Stanford Law Review

Volume 69 January 2017

NOTE

Unpacking Digital Containers: Extending *Riley*'s Reasoning to Digital Files and Subfolders

Michael Mestitz*

Abstract. The Supreme Court's recent decision in *Riley v. California* held that cell phones cannot be subject to warrantless searches incident to arrest, a strong statement that digital devices are entitled to the protections of the Fourth Amendment. But the opinion leaves many questions unanswered. One of the most important is what expectation of privacy individuals and businesses maintain in the separate digital "subcontainers" on their devices: the discrete files, folders, and application data that police may try to search within a given computer or cell phone. This question has important implications for the scope of warrantless searches in the digital age and has been the subject of a longstanding circuit conflict.

In this Note, I argue that *Riley*'s reasoning, as well as the text and history of the Fourth Amendment, suggest that digital subcontainers should be accorded robust privacy protections when they are subject to warrantless searches. Analyzing the Court's reasons for its holding in *Riley*, this Note demonstrates that those reasons apply with equal force to warrantless searches of all files and folders on a digital device, not just to the government's initial intrusion. On this reasoning, I propose that even if the government has authorization to conduct a search of some portion of the files on a device, the suspect maintains a constitutionally protected privacy interest in the other files that prevents the government from expanding its search without authorization. This bright-line rule is consistent with *Riley*, helps resolve unsettled questions how certain search doctrines apply to digital searches, and furthers the goal of providing a reasonable and administrable rule for law enforcement and courts to apply to warrantless digital searches.

* J.D., Stanford Law School, 2015. President, *Stanford Law Review*, Volume 67. I would like to thank Michael Evans, Jeffrey Fisher, Lawrence Marshall, Ticien Sassoubre, Robert Weisberg, and the editors of the *Stanford Law Review* for their feedback and assistance in preparing this Note for publication.

Table of Contents

Introduction

In June 2014, the Supreme Court unanimously held in *Riley v. California* that cellular phones are protected against warrantless searches incident to arrest.[1] The Court concluded cell phones differ "in both a quantitative and a qualitative sense" from other objects an arrestee might carry, rejecting the argument that phones are like other containers for the purpose of the Fourth Amendment.[2] The decision was hailed in headlines as "the dawn of a new digital age of privacy."[3] It is undoubtedly a significant case with broad implications.

The next great issue of digital privacy will be determining which legal rules and privacy interests separate one file from another file when the government is *already* conducting a search. Like a Russian nesting doll, a cell phone is not just one undifferentiated container: it contains separate folders and files—"subcontainers"[4]—all nested within each other. And although *Riley* spoke explicitly only to the broadest level of container, this Note argues that *Riley*'s reasoning applies equally to warrantless searches of the separate files and folders *within* those digital devices. Although the Court has not historically been concerned with the privacy interests in particular subcontainers, *Riley*'s approach in recognizing the special status of digital containers suggests this view is ripe for reexamination. To that end, it makes the most sense after *Riley* to treat each individual file or folder as an individual subcontainer—that is, as protected by a particular privacy interest unaffected by a search of the surrounding files, and requiring particular authorization to search in the form of either a warrant or a valid exception to the warrant requirement.

This interpretation is buttressed by the policy and history behind the Fourth Amendment. Traditionally, objects subject to search have been conceived of as "containers": a cigarette package in a pocket,[5] a backpack over the shoulder, or a lockbox in the trunk of a car.[6] Digital searches now force

1. *See* Riley v. California, 134 S. Ct. 2473, 2485 (2014).

2. *Id.* at 2489.

3. Justin P. Murphy & Louisa K. Marion, *The U.S. Supreme Court's Far-Reaching Decision on Police Searches of Cell Phones: The Dawn of a New Digital Age of Privacy*, WORLD DATA PROTECTION REP. 1 (Aug. 2014), https://www.crowell.com/files/The-U.S.-Supreme-Courts-Far-Reaching-Decision-on-Police-Searches-of-Cell-Phones-The-Dawn-of-a-New-Digital-Age-of-Privacy.pdf.

4. This term is borrowed from Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 BERKELEY J. CRIM. L. 112, 113 (2011). Goldfoot opposes conceptualizing digital files as containers at all, arguing instead that computers should be "examined" as a type of physical evidence (rather than "searched" as a container). *Id.*

5. *See* United States v. Robinson, 414 U.S. 218, 223 (1973).

6. *See* United States v. Chadwick, 433 U.S. 1, 4, 11, 21 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

courts to determine whether telephones, computers, and individual digital files are "containers" for the purpose of determining the permissible scope of warrantless searches, and how conventional physical search rules apply to digital searches. As the Court has previously observed, "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[7] *Riley* in particular represents the Court's unanimous acknowledgement that digital containers are, at least in some respects, different in kind from their physical counterparts.

It is easy to see why this issue will matter. When criminal suspects are subject to warrantless searches, questions naturally arise about the permissible scope of the search. And where containers are involved, those questions often turn on whether the defendant maintains a reasonable expectation of privacy in a given container. For investigators conducting the search, it means understanding the circumstances under which they may proceed and when they must stop. For some defendants, it can mean the difference between the admission and suppression of damning evidence. For all, it implicates profound intrusions on one's privacy.

Although lower courts are just beginning to feel *Riley*'s effects, *Riley*'s reasoning can resolve a longstanding split between courts on how to treat the files within computers and other digital devices. The Fifth and Seventh Circuits have held that warrantless searches of *part* of a computer allow searches of *all* of a computer, including unrelated files and subfolders.[8] The Sixth and Tenth Circuits, on the other hand, have subscribed to the theory that each folder on a partially searched computer is an individual container that carries with it a distinct expectation of privacy requiring either a warrant or an independent justification for a warrantless search.[9] *Riley* compels the conclusion that the latter approach is correct: just like cell phones themselves, the individual files in a computer or a cell phone can contain vast amounts of

7. Kyllo v. United States, 533 U.S. 27, 33-34 (2001).

8. *See infra* Part I.B.2.

9. *See infra* Part I.B.1. Some scholars have already examined a less-entrenched version of this circuit conflict in the context of searches conducted under valid warrants. *See* David J.S. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 846-49 (2005) (discussing the Tenth Circuit's approach); *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 554-57 (2005) (spending a few pages on the conflict). Since those articles were published in 2005, however, the Sixth and Seventh Circuits have issued opposing opinions deepening the split. *See infra* Part I.B.1-2. In addition, both of these pieces significantly predate *Riley*.

private information. To subject them to indiscriminate warrantless searches strikes at the very heart of Fourth Amendment protections.[10]

This Note proceeds in three Parts. Part I provides a brief overview of Fourth Amendment precedent on containers, describes the current divide among circuits, and outlines the Court's decision in *Riley*. Part II explains why *Riley* and the Fourth Amendment militate that the current circuit conflict be resolved in favor of more, not less, privacy protection of unopened computer files. It therefore proposes that each digital subcontainer should be considered protected by the Fourth Amendment. Finally, Part III examines two special doctrines for containers that lend further support to this Note's suggestion that conceptualizing individual files as containers provides a consistent and administrable rule to govern digital searches.[11] The Part concludes with a brief explanation of how this rule would look in practice when applied to a consent search, one of the most common forms of warrantless search conducted today.

I. Unpacking the Container Doctrine

The important question of containers—what counts as a container and therefore receives Fourth Amendment protection—arises throughout Fourth Amendment jurisprudence. This Part presents some doctrinal background on the container doctrine and the existing circuit split. Subpart A provides a brief historical overview of the relevant law. Subpart B delves deeper into how courts applied this law before *Riley* and how courts have approached so-called "subcontainers": containers that are themselves contained within larger packages. It explains the two views in the circuit split, the "virtual file" approach and the "physical device" approach. Subpart C describes the Court's

10. *See* Payton v. New York, 445 U.S. 573, 583 (1980) ("[I]ndiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment.").

11. Because the Fourth Amendment implications of the container doctrine are so broad, there are certain doctrines with which this Note does not concern itself. First, this Note is not concerned with searches of computers where the user arguably lacked a privacy interest in the first place. For example, it is not concerned with the potential individual liability of corporate employees who perform criminal acts on company computers. Second, this Note does not deal with the effect of third-party disclosures more generally. As Justice Sotomayor recently observed, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). Finally, this Note does not deal with the question of the permissible scope of seizures in the computer data context but only with the permissible scope of searches. So long as there is probable cause to believe a crime was committed, courts have generally permitted law enforcement officers to seize computers and examine their contents later. *See, e.g.*, Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001); United States v. Hay, 231 F.3d 630, 637-38 (9th Cir. 2000); Davis v. Gracey, 111 F.3d 1472, 1481 (10th Cir. 1997).

decision in *Riley* and sets the stage for the discussion of its application to digital subcontainers.

A. Containers and the Fourth Amendment

What constitutes a "container" for the purposes of the Fourth Amendment? The Supreme Court has defined a container as "any object capable of holding another object."[12] This simple definition alone tells us little beyond emphasizing how important it is to determine what constitutes a "container" and suggesting how vast and malleable that category might be.

The container doctrine itself, which recognizes a privacy interest in closed containers, owes its start to the bustling postal roads of the late nineteenth century. In *Ex parte Jackson*, the Court extended Fourth Amendment protections to sealed packages in the mail after Congress passed a law excluding certain items from postal delivery.[13] Enforcement of the new law would have permitted authorities to inspect closed envelopes and parcels.[14] Rejecting the notion that Congress had the power to authorize warrantless searches of those containers, Justice Field wrote that the packages were "as fully guarded from examination and inspection" as if they were still within the sender's home, and therefore any search of them must be "in subordination to the great principle embodied in the fourth amendment of the Constitution."[15]

The Court was not writing on a blank slate. The Fourth Amendment was a response to the British practice of issuing general warrants and writs of assistance, which empowered English authorities to "rummage through homes in an unrestrained search for evidence of criminal activity."[16] These writs of assistance—so called because they required "all officers and subjects of the Crown to assist in their execution"—gave investigators broad power to search and seize property with "practically absolute and unlimited" discretion.[17]

These much-hated searches often disregarded any expectation of privacy in containers. Section 5 of the Act of Frauds of 1662 expressly empowered English customs officials "to break open doors, Chests, Trunks & other Package[s]" and to seize the objects inside.[18] At the end of the seventeenth century, Parliament extended this authority to English officials in the

12. New York v. Belton, 453 U.S. 454, 460 n.4 (1981).

13. *See Ex parte* Jackson, 96 U.S. 727, 728, 733 (1878).

