FOURTH AMENDMENT SATISFACTION—THE "REASONABLENESS" OF DIGITAL SEARCHES

Thomas K. Clancy[*]

I. INTRODUCTION

"It takes no special insight to observe that digital evidence is everywhere and that law enforcement has learned its value."[1] The Fourth Amendment regulates—at least in part—the search and seizure of such evidence.[2] This Article discusses the Supreme Court of the United States' only major decision in this area, *Riley v. California*, and its impact on the evolution of the judicial treatment of Fourth Amendment satisfaction issues regarding governmental efforts to obtain digital evidence.[3]

[Editor's Note: This Article updates and expands the extensive and thorough Fourth Amendment analysis in Professor Clancy's treatise, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION (2d ed. 2014). As such, any analysis provided herein originally appearing in the Author's prior work is presented without direct attribution.]

* Research Professor Emeritus, University of Mississippi School of Law.

1. THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION § 1.5, at 22 (2d ed. 2014).

2. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

3. *See generally* Riley v. California, 134 S. Ct. 2473 (2014) (discussing searches and seizures of digital evidence); CLANCY, *supra* note 1, § 1.2, at 3–4 ("In analyzing any case involving a Fourth Amendment claim, three separate questions must be answered. First, is the Amendment applicable? The applicability question, in turn, is a two-sided inquiry: (a) does the governmental activity—which must be either a search or a seizure—invade (b) an individual interest protected by the Amendment? If the Amendment does not apply, that ends the inquiry; it does not matter if the governmental actions are reasonable or not."). "[D]igital evidence permeates modern life. It may be stored on a person's own digital device, in transit, or stored on a third party server in a network. The Fourth Amendment's applicability to those various devices and locations," *id.* § 12.4.8, at 682, has many complications. *See generally id.* § 1.5 (discussing acquiring digital evidence in computer searches). This Article assumes that a person has a protected interest and that the government searches when it examines the digital data. "Second, if the Amendment does apply, is it satisfied?" CLANCY, *supra* note 1, § 1.2, at 4. The language of the Amendment demonstrates that there are two separate satisfaction inquiries: the first clause mandates that all searches and seizures not be unreasonable; the second clause sets forth the requirements for a

Prior to *Riley*, the Supreme Court provided virtually no guidance and there was a fundamental split in the lower courts on how to treat governmental acquisition of digital evidence.[4] Two principal approaches emerged.[5] One view asserts that a computer—or any other digital device—is a form of a container and that the data in electronic storage on that device are mere forms of documents.[6] A second view maintains that searches for data require a "special approach," which supports new Fourth Amendment rules to regulate searches and seizures of digital evidence.[7] Underlying that approach, in large part, is a concern for broad searches akin to general searches and unfettered application of the plain-view doctrine.[8]

In my opinion, the proper view is that data searches are governed by the same Fourth Amendment rules regulating containers and document searches. What the prevalence of the acquisition of digital evidence teaches us, however, is that some of those traditional rules need to be rethought and modified—yet, they still regulate all searches and seizures.[9] This Article uses the Court's decision in *Riley* to illustrate that view within the context of searches incident to arrest.[10]

II. SEARCHES FOR DATA: PRE-*RILEY* LOWER COURT CASES

Two principal approaches to measuring the reasonableness of searches involving electronic data stored on computers developed in the two decades preceding *Riley*.[11] The first view asserts that a computer—or any other digital device—is a form of a container and that the data in electronic storage on that device are mere forms of documents.[12] As with all containers, digital devices can hold physical evidence, including such items as wires, microchips, and

---

warrant to issue. *See* U.S. CONST. amend. IV. Warrant Clause issues have proven problematic in the digital context, with some courts mandating special requirements for a warrant to issue. *See* CLANCY, *supra* note 1, § 12.4.8.2, at 684–85. These requirements have no basis in the text of the Amendment nor in Supreme Court precedent, which I have discussed elsewhere. *See id.* § 12.4.8, at 682–98 (Warrant Clause and digital evidence issues); *id.* § 12.5.6, at 714–18 (execution considerations). This Article focuses primarily on the reasonableness inquiry. "If it is found that the Amendment is applicable but not satisfied, a third question must be answered: what is the remedy, if any, for the violation? That third question is *not* a Fourth Amendment issue, given that the Supreme Court has, since 1974, stated that the exclusionary rule is not constitutionally mandated." *See id.* § 1.2, at 4. That third question has not generated any issues peculiar to digital evidence. *See generally id.* § 13 (detailing the exclusionary rule).

4. CLANCY, *supra* note 1, § 1.5, at 28; *see infra* Part II.

5. *See* CLANCY, *supra* note 1, § 1.5, at 28.

6. *Id.* § 12.4.8.2, at 684.

7. *See id.*; United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999).

8. *E.g.*, United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1170–77 (9th Cir. 2010) (en banc) (per curiam).

9. *See* Riley v. California, 134 S. Ct. 2473, 2484–95 (2014).

10. *See id.*

11. *See* CLANCY, *supra* note 1, § 12.4.8.2, at 684–85.

12. *Id.*

hard drives.[13] Digital devices also contain electronic evidence, a series of digitally stored *zeros* and *ones*, that—when combined with a computer program—yields information that includes images, words, and spreadsheets.[14] Accordingly, the traditional standards of the Fourth Amendment regulate obtaining the evidence in containers that happen to be computers and the documents that happen to be in digital form.[15]

For example, a warrant that authorizes a search for "writings" or "records" permits a search of computer files.[16] This is to say that the government need not know the exact "form that records may take."[17] Indeed, this view asserts that there is "no principled distinction between those records kept electronically and those in paper form"[18] and, hence, there is "no justification for favoring those who are capable of storing their records on computer over those who keep hard copies of their records."[19] In both instances, "innocuous documents may be scanned to ascertain their relevancy" in "recognition of 'the reality that few people keep documents of their criminal transactions in a folder marked "[crime] records."'"[20]

Courts adopting this view often analogize computers to filing cabinets or to containers:

> [The police] may search the location authorized by the warrant, including any containers at that location that are reasonably likely to contain items described in the warrant. This container rationale is equally applicable to

---

13. *Id.*

14. *Id.*

15. *Id.*

16. *See* United States v. Gregoire, 638 F.3d 962, 967–68 (8th Cir. 2011) ("records" includes computer files); United States v. Hunter, 13 F. Supp. 2d 574, 581 (D. Vt. 1998) (discussing that a warrant authorizing a search for "records" permitted a search of "computers, disks, and similar property"); United States v. Musson, 650 F. Supp. 525, 531 (D. Colo. 1986) (detailing a seizure of computer diskettes approved under a warrant authorizing the seizure of "any records or writings of whatsoever nature showing any business or financial transactions"); People v. Gall, 30 P.3d 145, 153–54 (Colo. 2001) (en banc) (stating that when a warrant authorized seizure of "written or printed material" indicating an intent to do physical harm to a person or building pursuant to an investigation of a conspiracy to murder and use explosives against a facility, the seizure of computers was permissible because they "were reasonably likely to serve as 'containers' for writings, or the functional equivalent of 'written or printed material'"); Frasier v. State, 794 N.E.2d 449, 454, 460 (Ind. Ct. App. 2003) (explaining that a warrant that authorized a search of "notes and/or records" of marijuana sales permitted police to examine computer files); People v. Loorie, 630 N.Y.S.2d 483, 485–86 (N. Y. Co. Ct. 1995) (discussing that a warrant authorizing a search for "records" permitted a search of computer files); *cf.* United States v. Harding, 273 F. Supp. 2d 411, 423 (S.D.N.Y. 2003) (explaining that because photographs may be taken by digital or film cameras and scanned if initially captured by film, a warrant authorizing the police to search for "photographs" allowed agents to open and inspect graphical image files on a zip disk).

17. United States v. Gawrysiak, 972 F. Supp. 853, 861 (D.N.J. 1997), *aff'd*, 178 F.3d 1281 (3d Cir. 1999); *accord* United States v. Henson, 848 F.2d 1374, 1383 (6th Cir. 1988).

18. United States v. Lievertz, 247 F. Supp. 2d 1052, 1063 (S.D. Ind. 2002).

19. *Hunter*, 13 F. Supp. 2d at 584.

20. *Id.* at 582, 584 (quoting United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990)); *accord* United States v. Gray, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999); Rosa v. Commonwealth, 628 S.E.2d 92, 95 (Va. Ct. App. 2006).

> nontraditional, technological "containers" that are reasonably likely to hold information in less tangible forms. Similarly a warrant cannot be expected to anticipate every form an item or repository of information may take, and therefore courts have affirmed the seizure of things that are similar to, or the "functional equivalent" of, items enumerated in a warrant, as well as containers in which they are reasonably likely to be found.[21]

Following this view, computers are "reasonably likely to serve as 'containers' for writings, or the functional equivalent of 'written or printed material.'"[22] This is despite the recognition that computer file searches present "a heightened degree" of intermingling of relevant and irrelevant material.[23]

Perhaps the most significant consequence of that view results from the application of the plain-view doctrine: in any legitimate search that permits looking at digital data, potentially all data is examinable to ascertain what it is.[24] Yet, accepting this view does not mean that wholesale searches of data on computers are permissible.[25] Instead, the courts following this view look to traditional means to limit the scope of document searches, such as the nature of the criminal activity alleged,[26]

---

21. *Gall*, 30 P.3d at 153 (citations omitted); *see also* United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002) (a computer is a form of container); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998) (same); People v. Diaz, 244 P.3d 501, 505 (Cal. 2011) (stating that a cell phone is a container for the application of search incident to arrest principles); *Loorie*, 630 N.Y.S.2d at 484–86 (a computer is a form of container).

