The New World of Mobile Communication: Redefining the Scope of Warrantless Cell Phone Searches Incident to Arrest

ABSTRACT

In many jurisdictions, law enforcement officials may conduct a warrantless search of the contents of an arrestee's cell phone incident to an arrest. The judicial precedent for this policy dates back to the early 1990s when courts equated early mobile technology, such as pagers and first generation cell phones, to physical containers capable of storing a limited number of calls or messages. Supreme Court precedent had long permitted the warrantless search of such containers incident to arrest. However, due to advancements in technology, mobile devices, such as smart phones, now have the capacity to hold a larger amount of personal information, including text messages, diaries, pictures, videos, financial information, and medical records. Because this information may increase an arrestee's expectation of privacy in the contents of a cell phone, an analogy to a finite physical container may no longer be appropriate. In recognition of this change, two courts now require law enforcement officials to have a warrant to search the contents of an arrestee's cell phone incident to arrest.

This Note surveys how courts have dealt with changing mobile technology in the context of a search incident to arrest and analyzes the jurisdictional split. It also addresses the expectations of privacy in today's mobile technology and suggests that courts use a function-based approach when determining what information stored in a mobile device may be viewed without a warrant and what information necessarily requires a warrant.

TABLE OF CONTENTS

Three hundred and twenty-two million: the number of wireless phone subscriptions in the United States—more than one per person.[1] One hundred and eighty-seven billion: the number of minutes each month that people in the United States spend talking on their wireless phones.[2] One hundred and ninety-six billion: the average number of text messages those individuals send every month,[3] equating to a monthly total of over 638 text messages per person.

As these statistics indicate, a mobile revolution is well underway in the United States. As our habits of communication evolve, so must the legal system adapt to account for these changes. With more than thirteen-and-a-half million people arrested annually in the United States,[4] it is more likely than ever that these individuals have a cell phone on their person or in their immediate area at the time of arrest. Currently, in all but a few jurisdictions, the arresting officer can search the entire contents of the arrestee's phone without a warrant.[5] This search could include photos, videos, Internet history, medical records, financial information, emails, mobile software applications (apps), and any other content stored on the phone.

Under the "search incident to arrest doctrine"—one of the US Supreme Court's exceptions to the Fourth Amendment's warrant requirement—an arresting officer has the right to search the arrestee

1. *See U.S. Wireless Quick Facts*, CTIA, http://www.ctia.org/advocacy/research/index.cfm/aid/10323 (last visited Oct. 9, 2012).

2. *Id.*

3. *Id.*

4. *Table 29: Estimated Number of Arrests*, FBI, http://www2.fbi.gov/ucr/cius2009/data/table_29.html (last visited Sept. 30, 2012) (displaying arrest statistics for the United States in 2009).

5. *See, e.g.*, United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007) (finding a search of a cell phone's contents permissible because the search was incident to a lawful arrest).

and his immediate area without probable cause or a warrant, so long as the search is contemporaneous with the arrest.[6] The "container doctrine" limits the scope of this search to any container on the arrestee and the contents therein.[7]

Lower courts dispute whether to apply the container doctrine to cell phones seized from an arrestee. Courts categorized early cell phones as containers, finding that law enforcement officials could search information stored therein without limitations. But sophisticated "smart phones" can store massive amounts of data, function like computers, and interact seamlessly with remote data servers.[8] The result of this technology is that individuals are capable of carrying vastly greater quantities of personal information on their person than ever before. As the quantity of personal information at our fingertips increases, an individual's expectation of privacy in that information likewise increases. A warrantless search of a smart phone is therefore much more intrusive than that of an early cell phone.

Only recently have courts begun to consider whether the changes in mobile technology should have an impact on the search-incident-to-arrest doctrine. In most cases, courts have not considered the implications of a warrantless search of a cell phone that has virtually unlimited storage capacity; however, recent opinions indicate an increased concern for individuals' expectations of privacy in their phone's contents.[9] In two significant opinions, *State v. Smith* and *Schlossberg v. Solesbee*, the Ohio Supreme Court and the US District Court for the District of Oregon, respectively, prohibited the search of cell phones incident to arrest.[10] These recent decisions demonstrate a divergence among courts. Many courts, in accordance with the weight of precedent, continue to apply the container doctrine and permit unlimited searches of cell phones incident to arrest. Nevertheless, some courts are beginning to consider the enhanced

---

6. United States v. Robinson, 414 U.S. 218, 236 (1973).

7. *See* Arkansas v. Sanders, 442 U.S. 753, 763-64 (1979); United States v. Chadwick, 433 U.S. 1, 15 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

8. *See* Liane Cassavoy, *What Makes a Smartphone Smart?*, ABOUT.COM, http://cellphones.about.com/od/smartphonebasics/a/what_is_smart.htm (last visited Feb. 26, 2012).