14. *See id.* at 735.

15. *Id.* at 733.

16. Riley v. California, 134 S. Ct. 2473, 2494 (2014).

17. NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 53-54 (1970).

18. M.H. SMITH, THE WRITS OF ASSISTANCE CASE 276 (1978).

American colonies,[19] and the pernicious language from the Act of Frauds reappears in several surviving writs issued in the colonies before the Founding. For example, a Massachusetts writ issued in 1762 authorized officers to "make diligent search into any trunk chest pack case truss or any other parcel or package whatsoever."[20] General warrants, by the same token, were often used to authorize searches of private homes and permitted the "breaking open" of "desks, boxes, &c., and searching and examining [of] papers."[21]

In 1761, Boston lawyer James Otis argued that writs of assistance were illegal in permitting unrestricted searches by officers of the Crown and allowing those officers to "break locks, bars, and every thing in their way."[22] Often, colonists specifically identified the invasiveness of searches as one of their grievances: a citizens' committee convened in November 1772 to "state the Rights of the Colonists" explicitly complained in its report that the "absolute and arbitrary" power conferred on investigators left colonists' "Boxes, Trunks and Chests broke open, ravaged and plundered."[23] The Framers' disdain for these invasive government searches animated the drafting and passage of the Fourth Amendment.[24] With such invasions in mind, the text of the Fourth Amendment protects citizens and their "persons, houses, papers, and effects" against unreasonable searches and overbroad warrants.[25]

A century after *Ex parte Jackson*, the Court reaffirmed the protected privacy interest in closed containers in *United States v. Chadwick*, determining it was unreasonable for investigators to search a double-locked footlocker in the

19. *See id.* at 16.

20. Specimen of 1762 Massachusetts Writ of Assistance, *in* SMITH, *supra* note 18, app. L, at 560; *see also* Writ of Assistance, Dec. 2, 1762, *in* DOCUMENTARY SOURCE BOOK OF AMERICAN HISTORY 1606-1913, at 105-09 (William MacDonald ed., new & enlarged ed. 1921).

21. Boyd v. United States, 116 U.S. 616, 626 (1886) (describing the famous English case of Entick v. Carrington (1765) 95 Eng. Rep. 807, 19 Howell's State Trials 1029).

22. Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 992, 1000-01 (2011) (quoting 2 THE WORKS OF JOHN ADAMS app. at 524-25 (Boston, Charles C. Little & James Brown 1850)). A young John Adams watched from the gallery. *Id.* at 996.

23. JOSIAH QUINCY, JR., REPORTS OF CASES ARGUED AND ADJUDGED IN THE SUPERIOR COURT OF JUDICATURE OF THE PROVINCE OF MASSACHUSETTS BAY, BETWEEN 1761 AND 1772, at 466-67 (Samuel M. Quincy ed., Russell & Russell 1969) (1865).

24. *See* Maryland v. King, 133 S. Ct. 1958, 1980-81 (2013) (Scalia, J., dissenting) (describing the history of the Fourth Amendment); JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES § 1005, at 709 (Boston, Hilliard, Gray & Co. 1833) (observing that the Fourth Amendment was "doubtless occasioned by the strong sensibility excited . . . upon the subject of general warrants almost upon the eve of the American Revolution").

25. U.S. CONST. amend. IV.

defendant's car without a warrant.[26] It later applied the same principle to unlocked luggage, observing that in the absence of a valid exception to the warrant requirement, allowing the police to search closed containers would impinge on the purpose of the Fourth Amendment.[27] As new situations have presented themselves, the Court has continued to guide law enforcement officers and judges by explaining how certain types of containers relate to the Court's various warrantless search doctrines.[28]

B. The Old Divide: The Virtual File Approach and the Physical Device Approach

By way of general summary, the Court's rule has been that the "touchstone" of the Fourth Amendment is "the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security."[29] It has further recognized that "[a] 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed" and has acknowledged that under the container doctrine outlined above, "sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."[30]

If that were the end of the matter, this Note would be much shorter. But the key question here is how to approach instances in which the government has already opened one container—a cell phone or computer—and now confronts the files inside. Does the government's initial intrusion into the device vitiate all expectation of privacy in the files, leaving them open to individual examination?

As Orin Kerr explains, "[t]he zone of a search determines the extent to which a particular search in a space eliminates privacy protection elsewhere in that space."[31] Federal courts of appeals have split over how broad this zone

26. *See* 433 U.S. 1, 11 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

27. *See* Arkansas v. Sanders, 442 U.S. 753, 759-60, 766 (1979), *overruled by Acevedo*, 500 U.S. 565.

28. *See, e.g.*, New York v. Belton, 453 U.S. 454, 460-61 (1981) (holding valid the search of any containers "open or closed" found in the passenger compartment of an arrestee's car).

29. Pennsylvania v. Mimms, 434 U.S. 106, 108-09 (1977) (quoting Terry v. Ohio, 392 U.S. 1, 19 (1968)).

30. United States v. Jacobsen, 466 U.S. 109, 113-14 (1984). This "reasonable expectation of privacy" standard, first defined in *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring), "posits a two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?" California v. Ciraolo, 476 U.S. 207, 211 (1986).

31. Kerr, *supra* note 9, at 554.

ought to be with respect to digital devices. That is, they disagree on how to address the uncertain scope of the government's authority to search devices and whether individuals maintain a reasonable expectation of privacy in the files on their computers or cell phones if *part* of those devices has already been searched.

1. The physical device approach: each device is a container

The Fifth and Seventh Circuits hold that discrete files on a computer are not individual containers and that investigators do not unconstitutionally expand the scope of a search if they open files on a device that has already been partially examined. Writing in 2005, Kerr called this the "physical device approach."[32] In *United States v. Runyan*, the defendant's wife was retrieving her belongings from his home after they separated.[33] While there, she saw approximately twenty disks that she believed were hers lying around a computer and, upon putting them in the computer, discovered they contained child pornography.[34] When she turned the disks over to the police, the police examined more files than she had, which led the defendant to claim that the police had unconstitutionally expanded the scope of the search.[35] Although the Fifth Circuit suppressed evidence discovered from disks she had not opened at all, it declined to suppress evidence found on the disks she had partially examined. It reasoned that once the contents of a container were partially examined, "an individual's expectation of privacy in the contents of a container has already been compromised" and therefore that "the police do not engage in a new 'search' for Fourth Amendment purposes each time they examine a particular item found within the container."[36]

In 2012, the Seventh Circuit adopted *Runyan*'s holding in *Rann v. Atchison*, determining the Fifth Circuit's approach struck the "proper balance" between the privacy interest "an individual retains in the contents of his digital media storage devices after a private search" and the degree to which government agents exceeded the scope of an earlier search of the defendant's computer drives by the defendant's daughter, S.R., and her mother.[37] The panel quoted the portion of *Runyan* in which the Fifth Circuit explained that its approach

32. Kerr, *supra* note 9, at 555.

33. 275 F.3d 449, 452-53 (5th Cir. 2001).

34. *Id.* at 453.

35. *Id.* at 460.

36. *Id.* at 465; *see also* United States v. Slanina, 283 F.3d 670, 680 (5th Cir.) (holding that an earlier warrantless search vitiated any expectation of privacy in the files remaining on the computer), *vacated on other grounds*, 537 U.S. 802 (2002).

37. 689 F.3d 832, 837 (7th Cir. 2012), *cert. denied*, 133 S. Ct. 672 (2012).

> is sensible because it preserves the competing objectives underlying the Fourth Amendment's protections against warrantless police searches. A defendant's expectation of privacy with respect to a container unopened by the private searchers is preserved unless the defendant's expectation of privacy in the contents of the container has already been frustrated because the contents were rendered obvious by the private search.[38]

Because the data in *Rann* had been partially examined by the private searchers, the Seventh Circuit dismissed the objection that police opened files the prior search did not, concluding that

> even if the police more thoroughly searched the digital media devices than S.R. and her mother did and viewed images that S.R. or her mother had not viewed, per the holding in *Runyan*, the police search did not exceed or expand the scope of the initial private searches. Because S.R. and her mother knew the contents of the digital media devices when they delivered them to the police, the police were "substantially certain" the devices contained child pornography.[39]

In other words, the court reasoned that because the partially searched drives contained *some* discovered contraband, the police could be "substantially certain" that other files contained the same material. Rann's privacy interest in *all* the files therefore vanished, and the police could proceed with a warrantless search of other, unopened files on the partially searched drives.[40]

A few courts other than the Fifth and Seventh Circuits have found the physical device approach persuasive, and they have arguably expanded the holdings of *Rann* and *Runyan* to cases where the contents of files are not "substantially certain." The District Court for the Southern District of New York, for example, cited *Runyan* in 2002 and adopted the position that "separate consent to search such an item [a closed container] found within a fixed premises is unnecessary."[41]

2. The virtual file approach: each file is a container

Opposing the physical device approach of the Fifth and Seventh Circuits, the Sixth and Tenth Circuits have held that each operation in which a folder or file is opened—"highlighted, clicked or otherwise manipulated so that its contents [go] from being unseen to exposed"[42]—constitutes a separate search.

---

38. *Id.* (quoting *Runyan*, 275 F.3d at 463-64).

39. *Id.* at 838 (quoting *Runyan*, 275 F.3d at 463).

40. *See id.*; *see also Runyan*, 275 F.3d at 464-65.

41. United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002).

42. United States v. Stabile, No. 08-145 (SRC), 2009 WL 8641715, at *8 (D.N.J. Jan. 21, 2009), *aff'd*, 633 F.3d 219 (3d Cir. 2011). In *Stabile*, the Third Circuit treated the opening of each file as a separate search in determining whether a search pursuant to a warrant exceeded the warrant's scope, *see Stabile*, 633 F.3d at 240-41, but ultimately held there was no Fourth Amendment violation.