22. *Gall*, 30 P.3d at 153.

23. *Hunter*, 13 F. Supp. 2d at 583.

24. CLANCY, *supra* note 1, § 1.5, at 28–29.

25. *See* Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 236–44 (2005); *cf.* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 565–66 (2005) (expressing concern that the particularity requirement offers "less protection against invasive computer searches, however, and today's diminished protections are likely to shrink even more as technology advances").

26. *See* Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (explaining that warrants seeking subscriber information in obscenity investigations that required communications and computer records pertaining to the listed offenses were as particular as circumstances permitted); United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) (stating that one way to make a warrant particular is to specify suspected criminal conduct being investigated, but that a warrant is invalid if it authorizes "the seizure of virtually every document and computer file" without indicating how the items relate to suspected crime); United States v. George, 975 F.2d 72, 76 (2d Cir. 1992) ("Mere reference to 'evidence' of a violation of a broad criminal statute or general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize."); *In re* Lafayette Acad., Inc., 610 F.2d 1, 5–6 (1st Cir. 1979) (holding that a warrant that resulted in removal of four or five truckloads of documents and computer-related materials violated the particularity requirement when it did not specify the type of fraud under investigation); United States v. Longo, 70 F. Supp. 2d 225, 251 (W.D.N.Y. 1999) (holding that a warrant that authorized a search of the hard drive and any data disks for "two documents, one a promissory note, entitled TGL-003, contained within the directory labeled MISC. and a purchase agreement entitled 911, contained in the directory entitled IMF," specifically described the area to be searched); *In re* Search Warrant for K-Sports Imps., Inc., 163 F.R.D. 594, 596–98 (C.D. Cal. 1995) (holding that a warrant for "all computer records and data," without limiting to crime under the investigation, violated the particularity requirement); State v. Nuckolls, 617 So. 2d 724, 726, 728 (Fla. Dist. Ct. App. 1993) (discussing a warrant seeking records of a used car business charged with forgery, odometer tampering, and other criminal violations as sufficient when it authorized a seizure of "[d]ata stored on computer, including, but not limited to, magnetic media

the nature of the objects sought,[27] or the actual reasonableness of the manner in which the search was conducted.[28] Nonetheless, a significant consequence of this view is the potential exposure of vast amounts of data, for at least cursory examination, if the object of the search could be in a digital format.[29]

A second perspective rejects the container analogy and views searches for data on a computer much differently than paper document searches.[30] An early leading case, *United States v. Carey*, espoused the view that law enforcement officers must take a special approach to the search of data contained on computers and that the "file cabinet analogy may be

---

or any other electronic form, hard disks, cassettes, diskettes, photo optical devices and file server magnetic backup tapes" because it left nothing to the discretion of the officers executing warrant).

27. *See* United States v. Wong, 334 F.3d 831, 837–38 (9th Cir. 2003) (discussing a warrant authorizing the search of a computer to "obtain data as it relates to this case" as sufficiently particular when combined with a warrant's list of items sought in the house); State *ex rel* Macy v. One (1) Pioneer CD-ROM Changer, 891 P.2d 600, 604–05 (Okla. Ct. App. 1994) (discussing seizure of a computer system as permissible under a warrant authorizing the seizure of "equipment . . . pertaining to the distribution or display of pornographic material in violation of state obscenity laws"); Schalk v. State, 823 S.W.2d 633, 644, app. at 651 (Tex. Crim. App. 1991) (stating that in theft of trade secrets prosecution, "magnetic tapes" that contained or were reasonably believed to contain stolen data, files, or both sufficiently described the items to be seized).

28. *E.g.*, United States v. Schlingloff, 901 F. Supp. 2d 1101, 1106 (C.D. Ill. 2012) (holding that forensic search for child pornography when executing a warrant for passport fraud was an unreasonable search); United States v. Gray, 78 F. Supp. 2d 524, 529 n.8 (E.D. Va. 1999) (finding that police searching computers are not obligated to conduct "the most technically advanced search possible" and that, instead, the proper question is "whether the search, as conducted was reasonable").

29. *E.g.*, United States v. Triplett, 684 F.3d 500, 506–07 (5th Cir. 2012) (recognizing the need for broad examination of data); United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010) ("[T]he sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents."); *Gray*, 78 F. Supp. 2d at 531 n.11 (holding that when an agent is engaged in a "systematic search" of computer files pursuant to a warrant, and as long as he is searching for the items listed in the warrant, any evidence discovered in the course of that search could be seized under the plain-view doctrine); Commonwealth v. Hinds, 768 N.E.2d 1067, 1072–73 (Mass. 2002) (holding that police had a right to open a file that an officer believed contained child pornography based on the file's name during a valid search of the computer for email; accordingly, the child pornography was in plain view); State v. Schroeder, 613 N.W.2d 911, 916 (Wis. Ct. App. 2000) (rejecting limitations on a search based on file names and concluding that, during a systematic search of all user-created files in executing a search warrant for evidence of online harassment and disorderly conduct, opening the file containing child pornography was in plain view).

30. *See* United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2009) (requiring that a warrant explicitly authorize a search of a computer and that a warrant that authorized a search for financial records was insufficient, even though the items sought "were *capable* of being stored in a computer"); State v. Smith, 920 N.E.2d 949, 953–54 (Ohio 2009) (declaring a cell phone is not a container for the purposes of search incident to arrest doctrine); Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 110 (1994) ("An analogy between a computer and a container oversimplifies a complex area of Fourth Amendment doctrine and ignores the realities of massive modern computer storage."); *see also* Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 60–63, 81–82 (2002) (setting forth some of the differences between searches of "paper documents and computer-generated evidence" and maintaining that courts should impose restrictions on computer searches, such as limiting the search by file types, requiring a second warrant for intermingled files, and imposing time frames for conducting the search).

inadequate."[31] The special approach has no foundation in prior Fourth Amendment jurisprudence, even by analogy, given its essential postulate that computer technology is so fundamentally different from anything that has been searched in the past.[32]

---

31. United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999). The Tenth Circuit has significantly limited *Carey* in later cases. *See, e.g.*, United States v. Burgess, 576 F.3d 1078, 1092–95 (10th Cir. 2009).

32. *See* CLANCY, *supra* note 1, at 692. In *United States v. Comprehensive Drug Testing, Inc.*, Circuit Judge Callahan, in a concurring and dissenting opinion, questioned both the wisdom and the authority of lower courts to create special rules for computer searches:

> [T]he proffered "guidelines" [of the concurring opinion] are troubling because they are overbroad, unreasonably restrictive of how law enforcement personnel carry out their work, and unsupported by citations to legal authority. For example, the concurring opinion does not explain why it is now appropriate to grant heightened Fourth Amendment protections in the context of searches of computers based on the nature of the technology involved when we have previously cautioned just the opposite.
>
> The concurring opinion also fails to acknowledge that its proffered guidance conflicts with the amendments to Federal Rule of Criminal Procedure 41(f)(1)(B), effective December 1, 2009. For instance, Rule 41(f)(1)(B) now states that in cases where an officer is seizing or copying electronically stored information, "[t]he officer may retain a copy of the electronically stored information that was seized or copied." This provision directly contradicts the suggestion that "[t]he government should not retain copies of such returned data." Similarly, Rule 41(f)(1)(B) now provides that "[i]n a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied." The concurring opinion, however, suggests that "the government should provide the issuing officer with a return disclosing precisely what it has obtained as a consequence of the search, and what it has returned to the party from whom it was seized." Presumably these suggestions are superseded by the detailed amendments to Rule 41, which provide comprehensive guidance in this area.
>
> In addition, the suggested protocols essentially jettison the plain-view doctrine in digital evidence cases, urging that magistrate judges "insist that the government waive reliance upon the plain-view doctrine in digital evidence cases." This is put forth without explaining why the Supreme Court's case law or our case law dictates or even suggests that the plain-view doctrine should be entirely abandoned in digital evidence cases. Instead of tailoring its analysis of the plain-view doctrine to the facts of this case, the concurring opinion takes the bold, and unnecessary step of casting that doctrine aside. The more prudent course would be to allow the contours of the plain-view doctrine to develop incrementally through the normal course of fact-based case adjudication. A measured approach based on the facts of a particular case is especially warranted in the case of computer-related technology, which is constantly and quickly evolving.
>
> Moreover, the concurring opinion offers no legal authority for its proposal requiring the segregation of computer data by specialized personnel or an independent third party. Also, the proposed *ex ante* restriction on law enforcement investigations raises practical, cost-related concerns. With respect to using an in-house computer specialist to segregate data, the suggestion essentially would require that law enforcement agencies keep a "walled-off," non-investigatory computer specialist on staff for use in searches of digital evidence. To comply, an agency would have to expand its personnel, likely at a significant cost, to include both computer specialists who could segregate data and forensic computer specialists who could assist in the subsequent investigation. The alternative would be to use an independent third party consultant, which no doubt carries its own significant expense. Both of these options would force law enforcement agencies to incur great expense, perhaps a crushing expense for a smaller police department that already faces tremendous budget pressures.

United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1183–84 (9th Cir. 2010) (en banc) (Callahan, J., concurring & dissenting in part) (citations omitted).