9. *See, e.g.*, United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007) ("[M]odern cellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures.").

10. Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012); State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009).

capacities of mobile phones and thus proscribe such searches to protect individuals' privacy.[11]

This Note addresses the concerns that arise when applying the container doctrine to modern cell phones. Part I of the Note explains the history and rationale of the container doctrine and explores its application to technological devices such as pagers, cell phones, cameras, and computers. Part II analyzes the lower courts' attempts to rationalize the privacy implications of mobile devices with the US Supreme Court's container doctrine and the need to maintain bright-line rules in Fourth Amendment jurisprudence. Finally, Part III discusses solutions proposed by courts and commentators, and suggests a function-based rule for applying the search-incident-to-arrest doctrine to cell phones and other similar wireless devices.

I. ADJUDICATING THE CONTAINER DOCTRINE AND MOBILE TECHNOLOGY

The language of the Fourth Amendment provides the rationale for the search-incident-to-arrest exception.[12] The container doctrine delineates the scope of this exception.[13] However, both the exception and the subsequent refinement were established prior to the advent of mobile technology.[14] This section first explores how courts have traditionally applied the container doctrine. Next, it examines the extent to which courts have adapted the doctrine to account for mobile technology.

A. The Development and Scope of the Container Doctrine

The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[15] A reasonable search generally requires the issuance of a warrant based on probable cause.[16] But

11. *Compare Park*, 2007 WL 1521573, at *8 (finding that a cell phone has heightened privacy concerns that caution against a warrantless search), *with* United States v. Hill, No. CR 10-00261 JSW, 2011 WL 90130, at *7 (N.D. Cal. Jan. 10, 2011) (finding that a cell phone should not be treated differently than any other container).

12. *See* Chimel v. California, 395 U.S. 752, 763 (1969).

13. *See* United States v. Robinson, 414 U.S. 218, 235 (1973).

14. *Robinson* and *Chimel* were decided in 1973 and 1969, respectively. *Id.*; *Chimel*, 395 U.S. 752. Both cases predate the first commercial cell phones by at least eleven years. *See First Cell Phone a True 'Brick'*, MSNBC NEWS (Apr. 11, 2005, 6:55 PM), http://www.msnbc.msn.com/id/7432915/ns/technology_and_science-wireless/t/first-cell-phone-true-brick.

15. U.S. CONST. amend. IV.

16. *See* Katz v. United States, 389 U.S. 347, 356-57 (1967).

courts have determined that some warrantless searches are reasonable in a limited number of circumstances. Among these circumstances are searches and seizures occurring when there are exigent circumstances and during a lawful arrest by a law enforcement official.[17]

The search-incident-to-arrest exception took its modern form in *Chimel v. California*.[18] The US Supreme Court based the doctrine on two rationales—officer safety and evidence preservation.[19] It held that it is reasonable for an officer to search an arrestee for weapons that may be used in resistance or escape and to prevent concealment or destruction of evidence.[20] The scope of the exception is spatially limited to "the area into which an arrestee might reach in order to grab a weapon or evidentiary items."[21] It is also temporally limited, as the officers must conduct the search contemporaneously with the arrest.[22]

The two rationales justify the rule itself, but they are not threshold requirements that law enforcement officers must satisfy before searching an arrestee.[23] In other words, law enforcement officials do not need to prove that there was a threat to officer safety or a need to preserve evidence at the time of the search in order to ensure that the search was lawful. As long as a search takes place contemporaneous to the arrest, it is valid.[24] Likewise, a court need not rely on these rationales to admit evidence obtained in a search incident to arrest. Thus, the rationales do not serve as an evidentiary standard, but rather as "an adequate basis for treating all custodial

17. *See Warrantless Searches and Seizures*, 34 GEO. L.J. ANN. REV. CRIM. PROC. 37, 37 (2005).

18. *See Chimel*, 395 U.S. at 763.

19. *See id.* at 762-63.

20. *See id.* at 763.

21. *See id.* Though the precise boundary of the "area" within which a search incident to arrest is lawful is often litigated, for the purposes of this Note, the analysis proceeds using the assumption that cell phones are on the person or within an area that the courts find permissible, such as in the passenger compartment of an automobile. *See, e.g.*, New York v. Belton, 453 U.S. 454, 460 (1981) (holding that a police officer may lawfully search the passenger compartment of a vehicle contemporaneous with the arrest when the arrestee was an occupant of that vehicle).