Kerr calls this the "virtual file approach."[43] This approach strictly limits investigators' ability to expand the scope of their search to new areas of the computer, including unrelated, closed files. Under this theory, "[e]xposing to view concealed portions of a space in which one may be authorized to search constitutes an independent search from the initial invasion and must be validly supported by a warrant or, alternatively, by an exception to the warrant requirement."[44]

The leading case embracing this approach is *United States v. Carey*.[45] There, investigators received Patrick Carey's consent to search his apartment for evidence of drug trafficking and, finding two computers and multiple drugs during their search, promptly secured a warrant to search Carey's computers for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances."[46] While searching the computers, a detective came across a number of JPEG files and opened one, discovering child pornography.[47] At that point, according to his later testimony, he "developed probable cause to believe the same kind of material was present on the other image files."[48] Rather than securing a warrant, however, he downloaded approximately 244 images from Carey's computer to nineteen disks and opened "about five to seven" images on each disk to confirm they all contained child pornography.[49]

The district court rejected Carey's challenge to the search, but the Tenth Circuit reversed, holding that the detective had "temporarily abandoned" his authorized search in favor of expanding his search into other areas of the computer and "only 'went back' to searching for drug-related documents after conducting a five hour search of the child pornography files."[50] It brushed away the government's argument that searching Carey's computer was just like searching a filing cabinet and that the detective was authorized to conduct a broad search because he needed to open every "drawer."[51] Not only did the court note that the analogy was inapposite on the facts—the detective was fully aware that the image files would likely contain pornography rather than

43. Kerr, *supra* note 9, at 554.

44. *Stabile*, 2009 WL 8641715, at *8; *see also* United States v. Stierhoff, 477 F. Supp. 2d 423, 443-44 (D.R.I. 2007) (holding that opening a computer folder and viewing the contents "undoubtedly" constituted a search).

45. 172 F.3d 1268 (10th Cir. 1999).

46. *Id.* at 1270.

47. *Id.* at 1271.

48. *Id.*

49. *Id.*

50. *Id.* at 1271, 1273, 1276.

51. *Id.* at 1274-75.

evidence of drug trafficking—but it also observed that "[r]elying on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.'"[52] The panel reversed Carey's conviction and remanded, holding that the district court erred in refusing to suppress the evidence, which was the result of "an unconstitutional general search."[53]

Only a few years after *Carey*, the Tenth Circuit cited the decision and again observed the urgent need for a new paradigm in digital searches:

> The advent of the electronic age and, as we see in this case, the development of desktop computers that are able to hold the equivalent of a library's worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law. *See Carey*, 172 F.3d at 1274-75. This does not, of course, mean that the Fourth Amendment does not apply to computers and cyberspace. Rather, we must acknowledge the key differences and proceed accordingly.[54]

Carey's holding has been cited numerous times within the Tenth Circuit, which has observed that *Carey* is limited to its egregious facts but has reaffirmed that it "stands for the proposition that law enforcement may not expand the scope of a search beyond its original justification."[55]

In the absence of clear guidance from their circuit courts, district courts around the country have cited and applied *Carey* as well. The District Court for the Western District of Pennsylvania cited *Carey* in holding that when a consent search permitted investigators to search a computer for "['illegal'] credit card activity over the Internet," the government's argument that child pornography on the computer was in "plain view" failed because "[t]he image files were not understood to be the types of files to be opened and thus a search of image files was beyond the scope of the consented search."[56] Similarly, a Western District of New York decision explicitly rejected the notion that a partial search destroyed any expectation of privacy in individual computer files, noting that that reasoning "would permit the government to conduct a

52. *Id.* at 1275 (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 110 (1994)).

53. *Id.* at 1276.

54. United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).

55. United States v. Grimmett, 439 F.3d 1263, 1268-69 (10th Cir. 2006); *see also* United States v. Mann, 592 F.3d 779, 783-84 (7th Cir. 2010) (discussing the key bases for *Carey*'s holding).

56. United States v. Richardson, 583 F. Supp. 2d 694, 716 (W.D. Pa. 2008) (first alteration in original).

warrantless search of the entirety of a computer and all of its unopened files based upon the earlier identification of merely one contraband file or image."[57]

Before *Riley*, the Sixth Circuit applied a rule similar to the Tenth Circuit's in a case where an investigator exceeded her prior authorization to search a computer.[58] And although the Sixth Circuit has cited *Runyan* and *Rann* approvingly after *Riley*, it has not adopted the physical device approach. On the contrary, the circuit's rule appears to be in line with *Carey* and the virtual file approach.

In *United States v. Lichtenberger*, the defendant's girlfriend discovered child pornography on his laptop and contacted the police, showing an officer some of the defendant's files.[59] Neither she nor the officer, however, could recall whether the child pornography files she showed the officer were the same ones she had *initially* examined during her own private searches, or whether she opened new files in the officer's presence.[60] In the absence of a "virtual certainty" as to this issue and the individual files' contents, the Sixth Circuit suppressed the evidence, noting that the folders the defendant's girlfriend opened with the police, if not the same as the ones she had previously examined, could have contained "[o]ther documents, such as bank statements or personal communications . . . [or] internet search histories containing anything from Lichtenberger's medical history to his choice of restaurant."[61] Although the Sixth Circuit cited *Runyan* and *Rann*, it relied on the portion of *Runyan*'s discussion suppressing the evidence from the *unexamined* disks, rather than its holding—at issue here—that a *partial* examination of a particular container vitiates all expectation of privacy in its contents even if those contents have not been examined.[62] By assuming the defendant maintained an expectation of

57. United States v. Howe, No. 09-CR-6076L, 2011 WL 2160472, at *12-13 (W.D.N.Y. May 27, 2011), *report and recommendation adopted by* 2012 WL 1565708 (W.D.N.Y. May 1, 2012).

58. *See* United States v. Lucas, 640 F.3d 168, 179-80 (6th Cir. 2011) (distinguishing the case from *Carey* by observing that there was "no evidence" that the investigator "purposefully exceeded the scope of [the suspect's] consent to search for 'other material or records pertaining to narcotics'" when he stumbled across child pornography and noting how, "[w]hen thumbnail images suddenly appeared on the screen, [the investigator] enlarged just a few of them to be certain he was looking at child pornography" and "immediately stopped searching and called the CACU detectives, who then obtained [the suspect's] voluntary consent, and subsequently a search warrant, to seize and search the computers thoroughly for child pornography").

59. 786 F.3d 478, 480-81 (6th Cir. 2015).

60. *Id.* at 481, 488-89.

61. *Id.* at 489, 491.

62. *Id.* at 489. The Sixth Circuit somewhat elided the distinction between the two sets of disks in *Runyan*, addressing only the private search doctrine without mentioning the container doctrine itself. *See id.* ("Where the defendant's ex-wife had previously viewed files on a disk and confirmed they contained child pornography, . . . the [Fifth Circuit]
footnote continued on next page

privacy in the files his girlfriend had not previously examined, the Sixth Circuit's reasoning is more consistent with the virtual file approach than the physical device approach, and indeed the court discussed the privacy interests underlying *Riley* at length.[63]

C. *Riley* and *Wurie*: The Opinion and Underlying Searches

In *Riley v. California*, the Supreme Court consolidated two cases concerning the search-incident-to-arrest doctrine,[64] which generally permits law enforcement officials to conduct a warrantless search of an arrestee and his effects.[65] In both cases, officers searched the defendants' cell phones without a warrant, citing this exception as justification for the searches. At the time the Supreme Court granted certiorari, the Fourth, Fifth, and Seventh Circuits had authorized law enforcement officers to search cell phones without warrants during searches incident to arrest, as had the highest courts in Georgia, Massachusetts, and California.[66] Conversely, the First Circuit and the highest courts in Florida and Ohio all held that the Fourth Amendment forbade warrantless searches of cell phones in such cases.[67] The Supreme Court

---

upheld the police's after-occurring inspection. However, where the ex-wife had not viewed a disk, the police had no 'substantial certainty' regarding their contents, and the court found that those searches violated the Fourth Amendment." (citation omitted)).

63. *See id.* at 487-88.

64. 134 S. Ct. 2473, 2480-81 (2014).

65. *See* United States v. Robinson, 414 U.S. 218, 235 (1973) ("A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification. It is the fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment."); Chimel v. California, 395 U.S. 752, 763 (1969) (finding "ample justification" for "a search of the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence").

66. *See* Petition for a Writ of Certiorari at 11-12, *Riley*, 134 S. Ct. 2473 (No. 13-132) (citing United States v. Flores-Lopez, 670 F.3d 803, 809-10 (7th Cir. 2012); United States v. Murphy, 552 F.3d 405, 411-12 (4th Cir. 2009), *cert. denied*, 556 U.S. 1196 (2009); United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007), *cert. denied*, 549 U.S. 1353 (2007); People v. Diaz, 244 P.3d 501, 510 (Cal. 2011), *cert. denied*, 132 S. Ct. 94 (2011); Hawkins v. State, 723 S.E.2d 924, 926 (Ga. 2012); and Commonwealth v. Phifer, 979 N.E.2d 210, 216 (Mass. 2012)).

67. *Id.* at 12 (citing United States v. Wurie, 728 F.3d 1, 13 (1st Cir. 2013), *aff'd sub nom.* Riley v. California, 134 S. Ct. 2473 (2014); Smallwood v. State, 113 So. 3d 724, 735-36 (Fla. 2013); and State v. Smith, 920 N.E.2d 949, 956 (Ohio 2009), *cert. denied*, 562 U.S. 947 (2010)).

resolved the circuit conflict, unanimously[68] holding that the rationales justifying the search incident to arrest of physical objects—officer safety and the preservation of evidence—could not be extended to digital data.[69]

"Absent more precise guidance from the founding era," the Court weighed the privacy interest and the governmental interest at stake in the search of cell phones incident to arrest.[70] It ultimately concluded that neither of the conventional justifications for searches incident to arrest applied, given that the search of "vast quantities" of information on a cell phone "bears little resemblance" to the conventional search of physical objects.[71] Because the information on cell phones differs "in both a quantitative and a qualitative sense" from other objects an arrestee might carry, the Court rejected the idea that a search of a cell phone was indistinguishable from a search of a cigarette pack, wallet, or purse.[72] On the contrary, the Court suggested that cell phones are more like voluminous trunks than "container[s] the size of [a] cigarette package," although both easily fit into an arrestee's pocket.[73] To that end, "[t]reating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained."[74] In other words, due to the type and volume of private data that digital storage devices ordinarily contain, they constitute a particular type of container requiring particular solicitude in at least some warrantless searches.[75]

Although the Court did not render an opinion about the permissible scope of the digital searches *within* the particular devices, the facts underlying the two cases underscore that investigators conducting digital searches will likely explore many different areas of a suspect's computer or cell phone. In *People v. Riley*, California police initially stopped David Riley for driving with expired tags and discovered he was also driving with a suspended license.[76] When Riley was arrested, the arresting officer accessed Riley's phone contacts and noticed

68. Chief Justice Roberts wrote the opinion of the 9-0 Court, *Riley*, 134 S. Ct. 2473, and Justice Alito wrote a separate concurring opinion, *id.* at 2495 (Alito, J., concurring in part and concurring in the judgment).