The special approach is premised, in part, on the fact that "electronic storage is likely to contain a greater quantity and variety of information than any previous storage method."[33] The following was typical reasoning:

> A computer is fundamentally different from a writing, or a container of writings, because of its capacity to hold a vast array of information in many different forms, to sort, process, and transfer information in a database, to provide a means for communication via e-mail, and to connect any given user to the internet. A computer may be comprised of a wide variety of personal information, including but not limited to word processing documents, financial records, business records, electronic mail, internet access paths, and previously deleted materials. Because of these differences, the seizure of a computer raises many issues beyond those that might pertain to mere writings.[34]
>
> . . . .
>
> . . . A "writing" is simply not particular enough to warrant a reasonable person to conclude that it includes a computer because a writing and a computer are two fundamentally different things, both in degree and in kind. . . . Moreover, Fourth Amendment analysis regarding the search and seizure of computers must be approached cautiously and narrowly because of the important privacy concerns inherent in the nature of computers, and because the technology in this area is rapidly growing and changing.[35]

Under this special approach, courts impose a variety of unique requirements, all designed in one way or another to limit the permitted examination of data.[36] These rules include creating unique procedures and detailed justifications for warrants to issue,[37] new limitations on the permissible scope of intrusions,[38] and new rules for search execution

---

33. Winick, *supra* note 30, at 105; *see also Comprehensive Drug Testing*, 621 F.3d at 1177 (discussing that over-seizure of electronic data is more likely to occur than with paper records); *In re* Search of: 3817 W. West End, 321 F. Supp. 2d 953, 958–59 (N.D. Ill. 2004) (asserting that searches of computers require "careful scrutiny of the particularity requirement" because of the "extraordinary volume of information that may be stored").

34. People v. Gall, 30 P.3d 145, 162 (Colo. 2001) (en banc) (Martinez, J., dissenting).

35. *Id.* at 164–65.

36. CLANCY, *supra* note 1, § 12.4.8.2.2, at 690.

37. *See id.* at 689–92.

38. *E.g.*, *Comprehensive Drug Testing*, 621 F.3d at 1179–80 (Kozinski, C.J., concurring) (asserting that, as a condition for a warrant to issue, the government must comply with a series of special rules, including waiving reliance on the plain-view doctrine); United States v. Carey, 172 F.3d 1268, 1272–75 (10th Cir. 1999) (holding that the opening of files containing child pornography, at least after the first file was opened, during the execution of the search warrant for documentary evidence related to drug dealing could not be justified by the plain-view doctrine because files were closed and unambiguously named); *cf.* United States v. Abbell, 914 F. Supp. 519, 520–21 (S.D. Fla. 1995) (discussing a criminal prosecution in which a large volume of computer generated data was seized from the defendant's law office, and that a special master would determine whether documents and data were responsive to the search warrant or fell within an exception to the search warrant requirement, such as the plain-view doctrine); United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996) (explaining that when an officer used a personal computer

procedures.[39] There are two basic techniques—using technology-based limitations on searches and creating new legal principles to regulate searches.[40] Limitations based on technology were more commonly used in the 1990s and early part of the decade that followed.[41] Examples include requiring police officers to limit the search by "observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory."[42] Moreover, some courts saw any special rules as having a limited shelf life:

> We realize that judicial decisions regarding the application of the Fourth Amendment to computer-related searches may be of limited longevity. Technology is rapidly evolving and the concept of what is reasonable for Fourth Amendment purposes will likewise have to evolve. . . . New technology may become readily accessible, for example, to enable more efficient or pinpointed searches of computer data, or to facilitate onsite searches. If so, we may be called upon to reexamine the technological rationales that underpin our Fourth Amendment jurisprudence in this technology-sensitive area of the law.[43]

Significant reasons exist to question the soundness of technology-based regulations.[44] In some earlier cases, for example, the court asserted that file name labels or suffixes accurately indicated what the file contained.[45]

---

to transport obscenity and child pornography, the plain-view doctrine did not apply to the search of computer files under a screen name not listed in the warrant).

39. *E.g.*, *Comprehensive Drug Testing*, 621 F.3d at 1175–77.

40. *See id.*

41. *See* cases cited *infra* note 42.

42. *Carey*, 172 F.3d at 1276; *see also In re* Search of: 3817 W. West End, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004) ("[C]omputer technology affords a variety of methods by which the government may tailor a search to target on the documents which evidence the alleged criminal activity."); *In re* Grand Jury Subpoena *Duces Tecum* Dated Nov. 15, 1993, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (asserting, based on the Government's concession, that a keyword search of information stored on a computer would reveal information likely to be relevant to a grand jury investigation); People v. Gall, 30 P.3d 145, 166 (Colo. 2001) (en banc) (Martinez, J., dissenting) ("[S]earches may be limited to avoid searching files not included in the warrant by 'observing files types and titles listed in the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory.'" (quoting *Carey*, 172 F.3d at 1276)); People v. Carratu, 755 N.Y.S.2d 800, 807–09 (N.Y. Sup. Ct. 2003) (stating that police did or did not have a right under warrant to open computer file folders based on the name associated with that folder); Winick, *supra* note 30, at 107 ("Once officers seize large quantities of computer memory, they have three methods of distinguishing relevant from irrelevant information. Officers can either read through portions of each file stored in the memory, conduct a key word search of the data stored on the disks, or print out a directory of the title and file type for each file on the disk.").

43. United States v. Hill, 459 F.3d 966, 979 (9th Cir. 2006) (citations omitted).

44. *See, e.g.*, *Carey*, 172 F.3d at 1274–75 (explaining the unreasonableness of defendant's proposed search methodology and the difficulties that would come with such search limitations).

45. *See id.* at 1275 ("This is not a case in which ambiguously labeled files were contained in the hard drive directory. It is not a case in which the officers had to open each file drawer before discovering its contents."); *Carratu*, 755 N.Y.S.2d at 807 ("[A] warrant authorizing a search of the text files of a computer for documentary evidence pertaining to a specific crime will not authorize a search of image files containing evidence of other criminal activity." (citing *Carey*, 172 F.3d at 1272–73)); Winick, *supra* note

Professional investigators, however, recognized long ago that computer users attempt to conceal criminal evidence by storing "it in random order with deceptive file names," thus, requiring a search of all the stored data to determine whether the warrant includes it.[46]

There are a variety of software programs that government investigators routinely employ when searching for electronic evidence.[47] "[A]utomated search techniques have inherent strengths and weaknesses . . . ."[48] The ability to hide evidence in electronic storage constantly evolves and the government must keep pace or catch up.[49] This is particularly evident with mobile devices, with a proliferation of operating systems and other barriers to examination, such as encryption.[50] Now, courts are less likely to utilize technology-based regulations premised on perceived technological capabilities at any given time.[51]

30, at 108–09 (arguing for file format-based limitations on a permissible search); Amy Baron-Evans, *When the Government Seizes and Searches Your Client's Computer*, CHAMPION, June 2003, at 18 ("Fortunately, the technical means exist to search computers for particular information without rummaging through private information not described in a warrant. For example, in a typical white collar case, relevant files can be isolated and irrelevant ones avoided through keyword searches. In a child pornography case, the government can search for picture files without the need to look at any text file."); *cf.* Commonwealth v. Hinds, 768 N.E.2d 1067, 1073 (Mass. 2002) (explaining that suggestive file names can create probable cause to search a computer for child pornography).

46. United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000) (quoting affidavit); *see also* United States v. Maali, 346 F. Supp. 2d 1226, 1265 (M.D. Fla. 2004) (stating that an expert could not rely on file names to determine what was responsive to warrant), *aff'd*, 502 F.3d 1281 (11th Cir. 2007); EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME 229–30, 632–43 (2d ed. 2004) (describing a methodical data-filtering process that includes several different tools, and observing that digital evidence analysis requires examiners to employ filtering procedures to find potentially useful data and that "[l]ess methodical data reduction techniques, such as searching for specific keywords or extracting only certain file types, may not only miss important clues but can still leave the examiners floundering in a sea of superfluous data"); Michael G. Noblett, Mark M. Pollitt & Lawrence A. Presley, FBI, *Recovering and Examining Computer Forensic Evidence*, 2 FORENSIC SCI. COMM., Oct. 2000, www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/index.htm/computer.htm (observing that there is "no such thing as generic computer evidence procedures," and that "evidence is likely to be significantly different every time a submission is received by the laboratory and will likely require an examination plan tailored to that particular evidence").

47. *See, e.g.*, *Why EnCase Products?*, GUIDANCE SOFTWARE, https://www.guidancesoftware.com/products/Pages/overview.aspx?cmpid=nav_ (last visited Oct. 2, 2015) (explaining EnCase, a commonly used tool designed by Guidance Software).

48. Brenner & Frederiksen, *supra* note 30, at 60–62; *see also* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 303 (2005) ("Existing technology simply gives us no way to know ahead of time where inside a computer a particular file or piece of information may be located.").

49. *See, e.g.*, CASEY, *supra* note 46, at 643 (discussing the challenges to investigators of compressed files, encrypted files, e-mails, and email attachments, which "require[] a combination of tools with different features").

50. *E.g.*, SANS DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR), https://digital-forensics.sans.org/media/DFIR-Smartphone-Forensics-Poster.pdf (last visited Oct. 2, 2015) (depicting the complicated nature of advanced smartphone forensics).