22. *See Chimel*, 395 U.S. at 764.

23. *See* United States v. Robinson, 414 U.S. 218, 226 (1973) (explaining that because the rationale of search-incident-to-arrest cases "speak[s] not simply in terms of an exception to the warrant requirement, but in terms of an affirmative authority to search, they clearly imply that such searches also meet the Fourth Amendment's requirement of reasonableness"). The Court also notes the "traditional and unqualified authority of the arresting officer to search the arrestee's person." *Id.* at 229.

24. *See id.* at 235 ("[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.").

arrests alike for purposes of search justification."[25] As such, the search-incident-to-arrest exception exemplifies the Court's preference for bright-line rules in Fourth Amendment jurisprudence.[26]

The container doctrine, enunciated in *United States v. Robinson*, further defines the permissible scope of a search incident to arrest.[27] In addition to the spatial and temporal limitations of *Chimel*, the container doctrine dictates that the lawful scope of a search incident to arrest may include the search of any container, and the contents therein, found on the arrestee or in his immediate area.[28] In *Robinson*, a District of Columbia law enforcement officer stopped and subsequently arrested the defendant on suspicion of driving with a suspended operator's permit.[29] Upon a warrantless search of the defendant, the officer found a crumpled up cigarette pack in the chest pocket of the defendant's shirt that contained fourteen capsules of heroin.[30] The defendant challenged the validity of the search, arguing that, by looking within the closed cigarette pack, the officer violated the defendant's Fourth Amendment rights.[31] The Court disagreed, stating: "Having in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it; and when his inspection revealed the heroin capsules, he was entitled to seize them as 'fruits, instrumentalities, or contraband' probative of criminal conduct."[32] Through *Robinson*, the court crafted the container doctrine by extending the search-incident-to-arrest doctrine to the contents of containers found on the arrestee.[33]

The Court readdressed the container doctrine eight years later in *New York v. Belton*, noting that although the arrestee may have a privacy interest in the container, it is "the lawful custodial arrest [that] justifies the infringement of any privacy interest the arrestee may have."[34] Thus, during an arrest, law enforcement officials can

---

25. *See id.*

26. *See Belton*, 453 U.S. at 458 ("[A] single, familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront." (quoting Dunaway v. New York, 442 U.S. 200, 213-14 (1979))).

27. *See Robinson*, 414 U.S. at 236.

28. *See id.*

29. *Id.* at 220-21.

30. *Id.* at 221-23.

31. The defendant argued that at the time the officer obtained the cigarette pack, there was no danger of the defendant either destroying the evidence or acquiring a weapon from it to resist the arrest; thus, the officer was required under the Fourth Amendment to obtain a search warrant. *Id.* at 219-20. For an analysis supporting defendant's position, see *id.* at 238-59 (Marshall, J., dissenting opinion).

32. *Id.* at 236 (majority opinion).

33. *Id.*

34. New York v. Belton, 453 U.S. 454, 461 (1981).

search the arrestee *and* the contents of any container found on the arrestee's person without probable cause, a warrant, or any additional justification.[35] Examples of lawfully searchable containers include purses,[36] wallets,[37] briefcases,[38] locked bags,[39] and address books.[40]

B. The Container Doctrine Meets Technology: Pagers, Cameras, and Cell Phones

As mobile technology reached consumer markets, courts faced the threshold question of determining whether these new devices were "containers" under the traditional container doctrine. The first of these devices was the pager. Without exception, courts found that the information contained on a pager was within the scope of a search incident to arrest.[41] In most cases, courts analogized the pager and the messages contained therein to a closed container and its contents.[42] In *United States v. Chan*, for example, the US Court of

35. However, the Supreme Court has narrowed this rule for containers found in the arrestee's immediate area, finding that one of the two justifications must be present for the warrantless search incident to arrest of such a container, but there is still no requirement to justify a search of containers found on the arrestee's person. *See* United States v. Chadwick, 433 U.S. 1, 14 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991). Some courts have classified phones as items in the arrestee's immediate area, thereby restricting searchability after the phone is seized and there is no longer a threat of the arrestee destroying it as evidence. *See, e.g.*, United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *4 (S.D. Fla. Dec. 22, 2008).

36. *See, e.g.*, Curd v. City Court of Judsonia, Ark., 141 F.3d 839 (8th Cir. 1998); United States v. Monclavo-Cruz, 662 F.2d 1285 (9th Cir. 1981); United States v. Garcia, 605 F.2d 349 (7th Cir. 1979).