69. *Id.* at 2484-85 (majority opinion).

70. *Id.* at 2484.

71. *Id.* at 2485.

72. *Id.* at 2489.

73. *Id.*

74. *Id.* at 2491 (defining a "container" as "any object capable of holding another object" (citing New York v. Belton, 453 U.S. 454, 460 n.4 (1981)).

75. At the end of his opinion for the Court, Chief Justice Roberts noted that although the search-incident-to-arrest exception did not authorize the warrantless search of cell phones, "other case-specific exceptions" might still permit a warrantless search. *Id.* at 2494 (identifying the exigent circumstances exception as one such doctrine).

76. People v. Riley, No. D059840, 2013 WL 475242, at *2 (Cal. Ct. App. Feb. 8, 2013), *rev'd and remanded*, 134 S. Ct. 2473 (2014).

that "all of the entries starting with the letter 'K' were preceded by the letter 'C,' which gang members use to signify 'Crip Killer.'"[77] On this basis, the officer gave the phone to a detective specializing in gangs, who searched the phone and discovered both videos and photos pointing to Riley's gang affiliation.[78]

The record provides little evidence on *how* the detective searched Riley's phone, and the exact methods employed were not at issue in the case. The California Court of Appeal wrote that the detective "looked through the phone,"[79] and the trial record provides only the detective's testimony that he "went through [Riley's] cell phone."[80] Both the detective's later statements[81] and the fact the officers viewed and downloaded a variety of photos and videos,[82] however, suggest the search thoroughly explored various files and areas within the phone.

In *United States v. Wurie*,[83] the precise steps taken to search the defendant's phone are somewhat clearer. The Supreme Court recorded that after officers observed Brima Wurie engaging in a drug sale and arrested him,

> the officers noticed that [Wurie's "flip phone"] was repeatedly receiving calls from a source identified as "my house" on the phone's external screen. A few minutes later, they opened the phone and saw a photograph of a woman and a baby set as the phone's wallpaper. They pressed one button on the phone to access its call log, then another button to determine the phone number associated with the "my house" label.[84]

In its opinion, the First Circuit was even more descriptive. It noted that when the repeated calls came in, "[t]he officers were able to see the caller ID screen, and the 'my house' label, in plain view."[85] The photograph of the woman and baby was visible "[i]mmediately upon opening the phone," and the officers only

77. *Id.* at *3; *see also* Direct Examination of Charles Dunnigan, Joint Appendix at 8, *Riley*, 134 S. Ct. 2473 (No. 13-132) ("I noticed that everything that started with a K was preceded by a C. And it's my experience that gang members typically write a C and a K to stand for Crip Killer.").

78. *Riley*, 2013 WL 475242, at *3.

79. *Id.*

80. Direct Examination of Duane Michael Malinowski, Joint Appendix at 11, *Riley*, 134 S. Ct. 2473 (No. 13-132).

81. *See id.* ("There's a lot of stuff on his cell phone . . . .").

82. *See id.* at 14 ("The videos were downloaded, along with a bunch of photos.").

83. 728 F.3d 1 (1st Cir. 2013), *aff'd sub nom.* Riley v. California, 134 S. Ct. 2473 (2014).

84. *Riley*, 134 S. Ct. at 2481.

85. *Wurie*, 728 F.3d at 2. The opinion goes on to note that Wurie conceded that under the plain view exception, "the officers were entitled to take notice of any information that was visible to them on the outside of the phone and on its screen (including, in this case, the incoming calls from 'my house')." *Id.* at 3 n.1. The plain view exception, and its application to digital subcontainers, is discussed later in this Note. *See infra* Part III.A.

needed to press two buttons to access the information they ultimately used.[86] Notwithstanding the narrow nature of this particular search, the panel held that the rationale underlying the Fourth Amendment required a warrant to search cell phones, even those seized incident to arrest.[87] And, as we know, the Supreme Court agreed.

II. Applying *Riley*: The Virtual File Approach Must Win Out

This Part explains why the Court's decision in *Riley* must be read to endorse the "virtual file" approach adopted by the Sixth and Tenth Circuits rather than the "physical device" approach of the Fifth and Seventh Circuits. This is the best resolution in light of *Riley*, the history and principles behind the Fourth Amendment, and the policy considerations inherent in the ever-advancing nature of digital storage. Adopting the virtual file approach is in keeping with what Kerr calls "equilibrium-adjustment," in that the virtual file approach most effectively "maintain[s] the role of the Fourth Amendment as changing technology and social practice threaten to alter the function of preexisting Fourth Amendment rules."[88] It creates a rule that both is practical to apply even as the nature of digital storage changes and adequately protects the myriad pieces of personal information that modern technologies collect.

A. The Virtual File Approach Follows Naturally from *Riley*

The Court's reasoning in *Riley* compels the conclusion that some privacy interest must inhere in individual virtual files within computers and cell phones in addition to the overall devices themselves. *Riley* dealt with the initial search of a cell phone incident to arrest.[89] That is, it dealt with whether the police could "open" and search a cell phone in the first instance, without drawing a distinction between the types of data on the phone. But its reasoning applies with equal force to individual digital files within a cell phone or computer when police seek to search those digital subcontainers without a warrant.

A straightforward application of the container doctrine would consider a person's phone a large container and view the individual digital files on the phone as subcontainers. Under this theory, we might expect a search of the phone itself to allow investigators to open the files and folders within. In *United States v. Ross*, for example, the Court opined that "[a] warrant to open a

86. *Wurie*, 728 F.3d at 2.

87. *Id.* at 13-14.

88. Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 290 (2015).

89. *Riley*, 134 S. Ct. at 2482.

footlocker to search for marihuana would also authorize the opening of packages found inside."[90] Instead of drawing a difficult-to-administer constitutional distinction between "worthy" and "unworthy" containers, the Court determined that probable cause to search essentially vitiated the privacy interests in nested containers and declined to require that officers secure a new warrant every time they open a package to find another box.[91] Rather, "[w]hen a legitimate search is under way, and when its purpose and its limits have been precisely defined, nice distinctions between [individual containers] . . . must give way to the interest in the prompt and efficient completion of the task at hand."[92] The implication is that once a container has been opened, the search legitimately extends to everything inside it, including smaller containers. This approach would in essence be the physical device approach, rooted in the idea that once a device is breached by investigators, no reasonable expectation of privacy remains in any of its contents. The key question after *Riley* is whether, in the absence of a warrant, this rule applies to the individual files on computers.

I propose that *Riley* gives us good reason to think this physical subcontainer rule does not apply to digital subcontainers like the files and folders found on individuals' computers. As *Ross* also made clear, the traditional physical search rule is premised on a key assumption about physical containers—that it is clear at the outset where "the object of the search may be found."[93] This serves as an important and useful check on many warrantless physical searches. For example, a search for weapons does not allow the government to open a suspect's letters;[94] a search for undocumented immigrants does not allow authorities to conduct a warrantless search of a suitcase.[95]

---

90. 456 U.S. 798, 821 (1982).

91. *Id.* at 821-22.

92. *Id.* at 821.

93. *Id.* at 820; *see also* United States v. Marshall, 348 F.3d 281, 288-89 (1st Cir. 2003) (holding that the viewing of videotapes was within the scope of a consent search because it was reasonably related to the object of searching for evidence of stolen video equipment); United States v. Rudolph, 970 F.2d 467, 469 (8th Cir. 1992) (holding that the search of a car for bottles of alcohol that revealed a gun behind the car seat was appropriate because an officer might reasonably expect to find a bottle of alcohol in that location); United States v. Milian-Rodriguez, 759 F.2d 1558, 1563-64 (11th Cir. 1985) (noting that, in a consent search for papers and files, searching a closet next to the defendant's desk might have been appropriate); United States v. Dichiarinte, 445 F.2d 126, 129 (7th Cir. 1971) (holding that consent to a narcotics search did not allow investigators to read the defendant's papers).

94. Winfield v. Trottier, 710 F.3d 49, 55 (2d Cir. 2013) (determining that consent to the search of a car where the trooper asked about guns and money did not allow the trooper to open a letter found in the car).

95. *See Ross*, 456 U.S. at 824 ("Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom,

footnote continued on next page

It is harder, however, to define the scope of a reasonable warrantless search when the container is digital, precisely because it is difficult to tell from the outside what a particular file or folder contains. Although a computer can be analogized to a container, this analogy fails to convey the fact that a computer also holds smaller, individual containers in the form of discrete files. "Each individual container, or discrete file, . . . potentially contains personal or business information entirely unrelated to that stored in the other containers."[96] As such, some courts have recognized the significant risk that "a search for one type of information will often reveal a tremendous amount of other unrelated information."[97]

It was exactly this uncertainty upon which the Court relied in *Riley* to determine that cell phones themselves were a special kind of container, one which "generally require[s]" a warrant to search.[98] It emphasized that "[w]ith all they contain and all they may reveal," cell phones "hold for many Americans 'the privacies of life.'"[99]

Indeed, by recognizing that phones are *special* containers, *Riley* endorses exactly the type of distinction between "worthy" and "unworthy" containers the Court previously rejected in *Ross*.[100] Rather than following a straightforward application of the container doctrine, the *Riley* Court articulated a new rule for digital devices, rejecting the analogy to physical objects and declaring that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[101] These privacy concerns spring from the "immense storage capacity" of cell phones, the conclusions about the "sum of an individual's private life" that may be drawn from cell phone information, and the "element of pervasiveness that characterizes cell phones but not physical records."[102] In addition, the Court observed that the information in cell phones, like browsing history or installed software, is "qualitatively different" from physical evidence because it implicates "detailed information about all aspects of a person's

probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase. Probable cause to believe that a container placed in the trunk of a taxi contains contraband or evidence does not justify a search of the entire cab.").

96. United States v. Stierhoff, 477 F. Supp. 2d 423, 443 (D.R.I. 2007).

97. *Id.*

98. Riley v. California, 134 S. Ct. 2473, 2493 (2014).

99. *Id.* at 2494-95 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

100. *Ross*, 456 U.S. at 822.

101. *Riley*, 134 S. Ct. at 2488-89. The Court also observed that saying physical and digital searches are materially indistinguishable is "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Id.* at 2488.

102. *Id.* at 2489-90.

life."[103] All of these considerations apply as strongly to digital subcontainers, like individual folders or files, as they do to cell phones as a whole.