51. United States v. Hill, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004), *aff'd*, 459 F.3d 966 (9th Cir. 2006). That court maintained:

> Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not seize a plastic bag containing a powdery white

The second methodology of the special approach is the creation of distinct rules for digital searches and seizures.[52] Those rules regulate the initial decision to intrude and the scope of the permissible intrusion.[53] An example of creating a unique rule to regulate the initial intrusion is *United States v. Payton*.[54] The authorities in *Payton* had a warrant to search for financial records in a drug investigation, but the warrant did not explicitly authorize a search of computers.[55] The court found that the subsequent search of a computer for digital evidence of drug dealing exceeded the authorized search.[56] Yet, the court conceded: "It is true . . . that pay/owe sheets indicating drug sales were physically capable of being kept on Payton's computer."[57] However, in mandating that the warrant specifically authorize a search of a computer for digital data, the court maintained that a contrary "ruling would eliminate any incentive for officers to seek explicit judicial authorization for searches of computers."[58]

There are also special principles to regulate the scope of a search for digital evidence.[59] Such rules include eliminating the plain-view doctrine and creating search execution protocols.[60] For example, the warrant may have to "include measures to direct the subsequent search of a computer."[61]

> substance if it is labeled "flour" or "talcum powder." There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it. The ease with which child pornography images can be disguised—whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated—forecloses defendant's proposed search methodology.

Id.; *accord* United States v. Gray, 78 F. Supp. 2d 524, 529–30 (E.D. Va. 1999); *see also* Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001) (explaining that agents could legitimately check contents of directories to see if the contents corresponded with labels placed on directories; otherwise, suspects would "be able to shield evidence from a search simply by 'misfiling' it in a directory labeled 'e-mail'"); United States v. Abbell, 963 F. Supp. 1178, 1201 (S.D. Fla. 1997) (upholding the seizure of computer disks despite the fact that they did not contain a responsive name because the seizing "agents were not required to accept these labels as indicative of the disks' contents"); State v. Schroeder, 613 N.W.2d 911, 916 (Wis. Ct. App. 2000) (rejecting limitations on a search based on file names and concluding that, during a systematic search of all user-created files in executing the search warrant for evidence of online harassment and disorderly conduct, opening the file containing child pornography was in plain view).

52. *See* Lily R. Robinton, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311, 339–40 (2010).

53. *See id.*

54. United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2009).

55. *Id.* at 862.

56. *Id.* at 864.

57. *Id.* at 863.

58. *Id.* at 864.

59. *See* Paige Bartholomew, Note, *Seize First, Search Later: The Hunt for Digital Evidence*, 30 TOURO L. REV. 1027, 1027–28 (2014).

60. *See* Kate Brueggemann Ward, Comment, *The Plain (or not so Plain) View Doctrine: Applying the Plain View Doctrine to Digital Seizures*, 79 U. CIN. L. REV. 1163, 1178 (2011).

61. People v. Gall, 30 P.3d 145, 164–65 (Colo. 2001) (en banc) (Martinez, J., dissenting); *see also* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1175–77 (9th Cir. 2010) (en banc) (per curiam) (detailing the need for clear rules when searching computers); *In re* Search of: 3817 W. West End, 321 F. Supp. 2d 953, 957 (N.D. Ill. 2004) (maintaining that an issuing magistrate had authority to

Because of the concern that a search of a computer will often expose to view intermingled documents, several creative attempts at establishing criteria to prohibit either the examination or the use of the data have developed.[62] For example, one court has maintained:

---

require the government to follow "search protocol that attempts to ensure that the search will not exceed constitutional bounds"). Numerous courts reject this view. *E.g.*, United States v. Farlow, 681 F.3d 15, 19 (1st Cir. 2012); United States v. Mann, 592 F.3d 779, 785–86 (7th Cir. 2010); United States v. Williams, 592 F.3d 511, 523–24 (4th Cir. 2010); United States v. Burgess, 576 F.3d 1078, 1092–94 (10th Cir. 2009). Thus, in *United States v. Brooks*, the Tenth Circuit observed:

> This court has never required warrants to contain a particularized computer search strategy. We have simply held that officers must describe with particularity the *objects of their search*. . . .
>
> . . . .
>
> The question of whether the nature of computer forensic searches lends itself to predetermined search protocols is a difficult one. Given the numerous ways information is stored on a computer, openly and surreptitiously, a search can be as much an art as a science. . . . [C]ourts will look to (1) the object of the search, (2) the types of files that may reasonably contain those objects, and (3) whether officers actually expand the scope of the search upon locating evidence of a different crime.

United States v. Brooks, 427 F.3d 1246, 1251–52 (10th Cir. 2005) (citations omitted).

62. *See Comprehensive Drug Testing*, 621 F.3d at 1170–78; United States v. Tamura, 694 F.2d 591, 595–97 (9th Cir. 1982). The origin of the intermingled-document doctrine can be traced to a non-computer case, which involved a large volume of material. *See id.* at 594–95. In *Tamura*, the Ninth Circuit established that the government can avoid violating the Fourth Amendment when executing a warrant by sealing documents recovered during the search pending issuance of a second search warrant, which would detail the permissible scope of further search. *Id.* at 595–97. The Ninth Circuit updated *Tamura* for computer searches in *Comprehensive Drug Testing*:

> The point of the *Tamura* procedures is to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases. If the government can't be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file—and we have no cavil with this general proposition—then everything the government chooses to seize will, under this theory, automatically come into plain view. Since the government agents ultimately decide how much to actually take, this will create a powerful incentive for them to seize more rather than less. . . . Let's take everything back to the lab, have a good look around and see what we might stumble upon.
>
> This would make a mockery of *Tamura* . . . .
>
> . . . .
>
> Everyone's interests are best served if there are clear rules to follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment. . . .
>
> We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.

Comprehensive Drug Testing, 621 F.3d at 1170–71, 1177; *cf.* United States v. Stabile, 633 F.3d 219, 234 n.8 (3d Cir. 2011) (questioning the application of *Tamura* to digital evidence searches); United States v. Hill, 459 F.3d 966, 975–77 (9th Cir. 2006) (discussing the applicability of *Tamura* as applicable precedent to a search of computer files and stating that the warrant affidavit must state why all storage media must

> [L]aw enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. The magistrate should then require officers to specify in a warrant which type of files are sought.[63]

Consistent with the broad trends in the lower courts prior to *Riley*, the courts were split on the question regarding the circumstances under which a permissible cell phone search could occur.[64] Some courts simply applied traditional Fourth Amendment principles.[65] Following that view, for a search incident to arrest of a cell phone found on the person of the arrestee, search of the device was permissible as a matter of course incident to arrest.[66] Just as all other objects—from the clothing worn by the suspect to the contents of wallets—are subject to search, so too were digital devices.[67] Courts following the special approach refused to allow searches of digital devices

---

be seized to be valid); United States v. Schesso, 842 F. Supp. 2d 1292, 1295–96 (W.D. Wash. 2011) (following *Comprehensive Drug Testing*), *rev'd*, 730 F.3d 1040 (9th Cir. 2013). *But 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, 858–61 (2005) (arguing the inapplicability of *Tamura* to computer searches). There appears to be no support for this doctrine in Supreme Court case law; indeed, there is broad ability of government investigators to view documents to ascertain their relevancy under a search warrant for documentary evidence. *See* CLANCY, *supra* note 1, § 12.4.7, at 680–82, § 12.5.6, at 714–18.

63. United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (citations omitted); *accord* United States v. Walser, 275 F.3d 981, 986–87 (10th Cir. 2001); United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000); Winick, *supra* note 30, at 105–07.

64. *See* Riley v. California, 134 S. Ct. 2473, 2482–83 (2014).

65. *E.g.*, State v. Carroll, 778 N.W.2d 1, 8 (Wis. 2010) (viewing cell phones as analogous to closed containers).

66. *E.g.*, United States v. Flores-Lopez, 670 F.3d 803, 806 (7th Cir. 2012); United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007); United States v. Wurie, 612 F. Supp. 2d 104, 110 (D. Mass. 2009) (collecting cases), *rev'd*, 728 F.3d 1 (1st Cir. 2013), *aff'd*, *Riley*, 134 S. Ct. 2473 (2014); Hawkins v. State, 723 S.E.2d 924, 925 (Ga. 2012); People v. Diaz, 244 P.3d 501, 511 (Cal. 2011); State v. Glasco, 90 So. 3d 905, 907 (Fla. Dist. Ct. App. 2012), *rev'd*, 137 So. 3d 104 (Fla. 2014).

67. *E.g.*, *Diaz*, 244 P.3d at 508:

> Even "small spatial container[s]" that hold less information than cell phones may contain highly personal, intimate and *private* information, such as photographs, letters, or diaries. If, as the high court held in [*United States v.*] *Ross,* "a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf [has] an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case," then travelers who carry sophisticated cell phones have no greater right to conceal personal information from official inspection than travelers who carry such information in "small spatial container[s]."

Id. (citations omitted) (quoting United States v. Ross, 456 U.S. 798, 822 (1982)).

> Were the rule otherwise, those carrying small spatial containers, which are legally subject to seizure *and search* if found upon the person at the time of arrest, would find little solace in discovering that their intimate secrets would have been protected if only they had used a device that could hold more personal information.