37. *See, e.g.*, United States v. McCroy, 102 F.3d 239 (6th Cir. 1996); United States v. Molinaro, 877 F.2d 1341 (7th Cir. 1989); United States v. Castro, 596 F.2d 674 (5th Cir. 1979); Evans v. Solomon, 681 F. Supp. 2d 233 (E.D.N.Y. 2010).

38. *See, e.g.*, United States v. Ivy, 973 F.2d 1184 (5th Cir. 1992); United States v. Johnson, 846 F.2d 279 (5th Cir. 1988).

39. *See, e.g.*, United States v. Silva, 745 F.2d 840 (4th Cir. 1984).

40. *See, e.g.*, United States v. Rodriguez, 995 F.2d 776 (7th Cir. 1993); United States v. Holzman, 871 F.2d 1496 (9th Cir. 1989).

41. *See, e.g.*, United States v. Charles, 138 F.3d 257 (6th Cir. 1998); United States v. Hunter, No. 96-4259, 1998 WL 887289 (4th Cir. Oct. 29, 1998); United States v. Ortiz, 84 F.3d 977 (7th Cir. 1996); United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996); United States v. Lynch, 908 F. Supp. 284 (D.V.I. 1995); United States v. Galante, No. 94 Cr. 633 (LMM), 1995 WL 507249 (S.D.N.Y. Aug. 25, 1995); United States v. Chan, 830 F. Supp. 531 (N.D. Cal. 1993).

42. *See, e.g.*, *Reyes*, 922 F. Supp. at 833; *Lynch*, 908 F. Supp. at 288 ("Just as police can lawfully search the contents of an arrestee's wallet or address book incident to an arrest, we hold that the agents here could lawfully search the contents of Thomas' pager incident to his arrest."); *Chan*, 830 F. Supp. at 536; *see also, e.g.*, *Ortiz*, 84 F.3d at 977. But some courts justified the search of a pager's contents on exigent circumstances because information could be lost or destroyed if the pager was turned off or if incoming pages filled the memory of the device. *See, e.g.*, *Hunter*, 1998 WL 887289 at *3 ("It is, therefore, imperative that law enforcement officers have the authority to immediately 'search' or retrieve, incident to a valid arrest, information

Appeals for the Sixth Circuit explained that "an electronic repository for personal data is . . . analogous to that in a personal address book or other repository for such information."[43] Accordingly, in a search incident to arrest, a law enforcement officer can search a pager irrespective of any expectations of privacy.[44]

As cell phones replaced pagers on the belt clip, courts largely placed the new technology, like pagers, squarely within the container doctrine.[45] In *United States v. Wurie*, for example, the defendant sought to suppress evidence of his cell phone's call log, which police had obtained during a search of his phone incident to arrest.[46] Surveying the jurisprudential landscape, the court found that decisions "trend heavily in favor" of validating cell phone searches in a search incident to arrest.[47] Noting that courts often analogize cell phones to pagers, the court concluded that there is "no principled basis for distinguishing a warrantless search of a cell phone from a warrantless search of other types of personal containers found on a defendant's person."[48] This court, like many others, thereby applied the traditional rules of the container doctrine to cell phones.[49]

Although initially few courts espoused Fourth Amendment concerns regarding the search of cell phones, recent cases show enhanced caution toward broadening the container doctrine to account for cell phones. Some courts have found that while seizing a cell phone is lawful in a search incident to arrest, searching the phone's memory is a separate question.[50] But these courts ultimately found that searching the phone's memory is lawful under an exigency exception since subsequent incoming calls could result in the deletion of the call logs.[51] Nevertheless, these decisions show that some courts

---

from a pager in order to prevent its destruction as evidence."). See *infra* Part II.C for an extended discussion on exigent circumstances rationale.

43. *Chan*, 830 F. Supp. at 534.

44. *Id.* at 535 (citing New York v. Belton, 453 U.S. 454 (1981)).

45. *See, e.g.*, United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007) (finding that a search incident to arrest of defendant's cell phone call logs and text messages was lawful because the permissible scope of a search incident to a lawful arrest extends to containers found on the arrestee's person) (citation omitted); United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008); United States v. Dennis, No. 07-CR-008-DLB, 2007 WL 3400500, at *7 (E.D. Ky. Nov. 13, 2007); United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1277 (D. Kan. 2007).

46. United States v. Wurie, 612 F. Supp. 2d 104, 105-07 (D. Mass. 2009).

47. *Id.* at 109.