1. *Riley*'s quantitative considerations apply to digital subcontainers

In Disney's 1964 film *Mary Poppins*, the eponymous governess sets her carpetbag on a table and removes a full-size hat stand, a wall mirror, a potted plant, and a floor lamp, much to the amazement of Jane and Michael Banks.[104] Seeing their astonishment, she chides them: "Never judge things by their appearance. Even carpetbags. I'm sure I never do."[105] This lesson applies to digital subcontainers as well: when opened, they might contain a single page—or an entire library.

If the storage capacity of cell phones presents a reason for strong privacy protection, then that reason is only magnified for laptop and desktop computers, which can store much more information. In *Riley*, the Court emphasized the privacy implications of devices with 16 to 64 gigabytes of memory, observing that 16 gigabytes translated in practical terms to "millions of pages of text, thousands of pictures, or hundreds of videos."[106] But many cell phones also "sync" with computers, copying all of their contents to a personal computer to back up their data or allow uploading and downloading of the same photos and videos that concerned the Court. Today, Apple's largest iPhone has a total internal memory capacity of 256 gigabytes.[107] But even this increase in capacity is dwarfed by the capacity of laptop and desktop computers. Affordable external hard drives can now store up to 4 terabytes of data, more than two hundred times as much as the 16-gigabyte phone in *Riley*.[108]

Imagine a hypothetical computer drive containing three folders, each of which is 300 gigabytes. The mere fact that these separate folders are stored on a single device does not diminish the quantity of private information each folder holds. From a user's perspective, folders are essentially independent of each other in their virtual space—they are accessed through different clicks of the mouse or by highlighting different icons, and they presumably all contain different files. In such circumstances, it makes little sense to follow *Runyan* and hold that searching one folder would necessarily vitiate the owner's privacy

103. *Id.* at 2490.

104. MARY POPPINS (Walt Disney 1964).

105. *Id.*

106. *Riley*, 134 S. Ct. at 2489.

107. *Compare iPhone Models*, APPLE, http://www.apple.com/iphone/compare (last visited Jan. 1, 2017).

108. *Storage*, APPLE, http://www.apple.com/shop/mac/mac-accessories/storage (last visited Jan. 1, 2017).

interest in the others. The fact that the government is authorized to search one of the folders ought not expose the other two folders to view, thereby revealing a huge quantity of potentially personal information under what began as a narrow and targeted search.

As time passes and hard drives get larger, *Riley*'s concern about data quantity will only grow more important. The storage capacity of computers and hard drives will increase, and the size of subcontainers within them will increase as a result. This rapid expansion in storage capacity counsels in favor of adopting the virtual file approach. More and more private information will be exposed under the physical device approach if a single contraband file "poisons the well" and allows warrantless examination of storage devices. When storage capacity was smaller, the physical device approach meant that viewing a single file on a device threatened to reveal many megabytes of data that otherwise would have been protected by the owner's expectation of privacy. Today, on larger drives, a search of a single file might destroy the privacy interest in many hundreds of *gigabytes* of data. Assuming storage capacity continues to increase,[109] the privacy implications of the physical device approach will only grow in the future. The one searched file will be more than just a drop poisoning the well; it will become a drop poisoning the ocean.

This concern is even more pointed in the increasingly prevalent context of cloud storage. In *Riley*, the Court described cloud computing as "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself."[110] Web-based e-mail services are now cloud-based, storing users' e-mails on large servers rather than storing them "locally" on an individual user's device.[111] Individuals or businesses can augment the storage capacity of their devices by using services like Box, Google Drive, or Dropbox, which provide additional storage for files, photos, videos, or whatever else the user may need to store. In 2013, one research firm estimated that there was 1 *exabyte* of data stored in the cloud—the equivalent of 1,073,741,824 gigabytes, or

109. This is a safe assumption. *See, e.g.*, Chip Walter, *Kryder's Law*, SCI. AM. (Aug. 1, 2005), http://www.scientificamerican.com/article/kryders-law (describing a "50-million-fold increase" since 1956 in the density of information that a standard disk drive is capable of storing).

110. *Riley*, 134 S. Ct. at 2491. Rather than storing files and data "locally"—that is, on a particular physical device—cloud computing allows users to store files on a server and access them from anywhere.

111. *See generally* Gabriel R. Schlabach, Note, *Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act*, 67 STAN. L. REV. 677, 686-90 (2015) (describing cloud-based services and the types of data they may collect on consumers).

67 million times the storage capacity of the cell phone the Court confronted in *Riley*.[112]

In *Riley*, the United States conceded that the search-incident-to-arrest exception would not allow a warrantless search of cloud storage.[113] The Court observed that "[s]uch a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house" because it might not be clear on a cell phone which information is stored locally and which files are stored in the cloud.[114] It further suggested that the analogy to physical containers "crumbles entirely" when a computer or cell phone allows investigators to access information that is actually stored elsewhere.[115]

But a major advantage of the virtual file approach is that the location of the digital data—whether local or in the cloud—is essentially irrelevant to whether a file may be permissibly searched. Even in the cloud, individual files and folders remain distinct from each other, easily distinguishable both by law enforcement during the course of warrantless searches and by courts reviewing those searches after the fact.

The physical device approach, on the other hand, results in absurd consequences based solely on where a particular file or folder happens to be stored. Because searching a file has the effect of opening the entire device to further examination, the precise configuration of local and cloud storage may affect both which files may be searched and whether, when law enforcement agents open files stored in the cloud, they are thus permitted to expand their searches into other cloud-based files. Particularly when it may not be immediately clear which files are stored locally and which are stored in the cloud,[116] pegging the privacy interest in a particular file to its location makes little sense. It would lead to substantial confusion for both investigators and reviewing courts—not to mention arbitrary deprivations of privacy for particular individuals based on where and how their data are stored.

Furthermore, the notion of a physical device breaks down when it comes to cloud computing. Files in the cloud are stored on company servers that may

112. John Callaham, *Research Firm: Over 1 Exabyte of Data Is Now Stored in the Cloud*, NEOWIN (Feb. 20, 2013), http://www.neowin.net/news/research-firm-over-1-exabyte-of-data-is-now-stored-in-the-cloud.

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

114. *Id.*

115. *Id.*

116. *See id.* ("[O]fficers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud.").

be anywhere in the world.[117] These files are stored on the same hardware as many other customers' data, and a single customer's files might be scattered across multiple servers in many different data centers in a technique known as "distributed storage."[118] If the privacy interest in a file hinges on the physical device in which it is stored, the cloud storage world quickly becomes incomprehensible to the Fourth Amendment. If privacy doesn't inhere in individual digital files, in other words, it quickly ceases to exist at all in a cloud-based world applying the physical device approach. In that world, searching any single file vitiates the privacy interest in everything else on the shared cloud storage server—a nonsensical result.

2. *Riley*'s qualitative considerations apply to digital subcontainers

In holding that the data on cell phones differ qualitatively from information that can be obtained from physical searches, the Court observed that cell phones contain "detailed information about all aspects of a person's life."[119] In our increasingly digital world, digital files record more and more of our everyday experience. As Kerr observes, computers today are "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more."[120] In recognition of this phenomenon, the Court's privacy jurisprudence has been tinged in recent years by the so-called "mosaic theory," which recognizes that when aggregated, even small and individually innocuous pieces of data can paint a revealing picture about a person.[121]

This concern is sharpest for cell phones, which are, as the Court noted, "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."[122] But it applies with equal force to the files found on myriad other digital devices. As common as cell phones are, other types of personal computers are similarly ubiquitous. A Pew Research survey showed that even though the

117. Google, for example, operates fifteen data centers across the Americas, Asia, and Europe. *Data Center Locations*, GOOGLE, http://www.google.com/about/datacenters/inside/locations/index.html (last visited Jan. 1, 2017).

118. Sean Gallagher, *The Great Disk Drive in the Sky: How Web Giants Store Big—And We Mean* Big—*Data*, ARS TECHNICA (Jan. 26, 2012, 6:00 PM), http://arstechnica.com/business/2012/01/the-big-disk-drive-in-the-sky-how-the-giants-of-the-web-store-big-data.

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

120. Kerr, *supra* note 9, at 569.

121. *See generally* Jace C. Gatewood, *District of Columbia* Jones *and the Mosaic Theory—In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory*, 92 NEB. L. REV. 504, 506-10 (2014) (describing the development and application of the mosaic theory).

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

percentage of the population that owns a smartphone has increased, the percentage that owns a laptop or desktop computer has remained constant in the high-70% range.[123] This suggests that even as smartphones become more popular, they are not substitutes for other devices. Fully "eight in ten U.S. adults (81%) say they use laptop and desktop computers somewhere in their lives—at home, work, school, or someplace else"—compared to the 58% of U.S. adults who own a smartphone.[124]

In addition, the voluminous and wide-ranging information that cell phones collect is equally likely to be present on stationary computers and servers, even if those storage devices are not constantly carried around with their owners. Syncing a cell phone to a home computer or the cloud will copy all of the sensitive information from the portable device to the stationary one. The fact that the information is no longer stored on a person's body should not reduce the privacy interest inherent in it. While storage on a stationary device means that information is unlikely to be the subject of a warrantless search incident to arrest, other types of warrantless searches may nonetheless reach desktop or laptop computers.

Further, stationary computers may contain sensitive and private information over and above what they sync from cell phones. Digital records of writing or watching habits may be more detailed on personal computers: many people prefer to generate content or consume media on personal computers rather than tablets or smartphones, owing to their more effective keyboards, speakers, and screens.[125] Consumers also prefer to do online banking from their personal computers rather than from mobile devices.[126] Similarly, web search habits may be more revealing on personal computers because people tend to conduct longer and more thorough web searches on their desktop computers than from their mobile devices.[127] The mere fact that certain devices are not carried on the person at all times does not necessarily mean that they do not contain a startling breadth of private information deserving of Fourth Amendment protection.

---

123. *See Device Ownership over Time*, PEW RES. CTR., http://pewrsr.ch/1m8siWD (last visited Jan. 1, 2017).

124. Susannah Fox & Lee Rainie, *Part 1: How the Internet Has Woven Itself into American Life*, PEW RES. CTR. (Feb. 27, 2014), http://pewrsr.ch/1mIfB5b.

125. *See* Quentin Fottrell, *PCs Outsell Tablets in College Dorms*, MARKETWATCH (July 31, 2013, 2:21 PM ET), http://on.mktw.net/2e4tQT8 ("You can't write a 10-page research paper with an iPad.").