Id. at n.11.

incident to arrest.[68] This was often based on the view that these devices are not within the category of containers.[69] Hence, in *State v. Smith*, in rejecting police authority to search a cell phone incident to arrest and, instead, requiring the police to obtain a warrant, the court removed digital devices from the category of containers:

> Objects falling under the banner of "closed container" have traditionally been physical objects capable of holding other physical objects. Indeed, [in *New York v. Belton*] the United States Supreme Court has stated that in this situation, "container" means "any object capable of holding another object."
>
> We acknowledge that some federal courts have likened electronic devices to closed containers. Each of these cases, however, fails to consider the Supreme Court's definition of "container" in *Belton*, which implies that the container must actually have a physical object within it. Additionally, the pagers and computer memo books of the early and mid 1990s bear little resemblance to the cell phones of today. Even the more basic models of modern cell phones are capable of storing a wealth of digitized information wholly unlike any physical object found within a closed container. We thus hold that a cell phone is not a closed container for purposes of a Fourth Amendment analysis.[70]

III. THE RHETORIC OF *RILEY* AND ITS SPECIAL RULE

The decision in *Riley v. California* is remarkable for both its result and the rhetoric supporting that result.[71] As to the result, the Court asserted: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[72] This is a special rule unique to cell phones.[73] The rhetoric supporting the *Riley* decision is even more surprising.[74] The opinion, written by Chief Justice Roberts, commented extensively on individual interests at stake when the government searches digital devices:

> [M]odern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.[75]
>
> . . . .
>
> Cell phones . . . place vast quantities of personal information literally in the hands of individuals.[76]

---

68. *E.g.*, Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1171 (D. Or. 2012).
69. *E.g.*, *id.* at 1169.
70. State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009) (citations omitted).
71. *See Riley*,134 S. Ct. at 2494–95.
72. *Id.* at 2495.
73. *See id.* at 2494–95.
74. *See infra* notes 75–87 and accompanying text.
75. *Riley*, 134 S. Ct. at 2484.
76. *Id.* at 2485.

> . . . .
>
> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life."[77]
>
> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.[78]
>
> One of the most notable distinguishing features of modern cell phones is their immense storage capacity.[79]
>
> . . . [T]he possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.[80]
>
> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.[81]
>
> . . . [T]here is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone,

77. *Id.* at 2494–95.
78. *Id.* at 2489.
79. *Id.*
80. *Id.* (citations omitted).
81. *Id.*

> with all that it contains, who is the exception. . . . Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.[82]
>
> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.[83]
>
> Mobile application software on a cell phone, or "apps," offer a range of tools for managing detailed information about all aspects of a person's life. 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 tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase "there's an app for that" is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life.[84]
>
> . . . A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[85]

The Chief Justice even found support for the Court's special rule in the general warrant controversy that served as a catalyst for the adoption of the Fourth Amendment, referencing James Otis's famous speech[86] and asserting: "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[87]

As discussed below, my point is that all of the rhetoric and the special rule created in *Riley* for digital evidence was unnecessary and unjustified. Yet, by embracing the rhetoric and methodology of the special approach to digital evidence, the Court took a giant step toward creating a two-track

---

82. *Id.* at 2490.

83. *Id.*

84. *Id.*

85. *Id.* at 2491.

86. *See generally* Thomas K. Clancy, *The Importance of James Otis*, 82 MISS. L.J. 487 (2013) (discussing Otis and his influence); Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment,* 86 IND. L.J. 979 (2011) (same).

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

Fourth Amendment: one track for digital evidence and a traditional one for all other evidence.[88] It took many years for the Court to weigh in on the Fourth Amendment's role in the digital world and it will take many more years before the implications of *Riley* are resolved.[89]

IV. SEARCHES INCIDENT TO ARREST RULES

The application of the "search incident to arrest" principle is one of the main consequences of an arrest. It involves a significant intrusion upon the person of the suspect as well as the suspect's belongings within the area under the suspect's control.[90] The evidentiary results of these searches often significantly influence the course of any subsequent criminal proceedings.[91] Searches incident to arrest are a common form of search, and given the development of modern police forces and the statutory expansion of the number of crimes, these searches now apply to large numbers of criminal suspects.[92] The practice of search incident to arrest is based on a common law rule pre-dating the Constitution.[93] Yet, in Supreme Court jurisprudence, "[n]o Fourth Amendment doctrine has a more interesting, more unpredictable, more pendular history than the search incident to arrest doctrine."[94]

Two justifications always support searches incident to arrest.[95] One aspect, always accepted, is that such searches serve to protect the safety of the officer by allowing the police to search for weapons and other objects that arrestees may use to attack the officer.[96] The cases have also recognized a second purpose for a search incident to arrest: to recover evidence.[97] It is

---

88. *See infra* notes 151–53 and accompanying text.

89. *See supra* note 4 and accompanying text.

90. CLANCY, *supra* note 1, § 8.1, at 415.

91. *Id.*

92. *Id.*; *see, e.g.*, Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 638 (1999); Myron Moskovitz, *A Rule in Search of a Reason: An Empirical Reexamination of* Chimel *and* Belton, 2002 WIS. L. REV. 657, 662 (citing Special Agent Handbook of United States Custom Service).

93. United States v. Robinson, 414 U.S. 218, 233 n.3 (1973); CLANCY, *supra* note 1, § 8.1.1, at 416; *see also* People v. Chiagles, 142 N.E. 583, 583–84 (N.Y. 1923) (tracing the origins of searches incident to arrest).

94. CLANCY, *supra* note 1, § 8.1, at 415; James J. Tomkovicz, *Divining and Designing the Future of the Search Incident to Arrest Doctrine: Avoiding Instability, Irrationality, and Infidelity*, 2007 U. ILL. L. REV. 1417, 1419 (2007).

95. *See* Chimel v. California, 395 U.S. 752, 762–63 (1969).

96. *Id.* Thus, for example, in *Chimel v. California*, the Court observed:

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated.

Id.

97. CLANCY, *supra* note 1, § 8.1.3, at 418; *see* Thornton v. United States, 541 U.S. 615, 620–21 (2004).

here that much conflict, ambiguity, and changes of course permeate the case law.[98] One view is that the permissible search is for evidence of the crime committed.[99] The broader and current view, with the exception of searches of motor vehicles and digital devices, is that the search may be for any evidence of any crime.[100] Depending on which view the courts adopt, the permitted scope of a search incident to arrest will vary.[101]

Many cases prior to *United States v. Robinson* viewed searches incident to arrest in terms of an exception to the warrant requirement, which intimated an exigent circumstances rationale and, perhaps, a need to justify the search in each case.[102] Although not all of the Supreme Court of the United States' cases reflected that view,[103] a dispositive doctrinal shift in the underlying justification for searches incident to arrest occurred in *Robinson*, in which the Court stated:

> 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.[104]

The Court's statement in the second sentence of this quotation deserves underlining: searches incident to arrests were viewed in *Robinson* not only as an exception to the general rule that required warrants but also as a rule unto themselves—their own general rule.[105] This allowed the Court to create a structure for searches incident to arrest without regard to any other Fourth Amendment satisfaction doctrines.[106] Thus, in *Robinson*, which involved the arrest of a person for driving after revocation of his license, the Court adopted a "categorical" search incident to arrest rule: it applied to all arrests,

---

98. CLANCY, *supra* note 1, § 8.1.3, at 418; *see generally Thornton*, 541 U.S. at 625–32 (Scalia, J., concurring) (discussing the rule for searches of automobiles within the immediate control of the occupant).

99. CLANCY, *supra* note 1, § 8.1.3, at 418.

100. *See id.* §§ 8.1.3–8.2, at 418–20.

101. *See supra* notes 99–100 and accompanying text.

102. United States v. Robinson, 414 U.S. 218, 232–33 (1973); *e.g.*, Chimel v. California, 395 U.S. 752, 760–62 (1969); Trupiano v. United States, 334 U.S. 699, 708 (1948), *overruled in part by* United States v. Rabinowitz, 339 U.S. 56 (1950). There was some common law authority that based a search incident to arrest on the circumstances of each case. *See, e.g.*, David E. Aaronson & Rangeley Wallace, *A Reconsideration of the Fourth Amendment's Doctrine of Search Incident to Arrest*, 64 GEO. L.J. 53, 55 (1975).

103. *E.g.*, *Rabinowitz*, 339 U.S. at 64–66.

104. *Robinson*, 414 U.S. at 235.

105. *See id.*

106. *See id.* ("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.").

regardless of the underlying factual circumstances.[107] In so ruling, the Court rejected a case-by-case inquiry and any analogy to a protective frisk for weapons, which must have justification in each case by examining whether there are circumstances giving rise to the reasonable belief that the person accosted is armed and dangerous.[108] The significance of *Robinson* was to distinguish the search incident to arrest principle from other situations in which the Court found an exception to the warrant preference rule.[109] For searches incident to arrest, permissibility is not determined by applying the case-by-case exigency analysis used to justify exceptions to the warrant preference rule.[110] Hence, the *Robinson* Court established bright-line authority to search, with no limitations based on the type of crime or the likelihood of finding additional evidence of that crime during the search.[111] Subject to the two exceptions discussed below, the effect of the Court's view is to afford the police complete discretion regarding the objects sought during the search.[112] The ramifications are dramatic: objects ranging from the clothing worn by the suspect to the contents of wallets are subject to search.[113]

The Court's decision in *Robinson*, and its adoption of a categorical approach to such searches, blunted any case-by-case examination of nuances, with the Court rejecting the view that a search incident to arrest must limit the search to discovering the fruits of the crime for which the arrest was made.[114] Failing to distinguish between the safety purpose and the evidentiary purpose of a search incident to arrest, the *Robinson* Court stated that it was not inclined:

> to qualify the breadth of the general authority to search incident to a lawful custodial arrest on an assumption that persons arrested for the offense of driving while their licenses have been revoked are less likely to possess

---

107. *Id.* ("[W]e 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."); CLANCY, *supra* note 1, § 8.1.2, at 417.

