it is understandable why the *Riley* court stated that modern phones contain more private information than a home.[272]

As technology advances and as people become increasingly dependent on their cellular phones, it will also become increasingly important to protect the data they will contain.[273] Therefore, this Comment urges that, based on *Riley's* analysis and on the continuing dependence on cell phones, they should be exempt from the private search doctrine in the same way they were exempt from the search incident to arrest exception.[274]

C. Applying the Legal Standard

A private search of a cell phone will rarely provide the "virtual certainty" required for all of the data an officer may view during a search.[275] As the *Lichtenberger* court explained its application of the doctrine, "[to stay within the scope of the private search, the officer] had to proceed with 'virtual certainty' that the 'inspection of the laptop and its contents would not tell him anything more than he had already been told by [the private party].'"[276] But with the vast amount of data contained in a cellular phone, it is a heavy task for an officer not to learn anything more while navigating the device.[277]

TODAY (Feb. 17, 2015), http://www.lawtechnologytoday.org/2015/02/data-stored-on-mobile-devices/ (on file with *The University of the Pacific Law Review*).

266. *Id.*

267. *Id.*

268. *Id.*

269. *Id.*

270. *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014) (phones are a pervasive part of daily life).

271. Lekowski, *supra* note 265.

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

273. *See id.* at 2484 (phones are a pervasive part of daily life).

274. *See id.* at 2495 (search incident to arrest does not apply to cell phones).

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

276. *Id.*

277. Lekowski, *supra* note 265; *See Riley*, 134 S. Ct. at 2491 (phones have immense storage capacity and contain a plethora of information).

For example, if a police officer wishes to view an incriminating text message that was previously viewed by a private party, the officer would need to open the messages application.[278] But upon opening the application, they would be confronted with different "threads" of conversations, showing the most recent message in each thread.[279] Therefore, an officer would inevitably see portions of multiple conversations, while trying to find the one incriminating text.[280] This demonstrates that the nature of the display of information makes it very difficult, if not almost impossible, for an officer to search through the contents of a modern cell phone without learning anything more than the private party had learned during the initial search.[281] Or, at the very least, it would be very difficult to tell if the officer viewed only what the private party viewed.[282]

With the risks of discovering new information so high, combined with the fact that phones store a plethora of data just as private as information contained in the home, this Comment urges that the scale weigh in favor of the individual.[283] The risks of infringing on such privacy interests are too great, and so the private search doctrine should not apply to modern cellular phones.[284]

VIII. CONCLUSION

After *Riley v. California*, the nature of electronic devices greatly increases the privacy interests at stake when the government searches them, "adding weight to one side of the scale when the other remains the same."[285] When a police officer searches a digital device, like the laptop in *Lichtenberger*, the heightened privacy interests instruct the use of a narrower standard—treating each digital file as its own container.[286] And when applying the private search doctrine's "virtual certainty" standard, it is unlikely a police officer could search a device like a modern phone without learning more information, risking the privacy interests at stake.[287]

---

278. *See* Scott Lowe, *Tweak Your Message Viewing Options in iOS and Android*, TECHREPUBLIC (Dec. 15, 2011, 10:30 AM), http://www.techrepublic.com/blog/smartphones/tweak-your-message-viewing-options-in-ios-and-android/ (on file with *The University of the Pacific Law Review*) (explaining how to rearrange messages, while showing they are viewable in the same phone application).

279. *Id.*

280. *See id.* (showing that threads are viewable at one place).

281. *See id.* (text conversations are displayed on the same page).

282. *C.f.* United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015) (finding that it was unknown whether the officer viewed thumbnails that the private party had not viewed).

283. *See supra* Part VI (explaining how officers may be likely to learn new information while searching and how the expectation of privacy in cell phones is high).

284. *See supra* Part VII.C (showing that the risks of infringing on privacy interests when an officer conducts a phone search are great).

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

286. *After Riley, Circuits Narrow Private Search Doctrine*, *supra* note 46.

287. *See Lichtenberger*, 786 F.3d at 488; *and* Riley v. California, 134 S. Ct. 2473, 2491 (phones have

Given the ever-growing dependence on technology, future courts are likely going to use the narrower standard.[288] And in the interests of each individual citizen, and the millions of phones and laptops involved, the private search doctrine should not apply to them because the risks of infringing on privacy interests are too great.[289]

immense storage capacity and contain a plethora of information).

288. *See supra* Part V (arguing that future courts are likely to use the narrower private search doctrine standard).

289. *See supra* Part VI (explaining why the doctrine should not apply to phones and similar devices).