126. *See* Jim Tierney, *Customers Still Prefer Laptops and Desktops to Smartphones and Tablets*, LOYALTY360 (Feb. 5, 2014), https://shar.es/1E4MOY.

127. *See* Madalina Lambrea, *Mobile vs Desktop: 13 Essential User Behaviors*, APPTICLES (Mar. 5, 2016), https://www.appticles.com/blog/2016/03/mobile-vs-desktop-13-essential-user-behaviors.

Finally, a privacy distinction between different devices that depends on how frequently the owner has a device with her will quickly become unworkable in practice. Trying to draw distinctions between different classes of digital containers or subcontainers invites the type of nonuniformity and unpredictability that *Riley* sought to avoid.[128] Laptops and other portable computing devices like tablets and e-readers have many of the same functions as cell phones and stationary computers—they can store documents, photographs, web browser histories, and software. But how much and how frequently individuals use these devices can vary widely; many consumers carry these devices around with them, while others prefer to use their laptops only in their homes, treating them as if they were traditional desktop computers. Attempting to distinguish between different classes of digital devices, where searches of files on each would be governed by different rules, would be an excruciating exercise in line drawing.

B. The Virtual File Approach Has a Sound Basis in History

Besides the considerations expressed in *Riley*, there are other strong reasons to prefer the virtual file approach over the physical device approach. The strong privacy protections of the virtual file approach are consistent with the text and structure of the Fourth Amendment and find support in the common law prohibition on exploratory searches of private papers.

This Note has already discussed the history of the Fourth Amendment as a reaction to the much-hated general warrants and writs of assistance that permitted government actors to search indiscriminately through colonists' homes and possessions.[129] Strong privacy protections, like the presumption that searching all files requires either valid warrants or valid warrant exceptions, are consistent with the historical underpinnings of the Fourth Amendment. In particular, the virtual file approach finds support in two major doctrinal analyses of the Fourth Amendment: the Amendment's general preference for warrants and what David Sklansky has called the Court's "new Fourth Amendment originalism."[130]

128. *See* Riley v. California, 134 S. Ct. 2473, 2491 (2014) (noting the Court's "general preference to provide clear guidance . . . through categorical rules").

129. *See supra* Part I.A; *see also Riley*, 134 S. Ct. at 2494. For a brief but general history of the Fourth Amendment, see 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1(a) (5th ed. 2012).

130. David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1744 (2000).

1. Warrant preference

Much of the discussion until now has been of warrantless searches, but such searches are the exception, not the rule. In the colonial period, "general, promiscuous intrusion by government officials provided the standard method of search and seizure in . . . America."[131] Colonial Americans "strongly resented" the writs and warrants that exposed their homes and effects to ransacking searches,[132] and after the Revolution, the Framers seized upon the opportunity for change. Rather than committing the discretion to investigators to search through personal homes, papers, and effects, the Framers wrote the warrant requirement into the Fourth Amendment to embody their determination that "[s]ecurity against unlawful searches is more likely to be attained by resort to search warrants than by reliance upon the caution and sagacity of petty officers while acting under the excitement that attends the capture of persons accused of crime."[133]

The Warrant Clause of the Fourth Amendment, providing that no warrant shall issue without probable cause, displays a "strong preference for searches conducted pursuant to a warrant."[134] Searches conducted without a judicially approved warrant are "*per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[135] The Justices have repeatedly emphasized that the warrant requirement was a tool implemented by the Founders as a "safeguard against recurrence of abuses so deeply felt by the Colonies as to be one of the potent causes of the Revolution."[136] Its purpose is to require that inferences through which citizens' privacy might be impinged "be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime."[137]

This preference for warrants means that, when faced with a new technology or situation, the Court should generally err in favor of *more* privacy

131. Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 939 (1997) (highlighting colonial laws affording officials broad power to search and seize without warrants).

132. *Id.* at 955.

133. United States v. Lefkowitz, 285 U.S. 452, 464 (1932).

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

135. Katz v. United States, 389 U.S. 347, 357 (1967) (footnote omitted); *see also* United States v. Rabinowitz, 339 U.S. 56, 70 (1950) (Frankfurter, J., dissenting) ("When the Fourth Amendment outlawed 'unreasonable searches' and then went on to define the very restricted authority that even a search warrant issued by a magistrate could give, the framers said with all the clarity of the gloss of history that a search is 'unreasonable' unless a warrant authorizes it, barring only exceptions justified by absolute necessity.").

136. *Rabinowitz*, 339 U.S. at 69 (Frankfurter, J., dissenting).

137. Johnson v. United States, 333 U.S. 10, 14 (1948).

protection rather than carving out a new warrant exception.[138] Thus, the virtual file approach's general rule that warrants are required to search individual files or folders is in keeping with the scheme the Founders laid out. Indeed, *Riley* validates this approach, observing that "[o]ur cases have historically recognized that the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'"[139] Based on the historical ambivalence toward broad investigatory discretion, the interest in requiring judicially issued warrants is heightened where a single officer might otherwise have free rein over voluminous private information. Consider the facts of *Carey*, where an officer "abandoned" his authorized search and spent five hours looking through the defendant's computer files.[140] Requiring warrants, rather than permitting general warrantless examinations on the whims of individual investigators, best promotes the Court's warrant-preference precedent and the intent of the Warrant Clause.

Some scholars have argued that the warrant and probable cause requirements are "toothless" and impose little real limitation on government action.[141] That is a broad charge, well outside the scope of this Note. Assuming it is true, though, all the better to have a doctrine that offers protection against warrantless searches and requires officers to incur some additional cost, however minimal, before exposing private files to view.

2. New Fourth Amendment originalism

A protective approach to digital subcontainers is also in keeping with common law tradition. David Sklansky persuasively argues that the Supreme Court has been slowly changing its approach to Fourth Amendment violations, increasingly engaging in a "new Fourth Amendment originalism" that "represent[s] the culmination of a campaign fought for close to a decade by Justice Scalia, assisted latterly by Justice Thomas."[142] Under this approach, the

138. Erring on the side of more protections is also prudent because

> a wrong turn by the Court in an area of developing technology may now be difficult to correct: if the Court rules early on that there is no protection for a new technology, defendants may be much less likely to challenge that precedent given the low (if not zero) chances of relief.

Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 542 (2011).

139. Riley v. California, 134 S. Ct. 2473, 2493 (2014) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

140. United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).

141. *See, e.g.*, Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1347 (2012).

142. Sklansky, *supra* note 130, at 1813.

Court asks whether a government action "was regarded as an unlawful search or seizure under the common law when the Amendment was framed" in order to determine whether it passes constitutional muster.[143] In 2012's *United States v. Jones*, for example, the Court used this approach to invalidate a high-tech search—the government's warrantless placement of a GPS tracking device on a defendant's car—on the rationale that the physical intrusion onto the defendant's property satisfied the elements of common law trespass to chattel.[144]

The Court seems unlikely to apply this approach to digital subcontainers, given that it noted in *Riley* an absence of "precise guidance from the founding era."[145] Nonetheless, drawing a connection between personal files and private papers, the logic of the common law suggests by analogy that a broad search of computer files is impermissible under the Fourth Amendment. This reasoning—though it casts computer files as private papers rather than subcontainers—bolsters the virtual file approach's view that each file should be protected rather than being exposed to general searches under the physical device approach.

At common law, citizens could bring trespass or false imprisonment suits to penalize officials who conducted searches or seizures that were not authorized by law.[146] As described above,[147] general warrants and writs of assistance permitted the breaking of containers and the examination of private papers, with few limits.[148] But in the few decades before the Revolution, English courts dramatically limited the ability of officers to search and seize private papers.

One of the most famous cases of the time, *Entick v. Carrington*,[149] dealt directly with the seizure of private papers and has been cited repeatedly by the Supreme Court as the "wellspring of the rights now protected by the Fourth Amendment."[150] In that case, officials seeking evidence of libel ransacked Entick's home, "read through Entick's books and papers, and seized several hundred pamphlets and charts."[151] Lord Camden's opinion upheld Entick's

143. Wyoming v. Houghton, 526 U.S. 295, 299 (1999).

144. *See* 132 S. Ct. 945, 949-50 (2012).

145. Riley v. California, 134 S. Ct. 2473, 2484 (2014).

146. *See* Maclin, *supra* note 131, at 932-33.

147. *See supra* Part I.A.

148. *See* Sklansky, *supra* note 130, at 1799.

149. (1765) 95 Eng. Rep. 807, 19 Howell's State Trials 1029.

150. Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 873 (1985) (quoting Stanford v. Texas, 379 U.S. 476, 484 (1965)); *see also, e.g.*, Boyd v. United States, 116 U.S. 616, 626 (1886).

151. Schnapper, *supra* note 150, at 880.

trespass claim against the officers, holding that although some searches are permitted in the interest of justice, "[i]f searches and seizures of papers were permitted, 'the secret cabinets and bureaus of every subject in this kingdom will be thrown open to the search and inspection of a messenger,' and an individual's 'most valuable secrets' could be exposed to government scrutiny."[152]

Entick's holding was digested into Founding-era legal manuals in the colonies to stand for the proposition that warrants to seize papers were "unknown to the common law."[153] Furthermore, in 1886, the Supreme Court recapped the *Entick* opinion in *Boyd v. United States* and observed that the principles in *Entick* "affect[ed] the very essence of constitutional liberty and security."[154] The Court specifically noted that in *Entick* the search involved the "opening [of] boxes and drawers," which it called a "circumstance[] of aggravation."[155] It held that "any forcible and compulsory extortion of a man's . . . private papers to be used as evidence to convict him of crime . . . is within the condemnation of [*Entick*'s] judgment"—and, by extension, the Fourth Amendment.[156]

One pamphlet published two years before *Entick* parallels the privacy concerns that arise today with respect to digital devices and files. At one point, the anonymous author describes the many types of private information that may be revealed by a general search of a man's papers:

> Our honour and fame, our estates, our amusements, our enjoyments, our friendships, *are*, and even our vices *may be*, there: things that men trust none with, but themselves; things upon which the peace and quiet of families, the love and union of relations, the preservation and value of friends, depend.[157]

Compare this enumeration with the privacy concerns that the *Riley* opinion identifies as being implicated by the applications on mobile phones:

> There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for

---

152. *Id.* at 880-82 (footnotes omitted) (quoting *Entick*, 19 Howell's State Trials at 1063-64).

153. Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 75 (2013) (examining Founding-era manuals for justices of the peace); *see also* Schnapper, *supra* note 150, at 884 ("Hargrave's 1775 annotation describes the *Entick* decision both as 'against the seizure of papers' and as holding that 'a warrant to search for and seize the papers of the accused, in the case of a seditious libel, is contrary to law.'" (footnote omitted) (quoting *Entick*, 19 Howell's State Trials at 1029, 1075-76)).

154. Boyd v. United States, 116 U.S. 616, 630 (1886).

155. *Id.*

156. *Id.*

157. Schnapper, *supra* note 150, at 890 (quoting A LETTER TO THE RIGHT HONOURABLE THE EARLS OF EGREMONT AND HALIFAX, HIS MAJESTY'S PRINCIPAL SECRETARIES OF STATE, ON THE SEIZURE OF PAPERS 9 (London, 1763)).

> tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life.[158]

The similarity between the two lists is striking. Personal papers in 1763 and digital files today implicate the same interests: financial information, romantic matters, embarrassing vices or habits, and other private facets of life that made searches of papers impermissible under the common law. If the Court is called upon to apply originalism in the digital realm, these considerations suggest that a warrantless search of files would be impermissible trespass and thus forbidden by the Fourth Amendment.

III. Applying the Container Doctrine to Individual Files

This Note has argued in favor of conceptualizing digital files as "subcontainers," thereby recognizing some protectible privacy interest in their contents equivalent to the protections suggested by *Riley*. Accepting files as a type of special, protectible subcontainer under *Riley* has a number of advantages, chief among which is that courts can apply a robust body of existing law on containers to resolve questions about digital searches as they arise. By likening individual files to containers, in other words, courts can simultaneously protect individual privacy and "provide clear guidance to law enforcement through categorical rules," rather than relying on law enforcement to balance privacy interests in an "ad hoc, case-by-case fashion."[159] This serves the interest of equilibrium-adjustment[160] and provides an existing set of coherent rules and analogies for courts to apply in adjudicating future challenges.

This Part discusses the specific rules for container searches before *Riley* and explains the advantages of applying existing container rules to digital files. These rules provide an administrable set of existing principles and work well to explain some key investigative techniques in use today. This Part concludes with a brief example of how this Note's proposal would work in practice when applied to a consent search of a suspect's cell phone.

A. Containers that Disclose Their Contents: The Plain View Exception

Even under the protective virtual file approach to digital subcontainers, investigators would still be entitled to rely on the "plain view" exception to admit evidence discovered inadvertently during the course of a legitimate search. The plain view exception to the warrant requirement allows investigators to seize evidence without a warrant if they are in a lawful

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

159. *Id.* at 2491-92 (quoting Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981)).

160. *See* Kerr, *supra* note 138, at 487; *supra* text accompanying note 88.

position to access the evidence and its incriminating character is immediately apparent.[161] In order for the exception to apply, the investigator must be acting within the scope of his authorized search when he comes across the evidence in question in "plain view."[162]

The plain view exception has a special application in the context of containers. Although the exception does not *generally* allow investigators to open containers they would not otherwise be permitted to view, it allows them to do so when the nature of the container clearly reveals its contents.[163] Various federal courts of appeals have applied this exception to digital searches.[164]

There is little Supreme Court guidance as to how the plain view exception applies to digital containers or subcontainers. *Riley* did not deal with the issue, although some of the information discovered in the search of Brima Wurie's phone was concededly in plain view upon opening the device.[165] It is clear that as a matter of practice, investigators cannot invoke the plain view doctrine as an excuse for opening file after file on a computer's hard drive until they find something incriminating.[166] But the plain view exception vitiates a suspect's expectation of privacy in any container whose "contents can be inferred from [its] outward appearance."[167] Thus, "a kit of burglar tools or a gun case . . . by their very nature cannot support any reasonable expectation of privacy."[168]

Some computer folders and files might be said to betray their own contents in various ways and thus would fall within the plain view exception for digital subcontainers. Image files with thumbnail icons revealing child pornography,

161. *See* Horton v. California, 496 U.S. 128, 136-37 (1990) (describing the plain view exception).

162. *See id.* at 135-36.

163. *See, e.g.*, United States v. Dichiarinte, 445 F.2d 126, 130-31 (7th Cir. 1971) (holding that physical papers are not in plain view, and must be excluded, when "their criminal character [is] not apparent on a mere surface inspection" and they have to be opened and read).

164. *See, e.g.*, United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003); *see also* United States v. Highbarger, 380 F. App'x 127, 131 (3d Cir. 2010); United States v. Miranda, 325 F. App'x 858, 860 (11th Cir. 2009); *cf.* United States v. Galpin, 720 F.3d 436, 451 (2d Cir. 2013) (remanding for the district court to determine whether computer files would have been in plain view during the original search).

165. *See supra* text accompanying notes 84-86.

166. *See* Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971) ("[T]he 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."); United States v. Issacs, 708 F.2d 1365, 1369 (9th Cir. 1983) (holding that a search cannot be permitted to exceed the plain view exception and devolve into "exploratory rummaging").

167. Arkansas v. Sanders, 442 U.S. 753, 764 n.13 (1979), *overruled on other grounds by* California v. Acevedo, 500 U.S. 565 (1991).

168. *Id.*

for example, would be searchable under this doctrine.[169] Files with inculpatory names, like "drug photos," might similarly be subject to warrantless searches.[170] Even if they do not rise to the level of clearly revealing a file's contents, many other visual clues in plain view, like the "CK" entries the detective in *Riley* knew commonly meant "Crip Killer"[171] or facially incriminating website names,[172] might provide probable cause to support a search.

A plain view approach to digital subcontainers also provides a useful theoretical framework for discussing one particular digital investigative technique called "hashing." Authorities often review digital files by feeding them through a hashing algorithm that converts each file into a unique string of digits—a "digital fingerprint."[173] The technique has "two important properties": the resulting hash value is uniquely associated with the input file, and the hashing algorithm works in only one direction.[174] That is, "[o]ne can calculate a hash value from input, but cannot derive the input from the hash value."[175] Once investigators run a file through a hashing algorithm, they cannot reverse the process to determine the contents of the original file, but the resulting hash value "can be used to determine to a high degree of certainty that one set of data is identical to or different from another," all without knowing anything about the particular contents of the file.[176] Authorities can compare the hash value for a known piece of child pornography, for example, with hash values for all the files on the defendant's computer; the values will only match if the child pornography file appears, pixel for pixel, on the defendant's drive.[177] Courts and academics hotly contest how hashing fits in

169. *See* United States v. Williams, 592 F.3d 511, 516, 521 (4th Cir. 2010) (determining that the plain view exception justified the seizure of image files where the thumbnails showed them to be child pornography).

170. *See* United States v. Borowy, 577 F. Supp. 2d 1133, 1138 (D. Nev. 2008) (holding that the agent had probable cause to seize files based on file names that suggested child pornography), *aff'd*, 595 F.3d 1045 (9th Cir. 2010); *cf.* United States v. Meada, 408 F.3d 14, 23 (1st Cir. 2005) (holding that a container's "GUN GUARD" label unambiguously disclosed its contents).

171. *See supra* note 77 and accompanying text.

172. *See, e.g.*, United States v. Alexander, 574 F.3d 484, 491 (8th Cir. 2009).

173. United States v. Thomas, 788 F.3d 345, 348 n.5 (2d Cir. 2015); *see also* Marcia Hofmann, *Arguing for Suppression of 'Hash' Evidence*, CHAMPION, May 2009, at 20.

174. Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 39-40 (2006).

175. *Id.* at 40.

176. Hofmann, *supra* note 173, at 20.

177. *See, e.g.*, United States v. Cartier, 543 F.3d 442, 447-48 (8th Cir. 2008) (upholding the validity of a warrant issued based on the determination that the defendant's computer contained files with hash values matching known child pornography images). Many Internet service providers have automated filters in place to compare e-mailed or

footnote continued on next page

with the Fourth Amendment, questioning whether it constitutes a search[178] and whether it resolves[179] or compounds[180] the problems with digital searches.

Treating individual computer files as containers may provide a convenient way to conceptualize hash searches under the Fourth Amendment. After all, hash values are essentially a feature of particular files, and just like the physical qualities of a closed physical container, they may "betray the contents" of a digital container for the purpose of the plain view exception. Imagine a closed box with a highly unusual shape—in this metaphor, a known piece of child pornography that investigators have run through a hashing algorithm. The image itself is cloaked in the distinctive packaging of the hash value. Now imagine the suspect's hard drive as a warehouse full of closed containers. Once investigators are authorized to access the warehouse, they can certainly search for an identical, distinctive package among all those closed containers without opening any of them. If they find a match for their highly distinctive container, then its observable characteristics have betrayed its contents under the plain view exception. If they open it, the investigators know they will discover the expected contraband image.[181] But the suspect retains a legitimate privacy interest in all the other closed containers (or files), no matter what they hold. Their contents, though revealed in some abstract sense by their hash values, are unknown.

The boundaries of the plain view exception in the digital world are ripe for reexamination, but this Note lacks the space to evaluate them. Other articles and notes have begun to propose adapting the plain view exception to

---

downloaded material with known child pornography images. *See* United States v. Ackerman, 831 F.3d 1292, 1294 (10th Cir. 2016) (describing AOL's filter).

178. *Compare* United States v. Crist, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008) (holding that comparing hash values is a search under the Fourth Amendment), *with* Salgado, *supra* note 174, at 39 (arguing that hashing for files containing illegal contraband like child pornography does not constitute a search).

179. *See* United States v. Ganias, 824 F.3d 199, 235 (2d Cir. 2016) (en banc) (Chin, J., dissenting) ("Hashing appears to make it easier for the Government to comply with the Fourth Amendment, not harder.").

180. *See, e.g.*, United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring) (suggesting that hashing "should not be used without specific authorization in [a] warrant, and such permission should only be given if there is probable cause to believe that such files can be found on the electronic medium to be seized").

181. In some respects, contraband images like child pornography are the easiest example because individuals have no reasonable expectation of privacy in forbidden contraband. United States v. Jacobsen, 466 U.S. 109, 123 (1984) (holding that because the possession of cocaine is "illegitimate," "governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest"). The same plain view reasoning, however, could apply to noncontraband files and allow authorities to search for any particular file, arguably without compromising the privacy interest in other files.

computer files, though often in the context of searches conducted under the authority of warrants.[182] What plain view means for warrantless computer searches is undoubtedly a fruitful area for future academic work.