108. *See Robinson*, 414 U.S. at 228 (explaining that there is "no basis to carry over to a probable-cause arrest the limitations this Court placed on a stop-and-frisk search permissible without probable cause," such as a protective search for weapons); CLANCY, *supra* note 1, § 8.1.2, at 417.

109. CLANCY, *supra* note 1, § 8.1.2, at 417.

110. *Id.*

111. *Id.* § 8.2, at 419; *Robinson*, 414 U.S. at 234; *see also* New York v. Belton, 453 U.S. 454, 461 (1981) (observing that containers permissibly searched "will sometimes be such that they could hold neither a weapon nor evidence of the criminal conduct for which the suspect was arrested"), *abrogation recognized by* Davis v. United States, 131 S. Ct. 2419 (2011).

112. *Robinson*, 414 U.S. at 234 (explaining that the need to disarm a suspect or the need to preserve evidence could serve as justification for a search in the course of a lawful arrest); CLANCY, *supra* note 1, § 8.2, at 419.

113. *E.g.*, United States v. Watson, 669 F.2d 1374, 1383–84 (11th Cir. 1982); Powell v. State, 796 So. 2d 404, 425 (Ala. Crim. App. 1999) (upholding a warrantless seizure of suspect's clothing and stating: "A police officer may search for and seize any evidence on the arrestee's person, even if the evidence is unrelated to the crime for which the arrest was made, in order to prevent concealment or destruction of evidence."), *aff'd*, 796 So. 2d 434 (Ala. 2001).

114. CLANCY, *supra* note 1, § 8.1.3, at 418; *see Robinson*, 414 U.S. at 234.

> dangerous weapons than are those arrested for other crimes. It is scarcely open to doubt that the danger to an officer is far greater in the case of the extended exposure which follows the taking of a suspect into custody and transporting him to the police station than in the case of the relatively fleeting contact resulting from the typical *Terry*-type stop. This is an adequate basis for treating all custodial arrests alike for purposes of search justification.[115]

Moreover, the *Robinson* Court emphasized the justification for a bright-line approach:

> We do not think the long line of authorities of this Court dating back to *Weeks* [*v. United States*], or what we can glean from the history of practice in this country and in England, requires such a case-by-case adjudication. A police officer's determination as to how and where to search the person of a suspect whom he has arrested is necessarily a quick *ad hoc* judgment which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search. The authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect.[116]

Robinson's view prevailed in subsequent decades until the recent decision in *Arizona v. Gant*, which changed the rule for searches of vehicles incident to arrest, and *Riley*, which created a third rule for cell phone searches.[117] *Gant*, rhetorically, viewed the category of searches incident to arrest as an exception to the warrant preference rule.[118] Under prior precedent, the police could always search the entire passenger compartment

---

115. *Robinson*, 414 U.S. at 234–35.

116. *Id.* at 235 (citing Weeks v. United States, 232 U.S. 383 (1914)). Lest there be any doubt of the Court's view, in a case decided the same day as *Robinson*, the Court asserted:

> It is sufficient that the officer had probable cause to arrest the petitioner and that he lawfully effectuated the arrest, and placed the petitioner in custody. In addition, as our decision in *Robinson* makes clear, the arguable absence of "evidentiary" purpose for a search incident to a lawful arrest is not controlling.

Gustafson v. Florida, 414 U.S. 260, 265 (1973); *see also* United States v. Chadwick, 433 U.S. 1, 14–15 (1977) ("The potential dangers lurking in all custodial arrests make warrantless searches of items within the 'immediate control' area reasonable without requiring the arresting officer to calculate the probability that weapons or destructible evidence may be involved."), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

117. *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014); Arizona v. Gant, 556 U.S. 332, 351 (2009); *e.g.*, Missouri v. McNeely, 133 S. Ct. 1552, 1558 (2013) (acknowledging a per se rule of searches incident to arrest); Virginia v. Moore, 553 U.S. 164, 176–77 (2008) (discussing a per se rule of *Robinson*); Michigan v. DeFillippo, 443 U.S. 31, 31 (1979) ("The fact of a lawful arrest, standing alone, authorizes a search [of the person arrested]."); *Gustafson*, 414 U.S. at 266 ("Since it is the fact of custodial arrest which gives rise to the authority to search," the lack of a subjective belief by the officer that the person arrested is armed and dangerous is irrelevant.).

118. *Gant*, 556 U.S. at 338.

incident to the arrest of an occupant of the vehicle.[119] The Court in *Gant* rejected that principle and created two new rules for searches incident to arrest of persons in vehicles.[120] The rules are: (1) a search is not permissible incident to a recent occupant's arrest after the arrestee is secured and cannot access the interior of the vehicle; or (2) a search is permissible if the police have reason to believe that evidence of the offense of arrest might be in the vehicle.[121]

The *Gant* majority viewed the primary rationale of the new rules as protecting privacy interests.[122] The majority saw the prior doctrine as creating "a serious and recurring threat to the privacy of countless individuals."[123] The Court also maintained that the prior rule was unnecessary to protect legitimate law enforcement interests.[124]

The *Gant* majority explicitly limited the new rules to motor vehicle searches.[125] As dissenting Justice Alito maintained in *Gant*, however, the new rules have no rational limitation to vehicle searches.[126] He argued, in part: Why does the rule not apply to all arrestees?[127] The majority's opinion failed to adequately answer Justice Alito's question.[128] Instead, *Gant* created the bizarre situation in which an individual has more protection in an

---

119. CLANCY, *supra* note 1, § 8.6, at 436–37; *see* New York v. Belton, 453 U.S. 454, 460 (1981) *abrogation recognized by* Davis v. United States, 131 S. Ct. 2419 (2011).

120. *Gant*, 556 U.S. at 335.

121. *Id.* at 335, 343.

122. *Id.* at 344.

123. *Id.* at 345.

124. *Id.* at 346. Justice Scalia, in a concurring opinion, said that he did not like the majority's new rules but liked the dissent's view even less. *See id.* at 353–54 (Scalia, J., concurring). He did not want to create a 4–1–4 situation and, therefore, joined the majority opinion, although he acknowledged that it was an "artificial narrowing" of prior cases. *Id.* at 354. Scalia stated that the rule he wanted allowed the police to only search a vehicle incident to arrest if the object of the search was evidence of the crime for which the arrest was made. *Id.* at 353; *see also* Thornton v. United States, 541 U.S. 615, 627–28 (2004) (Scalia, J., concurring) (viewing searches incident to arrest as an exception and engaging in fact-sensitive analysis of whether the search incident to arrest is justified in the case).

125. *Gant*, 556 U.S. at 335, 351.

126. *See id.* at 363–64 (Alito, J., dissenting).

127. *Id.* at 364. Several courts rejected broader application of *Gant*. *E.g.*, United States v. Perdoma, 621 F.3d 745, 757 (8th Cir. 2010); State v. Ellis, 355 S.W.3d 522, 525 (Mo. Ct. App. 2011). But other authority extended *Gant* beyond the automobile context. *See* United States v. Shakir, 616 F.3d 315, 321 (3d Cir. 2010) (discussing the search of a gym bag carried by arrestee held permissible under the following rule: "[W]e hold that a search is permissible incident to a suspect's arrest when, under all the circumstances, there remains a reasonable possibility that the arrestee could access a weapon or destructible evidence in the container or area being searched. Although this standard requires something more than the mere theoretical possibility that a suspect might access a weapon or evidence, it remains a lenient standard."); Angad Singh, Comment, *Stepping Out of the Vehicle: The Potential of* Arizona v. Gant *to End Automatic Searches Incident to Arrest Beyond the Vehicular Context*, 59 AM. U. L. REV. 1759, 1786–89 (2010) (seeking to apply *Gant* to searches incident to arrest of persons in their home); Jackie L. Starbuck, Comment, *Redefining Searches Incident to Arrest:* Gant*'s Effect on* Chimel, 116 PENN ST. L. REV. 1253, 1280 (2012) ("The Supreme Court should abolish any distinction between vehicle searches and home searches by making *Gant*'s explication of *Chimel* and the 'area of immediate control' the controlling authority for all searches incident to arrest.").

128. *See Gant*, 556 U.S. at 335–51 (majority opinion).

automobile than when arrested in his own home, which is fundamentally inconsistent with other aspects of Supreme Court doctrine.[129]

The *Robinson* line of authority offered a view of search incident to arrest doctrine that is categorical: such searches are per se reasonable.[130] Taken to its logical conclusion, what should flow from this view is a simple series of rules, permitting detailed searches of persons and the property they possess in all cases as an incident to arrest.[131] Such a bright-line rule avoids (or should avoid) inconsistent decisions based on similar facts and gives the police a workable rule to apply in each case.[132] That view is, however, a very blunt instrument. Frankly, it is an evidence-gathering technique. It has little relationship to the protective justification for searches incident to arrest in the many cases in which there is no factual basis for believing that the suspect could obtain evidence or a weapon.[133] *Gant* is fundamentally inconsistent with *Robinson* based on its view that searches incident to arrest are an exception to the warrant requirement and that it requires justification for searches beyond the fact of an arrest.[134]

Riley, as applied to searches incident to arrest, merely adds another inconsistency, resulting in three different rules.[135] Importantly, the Chief Justice in *Riley* did a factual analysis of why the search incident to arrest in *Robinson* was reasonable.[136] In *Robinson*, the officer made an arrest for a traffic offense and searched Robinson incident to that arrest.[137] He found drugs in a cigarette package that was on Robinson's person.[138] In *Riley*, the Chief Justice asserted:

> Once an officer gained control of the pack, it was unlikely that Robinson could have accessed the pack's contents. But unknown physical objects

---

129. CLANCY, *supra* note 1, § 8.8, at 450.

130. *Id.* § 8.8, at 448; *see* United States v. Robinson, 414 U.S. 218, 235–36 (1973).