48. *Id.* at 110.

49. *Id.*

50. *See* United States v. Parada, 289 F. Supp. 2d 1291, 1303 (D. Kan. 2003); *see also* United States v. Lottie, No. 3:07cr51RM, 2008 WL 150046, at *3 (N.D. Ind. Jan. 14, 2008).

51. *See Parada*, 289 F. Supp. 2d at 1303-04; *Lottie*, 2008 WL 150046, at *3.

are hesitant to expose the contents of a cell phone's memory in a search incident to arrest.

The judiciary's growing caution to permit the search of a cell phone's contents may be related to the rapid changes in mobile technology. In *United States v. Park*, the US District Court for the Northern District of California addressed the information capacity of modern cell phones (i.e., smart phones) and made clear its reluctance to permit warrantless searches of the content of these phones.[52] In *Park*, police searched the arrestee's cell phone in the police station during the booking process.[53] The court expressed a concern for an arrestee's privacy because "the line between cell phones and personal computers has grown increasingly blurry."[54] The court explained further:

> [T]he information contained in a laptop and in electronic storage devices renders a search of their contents substantially more intrusive than a search of the contents of a lunchbox or other tangible object. . . . People keep all types of personal information on computers, including diaries, personal letters, medical information, photos[,] and financial records.[55]

Despite its concerns, the court did not distinguish cell phones from containers; rather, in suppressing the evidence gathered from the phone, the court ultimately based its decision on the timing of the search.[56] The decision reflects the court's discomfort with a rule that permits an unrestrained search of a modern cell phone incident to arrest.[57]

Drawing on the reasoning from *Park*, two courts have diverged from precedent and prohibited law enforcement officials from searching the contents of cell phones incident to arrest.[58] Both courts held that cell phones are not containers and are therefore outside the scope of *Robinson* and its progeny.[59] In *State v. Smith*, the Ohio Supreme Court observed that cell phones of the modern age bear little

---

52. United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *5-9 (N.D. Cal. May 23, 2007). *But see* United States v. Chan, 830 F. Supp. 531 (N.D. Cal. 1993).

53. *Park*, 2007 WL 1521573, at *3.

54. *Id.* at *8.

55. *Id.* (quoting United States v. Arnold, 454 F. Supp. 2d 999, 1004 (C.D. Cal. 2006)).

56. *See id.* In excluding the evidence, the court found that the search of the cell phone during the booking process was not contemporaneous with the arrest, and therefore did not fall within the temporal scope of the search-incident-to-arrest doctrine. *Id.*

57. *See id.*; Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1168 (D. Or. 2012) ("Although the *Park* court's holding technically turned on the timing of the search . . . the decision makes clear that the court's disagreement with *Finley* was more fundamental.").

58. *Schlossberg*, 844 F. Supp. 2d at 1170-71; State v. Smith, 920 N.E.2d 949, 950 (Ohio 2009).

59. *Schlossberg*, 844 F. Supp. 2d at 1170; *Smith*, 920 N.E.2d at 949.

resemblance to early cell phones and pagers.[60] Modern cell phones "defy easy categorization," for "their ability to store large amounts of private data gives their users a reasonable and justifiable expectation of a higher level of privacy in the information they contain."[61] Although several federal courts previously had characterized cell phones as containers, the court held that modern cell phones are not containers, and officers must therefore obtain a warrant before searching a phone's contents.[62]

Though some courts have shown a reluctance to adopt the *Smith* rationale,[63] one federal district court recently embraced the Ohio Supreme Court's reasoning.[64] In *Schlossberg v. Solesbee*, a case involving the warrantless search of a digital camera,[65] a law enforcement officer seized a camera in a search incident to an arrest for unlawful inception of communication.[66] The officer reviewed the footage immediately thereafter.[67] In suppressing the evidence attained from the camera, the court explained that cases likening electronic devices, such as cell phones and digital cameras, to containers have two primary faults.[68] First, the court suggested that the Ohio Supreme Court defined "container" as a physical object that holds another physical object.[69] As the capacity of an electronic device is in no way relative to its size and as it cannot hold another physical object,[70] the Supreme Court's definition of container excludes personal electronic devices.[71] Second, the court reasoned that prior decisions failed to consider the large amounts of information that modern cell phones and personal electronic devices can hold.[72] To classify them as containers, and hence subject them to warrantless searches, would essentially create the following new rule: "any citizen committing even the most minor arrestable offense is at risk of having his or her most

60. *Smith*, 920 N.E.2d at 954.

61. *Id.* at 955.

62. *Id.* at 953-55.