B. Containers that Manifest a Particular Privacy Interest: Passwords and Encryption

The counterpoint to files that betray their contents are files in which the owner has manifested a particular subjective expectation of privacy—most commonly, by password-protecting or encrypting them. When a physical container is found in a common space, existing law holds that anyone with authority over that common area can permit a search of the container unless the owner has manifested some expectation of privacy or intent to exclude others.[183] If an individual wishes to maintain an expectation of privacy in his possessions in common spaces, "he is free to place these items in an area over which others do *not* share access and control, be it a private room or a locked suitcase under a bed."[184]

The same issues arise in the digital realm when investigators are faced with files on shared computers. Indeed, when faced with a password-protected or encrypted file on a shared computer, many courts already analogize individual files and folders to closed containers in finding a heightened expectation of privacy. The Third Circuit noted this analogy in observing that "[c]omputer users can protect their files by using a password, just as one who shares a footlocker can protect his photographs by placing them in a locked container inside the footlocker."[185] Other courts have similarly reasoned that if a computer or digital device is shared and not locked, an authorized co-user can freely allow authorities to search so long as the owner has not placed a password on or encrypted the relevant files.[186] Courts have also concluded

182. *See, e.g.*, Kerr, *supra* note 9, at 582-84 (suggesting abolishing the plain view exception for digital evidence); James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 FORDHAM L. REV. 2809 (2011); James T. Stinsman, Comment, *Computer Seizures and Searches: Rethinking the Applicability of the Plain View Doctrine*, 83 TEMP. L. REV. 1097 (2011).

183. The Court has moved toward limiting this rule by holding that if the owner is physically present and does not consent to the search, a co-occupant cannot authorize search of the owner's property. *See* Georgia v. Randolph, 547 U.S. 103, 106 (2006).

184. *Id.* at 135 (Roberts, C.J., dissenting).

185. United States v. King, 604 F.3d 125, 137 n.6 (3d Cir. 2010).

186. *See* United States v. Tosti, 733 F.3d 816, 824 (9th Cir. 2013) (holding that the defendant's wife could consent to a search of his computer in part because "the computer and electronic media were neither password protected nor encrypted"); United States v. Stabile, 633 F.3d 219, 233 (3d Cir. 2011) ("The failure to use password protection indicates that Stabile relinquished his privacy in the contents of the computer."); *King*, 604 F.3d at 137 (holding that the defendant "assumed the risk" the computer's co-owner

footnote continued on next page

from the presence of a password or encryption that users maintain an expectation of privacy in their files against cohabitants, which courts often analogize to the privacy interest in a locked physical container.[187]

In this case, then, many courts already view individual files as particular containers carrying with them distinct privacy interests. Extending the other rules of the container doctrine to the same files and folders makes sense and allows a uniform approach to individual files going forward.

C. The Rule in Action: A Hypothetical Consent Search

Consider the balance struck by a rule treating individual files as subcontainers with individually protected privacy interests under the Fourth Amendment. This approach is undoubtedly protective as a default rule in warrantless searches, but that was the Court's goal in *Riley*—to establish a strong presumption of privacy against warrantless digital searches, with a "simple" answer: "get a warrant."[188]

To explore this rule in action, I will use the example of a consent search, a common form of warrantless search in which a suspect gives his consent for officers to search his person or property. Consent searches provide a useful illustration here for two reasons. First, for all the attention that search warrants get in judicial opinions and Fourth Amendment scholarship, consent searches are a ubiquitous feature of the law enforcement landscape. Indeed, "there is no disagreement that police prefer consent searches to other types of investigative techniques"[189] or that consent searches are the most common type of warrantless search.[190] Some estimates suggest that a staggering 98% of warrantless searches conducted by law enforcement are consent searches.[191] As

would consent to search when the defendant placed his hard drive in their shared computer "without any password protection").

187. *See, e.g.*, Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (holding that although the defendant's roommate "had authority to consent to a general search of the[ir] [shared] computer, her authority did not extend to [the defendant's] password-protected files" and citing a case in which the court concluded that a mother could consent to a search of her child's room but that "[t]he mother's authority did not extend to a search of a locked footlocker located within the room" (citing United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978))).

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

189. Tracey Maclin, *The Good and Bad News About Consent Searches in the Supreme Court*, 39 MCGEORGE L. REV. 27, 30 (2008).

190. 6 JOEL M. ANDROPHY, WHITE COLLAR CRIME § 54:11 (2d ed. 2011); *see also* 1 JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE § 16.01, at 261 (4th ed. 2006) (calling consent searches "a dominant—perhaps *the* dominant—type of lawful warrantless search").

191. Rebecca Strauss, Note, *We Can Do This the Easy Way or the Hard Way: The Use of Deceit to Induce Consent Searches*, 100 MICH. L. REV. 868, 871 (2002). The lack of routinized reporting procedures makes the exact number of consent searches difficult to

footnote continued on next page

recently as 2014, the Supreme Court unequivocally reaffirmed that "'[c]onsent searches are part of the standard investigatory techniques of law enforcement agencies' and are 'a constitutionally permissible and wholly legitimate aspect of effective police activity.'"[192] Since it is unlikely, to say the least, that consent searches will lose their luster in the years to come, it is important to determine how this widely applied investigative strategy functions in an era of digital evidence.[193]

Second, consent searches pose particular problems when the scope is extended within digital devices because these searches are particularly reliant on the physical nature of containers. In conventional, physical consent searches, the scope of the search—delimited by what the officer reasonably understands the suspect to be authorizing him to search—necessarily depends on the physical size of the container in question.[194] With digital subcontainers, as already discussed, the physical search metaphor breaks down.[195] When a person consents to a search of a digital device, what is the permissible scope of the search? What is the person's liability if, while conducting a search of that person's computer, government investigators discover unexpected evidence of an unrelated crime? Clear answers to these questions will benefit both individuals subject to digital searches and the investigators tasked with conducting those searches while still respecting the Fourth Amendment.

Now that the Court has determined that cell phones cannot be searched without a warrant or the application of some exception to the warrant requirement,[196] it is reasonable to expect an increase in consent searches of those devices. Innocuous questions like "Can I use your phone?" and "Can I look at your phone?" will now unlock for authorities what the search-incident-to-arrest doctrine cannot.[197] And the recent spate of cyberattacks against

---

determine. Janice Nadler describes the increase in consent searches during motor vehicle stops, and it is clear from her statistics alone that the number of consent searches that take place annually is substantial. Janice Nadler, *No Need to Shout: Bus Sweeps and the Psychology of Coercion*, 2002 SUP. CT. REV. 153, 208-10.

192. Fernandez v. California, 134 S. Ct. 1126, 1132 (2014) (quoting Schneckloth v. Bustamonte, 412 U.S. 218, 228, 231-32 (1973)).

193. Indeed, the Court in *Riley* noted the value of providing law enforcement with "clear guidance" through "categorical rules." 134 S. Ct. at 2491.

194. *See* Florida v. Jimeno, 500 U.S. 248, 251 (1991).

195. *See supra* Part II.A.

196. *See Riley*, 134 S. Ct. at 2494 (noting that other exceptions to the warrant requirement may apply).

197. Compare these requests with the exchange in *United States v. Drayton*, 536 U.S. 194 (2002), where a police officer asked a suspect, "Do you mind if I check your person?" and, when the suspect agreed to be searched, the officer discovered cocaine taped to the suspect's thighs. *Id.* at 199. The Court upheld the search under the consent search exception. *Id.* at 206.

American businesses provides a compelling reason for corporations to consent to searches of their computer systems in order to cooperate with investigative authorities.[198]

Imagine the virtual file approach in action in a consent search. A traffic officer pulls over a driver, believing the driver was texting while driving in violation of local law. The officer asks to examine the driver's phone to determine if the driver had recently sent a text message to anyone. If the driver consents to a search for that purpose, the officer has *limited* authority to open the driver's recent text message conversations and check the timestamps to determine whether any were recently sent or received. That is the extent of the permissible scope.

Because the virtual file approach protects the driver's privacy interests in the other digital subcontainers on her phone, and her text messages are the only subdivision in which the object of the search is reasonably likely to be found, the officer cannot conduct a general search of her photographs, videos, contacts, or applications. Suppose the officer actually pulled her over because he believed that she was carrying drugs with the intent to sell them;[199] without express consent, he still cannot explore other areas of her phone for evidence of narcotics use or drug trafficking.

The scope of the search under the virtual file approach is necessarily narrow—it is circumscribed on all sides by the continued privacy interests in all the other subcontainers on the device. But that does not leave the police officer helpless. For example, the driver might consent to a very broad search, authorizing the officer to look into more areas of her phone; generally, it is up to the suspect to limit the scope of consent. Alternatively, while searching the text messages, the officer might discover texts giving rise to probable cause to believe that the suspect is in fact selling drugs, such as texts with potential buyers. In that case, that evidence would be admissible under the plain view exception, and he can ask for explicit permission to search more of the phone or detain the suspect until he is able to secure a warrant for a broader search.

Conclusion

This Note has argued that *Riley* is a victory for digital privacy that provides a path forward as courts and law enforcement contend with more

198. President Obama has called for close cooperation between private industry and government investigators in this context. President Barack Obama, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), http://stanford.io/1RNRVGc.

199. *See, e.g.*, United States v. Magallon-Lopez, 817 F.3d 671, 675 (9th Cir. 2016) (explaining that officers need not disclose the real reason for a traffic stop so long as they possess some probable cause).

nuanced questions about the permissible scope of digital searches. As storage devices become larger and cloud computing grows more prevalent, the question of searches *within* digital storage media will become more and more important. If the Fourth Amendment is to provide meaningful protection, some privacy interest must inhere in individual files, not merely in the broad devices in which they are found. To that end, it makes the most sense after *Riley* to treat each individual file or folder as an individual subcontainer—that is, as possessing a particular privacy interest unaffected by a search of the surrounding files.

The foregoing Note discusses limitations on the government's ability to undertake a *warrantless* search. But, of course, the government always has the option of making a showing of probable cause to a magistrate and securing a warrant.[200] So long as officers can make that showing, they are not foreclosed from searching a suspect's electronic devices; the virtual file approach proposed here is simply a way of recognizing that digital files contain important information that may not be lightly examined. The *Riley* Court even observed that requiring a warrant is hardly onerous and that advances in technology have "made the process of obtaining a warrant itself more efficient."[201] The example of digital consent searches shows how recognizing privacy interests in individual files furthers the goals of the Fourth Amendment and comports with history and sound policy. *Riley*'s reasoning has paved the way for digital files to be individually protected under the Fourth Amendment—a result that is sound as a matter of policy and precedent.

200. *See* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . .").

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