131. CLANCY, *supra* note 1, § 8.8, at 448.

132. *Id.*

133. *Id.*; *see* Moskovitz, *supra* note 92 at 660–62.

134. *See* Arizona v. Gant, 556 U.S. 332, 338–39 (2009).

135. *See generally* Riley v. California, 134 S. Ct. 2473 (2014) (applying the search incident to arrest doctrine to digital evidence). Chief Justice Roberts in *Riley* recharacterized prior search incident to arrest doctrine in several ways. *See id.* at 2482, 2484. First, unlike *Robinson* but consistent with *Gant*, he characterized it as "an exception to the warrant requirement." *Id.* at 2482. Second, he maintained that the exception was "limited to 'personal property . . . immediately associated with the person of the arrestee.'" *Id.* at 2482 (quoting United States v. Chadwick, 433 U.S. 1, 15 (1977)). Frankly, that was not what prior precedent established. *See generally* CLANCY, *supra* note 1, § 8.3 (detailing timing and location of searches). Third, he characterized the search incident to arrest addressed in *Robinson* as resting in part on "privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself." *Riley*, 134 S. Ct. at 2485. But *Robinson* has no such analysis. *See generally Robinson*, 414 U.S. 218 (stating that searches incident to arrest are per se unreasonable). Justice Alito, in his concurring opinion in *Riley*, noticed some of this recharacterization but joined the Court's opinion. *Riley*, 134 S. Ct. at 2495, 2497 (Alito, J., concurring).

136. *Riley*, 134 S. Ct. at 2484–85 (majority opinion).

137. *Robinson*, 414 U.S. at 220–23.

138. *Id.* at 223.

> may always pose risks, no matter how slight, during the tense atmosphere of a custodial arrest. The officer in *Robinson* testified that he could not identify the objects in the cigarette pack but knew they were not cigarettes. Given that, a further search was a reasonable protective measure.[139]

Nonetheless, under the principles articulated in *Robinson*, this factual analysis was unnecessary.[140] Similarly, the Chief Justice in *Riley* essentially did a factual analysis of the stakes involved in searches of digital data incident to arrest:

> Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.
>
> . . . As the First Circuit explained, the officers who searched Wurie's cell phone "knew exactly what they would find therein: data. They also knew that the data could not harm them."[141]

Looking broadly at the search incident to arrest doctrine, the Court traditionally rejected two separate analyses that would reflect the application of two independent legal questions: (1) whether an arrest occurred; and (2) whether a search incident to arrest is permissible.[142] Those are two separate intrusions. The first is based on probable cause that the person is involved in criminal activity and is not of concern here.[143] The second intrusion raises the concern of whether to modify the traditional search incident to arrest rule.[144] If the purpose of the Fourth Amendment is to protect the individual, it would seem that the government should have to justify each intrusion separately.[145]

---

139. *Riley*, 134 S. Ct. at 2485 (citations omitted).

140. *See Robinson*, 414 U.S. at 235.

141. *Riley*, 134 S. Ct. at 2485 (quoting United States v. Wurie, 728 F.3d 1, 10 (1st Cir. 2013)). *Wurie* was issued as a joint opinion with *Riley*. *See id.* at 2481.

142. *See, e.g.*, *id.* at 2482–83.

143. *See id.* at 2483–84.

144. *See id.* at 2482–83.

145. *Id.* at 2488–91. The Chief Justice in *Riley* recognized that a cell phone both contains data and can be a portal to access data stored in the cloud. *Id.* at 2491. Other courts have barely noticed this and have generated no holdings. *See, e.g.*, United States v. Flores-Lopez, 670 F.3d 803, 810 (7th Cir. 2012) (ignoring cloud remote server data storage); Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 36 (2008) (noting a lack of authority regarding search and seizure of cloud data). Traditional Fourth Amendment search incident to arrest doctrine has contemporaneous location limitations on the search. *See* CLANCY, *supra* note 1, § 8.7, at 445. If the police, when searching the device, are not merely accessing data stored on the phone but, instead, are using it as a portal, then the location is not at the place of the arrest. *Id.* Therefore, the traditional doctrine would not justify the search. *Id.*

Gant's second rule—requiring that the police have reason to believe that evidence of the offense of arrest might be in the area searched—required a case-by-case factual analysis, with an overriding concern with broad evidentiary searches.[146] Similarly, much of the Chief Justice's analysis in *Riley*—once the rhetoric of the special approach is put to one side—is a concern about evidentiary searches.[147] Consider this quotation from *Riley*:

> In the vehicle context, *Gant* generally protects against searches for evidence of past crimes. In the cell phone context, however, it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurred. Similarly, in the vehicle context *Gant* restricts broad searches resulting from minor crimes such as traffic violations. That would not necessarily be true for cell phones. It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone. Even an individual pulled over for something as basic as speeding might well have locational data dispositive of guilt on his phone. An individual pulled over for reckless driving might have evidence on the phone that shows whether he was texting while driving. The sources of potential pertinent information are virtually unlimited, so applying the *Gant* standard to cell phones would in effect give "police officers unbridled discretion to rummage at will among a person's private effects."[148]

In contrast, for non-digital items or for items not found in a vehicle, the *Riley* Court in effect continued to conclude that the interests of those arrestees in their possessions and their bodies are less worthy of protection.[149] Thus, in *Riley*, the Chief Justice rejected the State of California's analogue test, which would have permitted officers to "search cell phone data if they could have obtained the same information from a pre-digital counterpart."[150] The Chief Justice wrote:

> But the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form. In Riley's case, for example, it is implausible that he would have strolled around with video tapes, photo albums, and an

146. Arizona v. Gant, 556 U.S. 332, 351 (2009).
147. *Riley*, 134 S. Ct. at 2488–91.
148. *Id.* at 2492 (citations omitted) (quoting *Gant*, 556 U.S. at 345).
149. *Id.* at 2492–93.
150. *Id.* at 2493.

> address book all crammed into his pockets. But because each of those items has a pre-digital analogue, police under California's proposal would be able to search a phone for all of those items—a significant diminution of privacy.
>
> In addition, an analogue test would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records. Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip?[151]

According to this reasoning, it is permissible to read letters, to examine paper bank statements, to look at a photograph or two, or to search a wallet for any evidence that may turn up.[152] Why is this so? Why are those items less worthy if not found in a vehicle or not in digital form?[153]

A lesson I draw from *Riley* is that all evidentiary searches incident to arrest should be eliminated and that, consistent with that decision, the police should obtain a warrant to search the items seized beyond any intrusion necessary to ascertain if the item is dangerous. In other words, the sole purpose of a search incident to arrest for all arrests should be to protect the police; hence, the scope of those searches is limited by that purpose.[154] Thus, an officer could physically examine a cell phone or a package of cigarettes to ensure that the item does not contain a dangerous object, such as a razor blade.[155] Once that protective examination is satisfied, the examination must stop.[156]

---

151. *Id.*

152. *See id.*

153. *See id.* at 2497 (Alito, J., concurring). Justice Alito, concurring in *Riley*, noted that "the Court's approach leads to anomalies":

> For example, the Court's broad holding favors information in digital form over information in hard-copy form. Suppose that two suspects are arrested. Suspect number one has in his pocket a monthly bill for his land-line phone, and the bill lists an incriminating call to a long-distance number. He also has in his a wallet a few snapshots, and one of these is incriminating. Suspect number two has in his pocket a cell phone, the call log of which shows a call to the same incriminating number. In addition, a number of photos are stored in the memory of the cell phone, and one of these is incriminating. Under established law, the police may seize and examine the phone bill and the snapshots in the wallet without obtaining a warrant, but under the Court's holding today, the information stored in the cell phone is out.

Id.

154. *See* CLANCY, *supra* note 1, § 8.1.3, at 418–19. I advocated other modifications in Thomas K. Clancy, *The Purpose of the Fourth Amendment and Crafting Rules to Implement That Purpose*, 48 U. RICH. L. REV. 479 (2014).

155. *See Riley*, 134 S. Ct. at 2485 (majority opinion).

156. *See id.* at 2473.

The rise of digital evidence does not call for the creation of special rules for special devices; instead, it should make the Court re-examine rules of general application.[157] *Riley*, at bottom, repeats a previous mistaken path.[158] The Supreme Court at one point attempted to distinguish among types of containers in ranking expectations of privacy.[159] Luggage had high expectations of privacy.[160] But other containers did not "deserve the full protection of the Fourth Amendment."[161] The bankruptcy of an analytical structure based on distinguishing between types of containers soon became evident, at least to a plurality of the Court in *Robbins v. California*: That framework had no basis in the language of the Amendment, which "protects people and their effects . . . whether they are 'personal' or 'impersonal.'"[162] Thus, the plurality maintained, the contents of closed footlockers or suitcases and opaque containers were immune from a warrantless search because the owners "reasonably 'manifested an expectation that the contents would remain free from public examination.'"[163] Moreover, the *Robbins* plurality believed that it would be "impossible to perceive any objective criteria" to distinguish between containers: "What one person may put into a suitcase, another may put into a paper bag."[164] A majority of the Court later adopted

---

157. *See* CLANCY, *supra* note 1, § 12.4.8.2.3, at 697. In *United States v. Flores-Lopez*, the Seventh Circuit reasoned:

> It's not even clear that we need a rule of law specific to cell phones or other computers. If police are entitled to open a pocket diary to copy the owner's address, they should be entitled to turn on a cell phone to learn its number. If allowed to leaf through a pocket address book, as they are, they should be entitled to read the address book in a cell phone. If forbidden to peruse love letters recognized as such found wedged between the pages of the address book, they should be forbidden to read love letters in the files of a cell phone.