63. *See, e.g.*, People v. Diaz, 244 P.3d 501, 511 n.17 (Cal. 2011) ("The Ohio court's focus on the extent of the arrestee's expectation of privacy is, as previously explained, inconsistent with the high court's decisions."), *cert. denied*, 132 S. Ct. 94 (2011); *see also* Fawdry v. State, 70 So. 3d 626, 630 (Fla. Dist. Ct. App. 2011) ("We are unpersuaded by *Smith*.").

64. *Schlossberg*, 844 F. Supp. 2d at 1169 (finding *Smith*'s reasoning persuasive and that cell phones are not containers).

65. *Id.* at 1170 ("Having found that personal electronic devices such as cameras and cell phones cannot be considered closed containers, I must consider how they should be classified.").

66. *Id.* at 1166.

67. *Id.*

68. *Id.* at 1169.

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.*

intimate information viewed by an arresting officer."[73] This may violate the public's objective expectation of privacy in the contents of a cell phone, as originally espoused in *Katz v. United States*;[74] thus, the new rule is untenable and contravenes the Fourth Amendment. The Court further found that it is impractical for officers to distinguish between types of personal electronic devices, so the rule must prohibit a search incident to arrest of any of these devices.[75]

Interestingly, as of the writing of this Note, no federal courts and only one state court[76] have addressed whether law enforcement officials can search a personal computer incident to arrest.[77] As Professor Matthew Orso suggested:

> The answer may be that even police do not believe a search of a computer incident to arrest is permissible, seeking instead a warrant for the search of computers. One may look to the plethora of case law discussing the search of computers pursuant to warrants in support of this answer.[78]

Nonetheless, courts have, on occasion, addressed the computer-like features of a cell phone, distinguishing them from the phone's other features. One federal court suggested that when a search was limited to an address book and call log on a cell phone, the search was permissible, "leav[ing] for another day the propriety of a broader search equivalent to the search of a personal computer."[79]

As these cases indicate, courts have traditionally applied the container doctrine to mobile devices.[80] Recently, however, some courts have hesitated to categorize computer-like mobile devices as containers.[81] The result is a divergence among courts regarding the extent to which a law enforcement officer may search an arrestee's mobile device incident to arrest.[82]

---

73. *Id.*

74. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining that a government search requires a warrant under the Fourth Amendment if the individual has an actual expectation of privacy and society is prepared to accept this expectation as reasonable).

75. *Schlossberg*, 844 F. Supp. 2d at 1170.

76. State v. Washington, 110 Wash. App. 1012 (Ct. App. 2002).

77. Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 SANTA CLARA L. REV. 183, 215 (2010).

78. *Id.*

79. United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008).

80. *See, e.g.*, United States v. Wurie, 612 F. Supp. 2d 104, 110 (D. Mass. 2009).

81. *See, e.g.*, Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012).

82. *Compare id.* (finding that mobile electronic devices are not containers and their contents cannot be searched incident to arrest), *with Wurie*, 612 F. Supp. 2d at 110 (finding that cell phones are containers and their contents may be searched in accordance with the container doctrine).

II. ISSUES CONFRONTING COURTS IN WARRANTLESS CELL PHONE SEARCHES

The large number of warrantless cell phone search cases in the past decade[83] reflects both the explosion of mobile usage in the United States[84] and the ambiguity of the warrantless cell phone search standard. A clear rule for the search of a cell phone incident to arrest would not only be valuable guidance for law enforcement officials, but would also serve as a privacy notice for cell phone owners.

The jurisprudence to date highlights four significant issues courts face in analyzing cell phone searches. First, courts must address a possible heightened expectation of privacy for information on cell phones, analyzing both the quantitative and qualitative capacities of modern phones. Second, courts must determine whether a cellular device is a "container" under *Robinson*. The decision is fundamentally about the appropriate scope of the doctrine itself—how, if at all, does the doctrine address virtual and spatial parameters? Third, courts must determine whether exigent circumstances exist to justify the search of a cell phone. Finally, courts must maintain bright-line rules not only to facilitate law enforcement officials in the application of the rules, but also to avoid ambiguity with future technologies of wireless devices.

A. The Expectation of Privacy in Cell Phone Content

Reasonableness under the Fourth Amendment requires balancing the state's need to conduct a search and the individual's right to privacy.[85] But the Supreme Court determined that the rationale for the rule always outweighs potential interests in privacy expectations.[86] The Court held that a search incident to arrest is a "reasonable" search under the Fourth Amendment.[87] Thus, "the lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have."[88]

---

83. *See* Marjorie A. Shields, Annotation, *Validity of Search of Wireless Communication Devices*, 62 A.L.R. 161 (6th ed. 2011) (identifying more than fifty cases involving a search incident to arrest of a wireless communication device).

84. *See U.S. Wireless Quick Facts*, *supra* note 1 (finding that, at 321.7 million wireless subscriber connections, there are more cell phones in the United States than people).

85. *See* Bell v. Wolfish, 441 U.S. 520, 559 (1979) ("In each case it requires a balancing of the need for the particular search against the invasion of personal rights that the search entails.").

86. *See* New York v. Belton, 453 U.S. 454, 461 (1981) (noting that a search incident to arrest is lawful despite an arrestee's privacy interest in the contents of the container).

87. United States v. Robinson, 414 U.S. 218, 235 (1973).

88. *See Belton*, 453 U.S. at 461.

The Court's decision that a warrantless search within the scope of the container doctrine is per se reasonable implies that the need to protect officers and preserve evidence outweighs the arrestee's privacy interest. When officers act beyond the scope of the search-incident-to-arrest exception, the rationales behind the exception are less applicable. As a result, the state's need to conduct a warrantless search is likely less compelling when balanced against the arrestee's expectation of privacy, and a search incident to arrest may be unreasonable.[89] For example, when an individual is arrested in his home, which represents the zenith of privacy expectations, an officer may search a desk drawer immediately in front of the arrestee for a weapon or evidence, but not the other drawers in the room.[90] As the officer distances his search from the "immediate area" of the arrestee, the state's need to locate a weapon or preserve evidence decreases; however, the arrestee's high expectation of privacy in his home remains the same. Similarly, when an officer does not conduct a search contemporaneous with the arrest, the officer acts beyond the temporal scope of the doctrine and the state's need to conduct the search decreases.[91] When the state's need to search decreases and the individual's privacy interest remains high, a court is more likely to find that the search was unreasonable and thus violates the Fourth Amendment.

The converse is true as well: when an individual's expectation of privacy increases, it may outweigh the state's need to conduct the search. When the Supreme Court decided *Robinson* and *Belton*, an arrestee's privacy expectations were limited to the physical objects that he could carry on his person.[92] At that time, no cell phones or other personal electronic devices existed.[93] Thus, the container doctrine, which states that the search of a physical container and its contents incident to arrest is reasonable under the Fourth Amendment, was appropriate because of the physical limitations of information storage. For example, in 1969, a lifetime of financial records would likely be kept in paper form, contained within a large filing cabinet that an individual could not carry. Now, however, those same records can be stored and accessed on a cell phone and carried at all times. If courts believe that a cell phone's capacity to store

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

90. *See id.*

91. *See* United States v. Chadwick, 433 U.S. 1, 15 (1977) (finding that a search of a footlocker incident to arrest is not lawful when the property seized is "not immediately associated with the person" and is searched more than an hour after the arrest), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

92. *See* discussion *supra* Part I.A.

93. *See supra* note 14 and accompanying text.

virtually unlimited information creates a higher expectation of privacy, applying the bright-line rule of *Robinson* to wireless devices may violate the Fourth Amendment.[94]

An individual's privacy interest may depend on what type of information a law enforcement officer accesses on the phone. While "the phone's address book and call history" do not implicate increased privacy concerns, "listen[ing] to voice mails or read[ing] . . . text messages" may implicate those same concerns.[95] This reasoning is indicative of a body of jurisprudence that associates various expectations of privacy with different cell phone features.[96] Generally speaking, call logs have minimal privacy expectations,[97] data storage has significant privacy expectations,[98] and text messages fall somewhere in between.[99]

Under current Fourth Amendment jurisprudence, there is no heightened expectation of privacy in a cell phone's call log.[100] Courts principally rely on the Supreme Court's decision in *Smith v. Maryland*, where the Court found that when a person dials a number from a landline, he knowingly conveys that number to the telephone company; thus, he forfeits any expectation of privacy in that number.[101] That reasoning seamlessly translates to cell phone usage.[102] Customers receive detailed bills about their phone usage and call history, indicating that a third party maintains records of their phone activity.[103] Therefore, courts may reason that the

---

94. *See* State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009).

95. United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008).

96. *See infra* notes 100-117 and accompanying text.

97. *See, e.g.*, Beckwith v. Erie Cnty. Water Auth., 413 F. Supp. 2d 214, 223-24 (W.D.N.Y. 2006) ("[T]here is no reasonable expectation of privacy in the telephone numbers one dials.").