United States v. Flores-Lopez, 670 F.3d 803, 807 (7th Cir. 2012) (citations omitted).

158. *See generally Riley*, 134 S. Ct. 2473 (examining searches of digital devices).

159. *See, e.g.*, United States v. Chadwick, 433 U.S. 1, 12–13 (1977) (contrasting the reduced expectation of privacy in an automobile compared to luggage: "Unlike an automobile, whose primary function is transportation, luggage is intended as a repository of personal effects. In sum, a person's expectations of privacy in personal luggage are substantially greater than in an automobile."), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991); *accord* Florida v. Jimeno, 500 U.S. 248, 253–54 (1991); s*ee also* Wyoming v. Houghton, 526 U.S. 295, 303, 308 (1999) (Breyer, J., concurring) (arguing that "[p]urses are special containers"); Donald A. Dripps, *The Fourth Amendment and the Fallacy of Composition: Determinacy Versus Legitimacy in a Regime of Bright-Line Rules*, 74 MISS. L.J. 341, 379–87 (2004) (discussing the Court's inconsistent treatment of containers in vehicles).

160. *See Chadwick*, 433 U.S. at 13.

161. Arkansas v. Sanders, 442 U.S. 753, 764 n.13 (1979), *abrogated by Acevedo*, 500 U.S. 565. Indeed, "some containers (for example a kit of burglar tools or a gun case) by their very nature [could not] support any reasonable expectation of privacy because their contents [could] be inferred from their outward appearance." *Id.*; *accord* Walter v. United States, 447 U.S. 649, 658 n.12 (1980). Those examples were, however, later viewed as just being "little more than . . . variation[s] of the 'plain view'" doctrine, given that "the distinctive configuration of a container proclaims its contents." Robbins v. California, 453 U.S. 420, 427 (1981) (plurality opinion), *overruled on other grounds by* United States v. Ross, 456 U.S. 798 (1982).

162. *Robbins*, 453 U.S. at 426.

163. *Id.* (quoting *Chadwick*, 433 U.S. at 11).

164. *Id.*

the view that there was no distinction between "worthy" and "unworthy" containers:

> [T]he central purpose of the Fourth Amendment forecloses such a distinction. For just as the most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion, so also may a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf claim an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case.[165]

The same is true of digital and non-digital evidence: just as one person may keep items in a paper bag and another in a locked brief case, others may keep a written diary, and still others a digital record of their thoughts.[166] There is no viable distinction among those situations.[167]

V. CONCLUDING THOUGHTS: THE FUTURE OF DIGITAL EVIDENCE SEARCHES

Riley's rule is a good one: Get a warrant for evidentiary searches.[168] The warrant application and review framework may be a major avenue to regulate digital evidence searches in the future.[169] But there will always be significant exceptions.[170] Consent

---

165. *Ross*, 456 U.S. at 822; *accord* Florida v. Jimeno, 500 U.S. 248, 253–54 (1991); Colorado v. Bertine, 479 U.S. 367, 374–75 (1987); *see also* O'Connor v. Ortega, 480 U.S. 709, 716 (1987) (plurality opinion) ("While whatever expectation of privacy the employee has in the existence and the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the *contents* of the luggage is not affected in the same way."); California v. Carney, 471 U.S. 386, 394 (1985) (rejecting a distinction between worthy and unworthy motor vehicles); New Jersey v. T.L.O., 469 U.S. 325, 337–39 (1985) (explaining that a student has a protected privacy interest in her purse at school). *But cf.* California v. Greenwood, 486 U.S. 35, 40–41 (1988) (discussing that a person leaving plastic trash bags for collection has no reasonable expectation of privacy in the contents of the bags).

166. *See* United States v. Flores-Lopez, 670 F.3d 803, 807 (7th Cir. 2012) (discussing the analogy between keeping addresses in a pocket book and keeping addresses in a cell phone).

167. *See id.*

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

169. *See supra* notes 36–39 and accompanying text.

170. *See* Katz v. United States, 389 U.S. 347, 357–58 (1967). For cases discussing other rationales to search cell phones without a warrant, see *Flores-Lopez*, 670 F.3d at 807–10 (discussing the dangers of remote wiping of a cell phone); United States v. Ortiz, 84 F.3d 977, 982–84 (7th Cir. 1996) (stating that the officers seized an electronic pager incident to Ortiz's arrest for the distribution of heroin and pushed a button on the pager, revealing numeric codes that the pager had previously received; and holding that the officers' actions were justified under the exigent circumstances analysis); United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *3–4 (S.D. Fla. 2008) (rejecting the application of exigent circumstances to justify a warrantless search of a cell phone); United States v. Fierros-Alavarez, 547 F. Supp. 2d 1206, 1212 (D. Kan. 2008) (discussing a cell phone as a container in a vehicle based on probable cause to believe the vehicle had evidence of drug activity); United States v. De La Paz, 43 F. Supp. 2d 370, 375–76 (S.D.N.Y. 1999) (concluding that when a government agent lawfully possessed the phone and there was probable cause to believe it was used in illegal drug activity, the agent could answer incoming calls if the calls arrive when impracticable to obtain a warrant); State v. Boyd, 992 A.2d 1071,

is one.[171] *Riley* itself explicitly listed another important one—exigency.[172] Many questions remain after *Riley*, including important Fourth Amendment applicability and satisfaction issues.[173] *Riley* itself—while adopting a good rule for searches incident to arrest—is problematic for its treatment of digital evidence as a special category of evidence.[174] In the short run, *Riley* will promote a diversity of views.[175] In the long run, perhaps *Riley* will lead to more use of warrants to search for all evidence.[176] More generally, perhaps the prevalence of digital evidence will prompt the Court to rethink traditional Fourth Amendment principles to more adequately promote the purpose of the Fourth Amendment—to protect the individual from unreasonable governmental intrusions.[177]

1090 (Conn. 2010) (probable cause based vehicle search); State v. Smith, 920 N.E.2d 949, 955–56 (Ohio 2009) (finding that an exigent circumstances claim to justify the search of a cell phone was not proper and reasoning: "[E]ven if one accepts the premise that the call records on Smith's phone were subject to imminent permanent deletion, the state failed to show that it would be unable to obtain call records from the cell phone service provider, which might possibly maintain such records as part of its normal operating procedures."); State v. Carroll, 778 N.W.2d 1, 9, 12 (Wis. 2010) (discussing the plain-view doctrine to view an image displayed on the phone, exigent circumstances to detain and to answer the phone, but rejecting that doctrine to view images in memory). Most courts reject an inventory rationale to justify access to data on a cell phone. *E.g.*, *Wall*, 2008 WL 5381412, at *4; United States v. Flores, 122 F. Supp. 2d 491, 495 (S.D.N.Y. 2000); People v. Nottoli, 130 Cal. Rptr. 3d 884, 896–97 (Cal. Ct. App. 2011). A contrary decision, *United States v. Ochoa,* failed to acknowledge that there is no inventory-related reason for the police to turn on a cell phone. United States v. Ochoa*,* 667 F.3d 643, 650 (5th Cir. 2012).

171. *E.g.*, CLANCY, *supra* note 1, § 10.4.4.2.2, at 529 (collecting consent cases regarding digital evidence).

172. *Riley*, 134 S. Ct. at 2494. Exigent circumstances, according to *Riley*, would include concerns about remote-wiping attempts and other case-by-case concerns with "imminent destruction of evidence." *Id.* Exigent circumstances is one of the few Fourth Amendment principles that has experienced doctrinal development by the Roberts Court. *See* CLANCY, *supra* note 1, § 10.6, at 540 (discussing the Court's treatment of exigent circumstances). What is notable about the Roberts Court treatment of the doctrine is that it muddies the standard by which to measure exigency. *E.g.*, City and Cty. of San Francisco v. Sheehan, 135 S. Ct. 1765, 1775 (2015) (stating that the Fourth Amendment standard is "reasonableness" to measure exigency); Brigham City v. Stuart, 547 U.S. 398, 406 (2006) (reasonable belief supports the intervention); Georgia v. Randolph, 547 U.S. 103, 118 (2006) ("good reason" to believe intervention was needed). The majority in *Kentucky v. King* indicated that the warrant preference rule was subject to "reasonable exceptions" and that exigent circumstances was one of those exceptions justified by "compelling" law enforcement needs. Kentucky v. King, 131. S. Ct. 1849, 1856 (2011). Justice Ginsburg in dissent viewed the result reached by the majority in *King* as inconsistent with the "once-guarded exception for emergencies" and that the doctrine needed to be "appropriately reined-in." *Id.* at 1865 (Ginsburg, J., dissenting); *see also* People v. Troyer, 246 P.3d 901, 907 (Cal. 2011) (collecting cases, declining to engage in a "debate over semantics," and concluding that the court's "task [was] to determine whether there was an objectively reasonable basis" for the warrantless entry). By failing to give some objective measure, the Court opens a path for broad application of the doctrine when applied to digital evidence.

173. *See generally* CLANCY, *supra* note 1, § 12.4.8 (analyzing the Fourth Amendment in regards to digital evidence).

174. *See supra* Part III.

175. *See supra* note 135 and accompanying text.

176. *See supra* Parts III–IV.

177. *See supra* notes 1–3 and accompanying text.