98. *Compare Smith*, 920 N.E.2d at 955 ("[Cell phones] have the ability to transmit large amounts of data in various forms, likening them to laptop computers, which are entitled to a higher expectation of privacy."), *with id.* at 957 (Cupp, J., dissenting) (contesting the application of standards for address books and computers to more complicated cellular phones).

99. *See infra* notes 105-06.

100. *See, e.g.*, *Beckwith*, 413 F. Supp. 2d at 224 ("When Beckwith used his cellular telephone to call the media, he voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business, and therefore lost any reasonable expectation of privacy in the existence and identity of such calls." (citation omitted) (internal quotation marks omitted)).

101. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.").

102. *See, e.g.*, *Beckwith*, 413 F. Supp. 2d at 224.

103. *See Smith*, 442 U.S. at 742 ("All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.").

customer has forfeited his privacy interests in the cell phone call logs.[104]

Courts show more privacy concerns when analyzing text messages, though decisions cut both ways. Some courts do not identify higher expectations of privacy in the content of text messages,[105] even reasoning that courts should afford electronic messages less privacy than call logs.[106] One rationale for this approach is that when a text message is sent, the sender does not know who possesses the phone; thus, the sender can have no expectation of privacy in that message.[107] On the other hand, some courts afford text messages the highest expectation of privacy, likening them to sealed letters.[108] Such items constitute a "class of effects in which the public at large has a legitimate expectation of privacy," rendering a warrantless search presumptively unreasonable.[109]

Courts are likely to find a substantial expectation of privacy in digital information stored on a phone's memory. For example, in *Smith*, the Ohio Supreme Court considered the large amounts of personal data on "standard" cell phones.[110] This functionality "gives . . . users a reasonable and justifiable expectation of a higher level of privacy in the information they contain."[111] Similarly, in *Schlossberg*, the court found modern cell phones are able to hold large amounts of private information, including "phonebook information, appointment calendars, text messages, call logs, photographs, audio and video recordings, web browsing history, electronic documents[,]

---

104. *See, e.g.*, *Beckwith*, 413 F. Supp. 2d at 224.

105. *See, e.g.*, United States v. Young, 278 F. App'x 242, 246 (4th Cir. 2008) (finding that "officers permissibly accessed and copied . . . text messages" in a search incident to arrest); United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007) (holding that officers could search a cell phone's call records and text messages incident to arrest).

106. *See* United States v. Meriwether, 917 F.2d 955, 959 (6th Cir. 1990) (finding no expectation of privacy for electronic pager messages because when one sends an electronic message, there is no way to know who is in possession of the device receiving the message, as opposed to a telephone call where one can hear the recipient's voice prior to transmitting information); *see also* United States v. Whitten, 706 F.2d 1000, 1011 (9th Cir. 1983) (finding no reasonable expectation of privacy in an audible message left on telephone answering machine).

107. *See Meriwether*, 917 F.2d at 959.

108. *See* United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *4 (S.D. Fla. Dec. 22, 2008) (citing United States v. Jacobsen, 466 U.S. 109, 114 (1984)) ("The content of a text message on a cell phone presents no danger of physical harm to the arresting officers or others . . . [and] searching through information stored on a cell phone is analogous to a search of a sealed letter, which requires a warrant.").

109. *Jacobsen*, 466 U.S. at 114.

110. *See* State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009). To be clear, the court analyzed the data capacity of a cell phone that is less sophisticated than a smart phone. *See id.*

111. *See id.*

and user location information."[112] Because of this capacity, the court held that these devices are entitled to "a higher standard of privacy," and therefore the Fourth Amendment protects them from warrantless searches, even incident to a lawful arrest.[113]

It is logical that only a few courts have considered the privacy expectations of information storage on cell phones, as a majority of cases were decided before the advent of smart phones.[114] Even in instances involving more sophisticated cell phone technology, though acknowledging the risks to individual privacy, federal district courts would not turn against the weight of precedent without guidance from higher courts.[115] Other recent holdings involving smart phones are limited to the suppression of call logs or text messages, rather than other types of data storage.[116] Nevertheless, the weight of judicial authority affords a higher degree of privacy to the advanced storage functions of cell phones and personal electronic devices—certainly more so than that traditionally afforded to call logs and, arguably, text messages.[117] Despite judicial recognition of increased privacy rights in certain cell phone functions, only a few courts have held that the expectation of privacy is substantial enough to warrant Fourth Amendment protection from a search incident to arrest.

B. Cell Phones as Traditional Containers under Robinson

An overbroad search, like a heightened expectation of privacy, may render a search unreasonable, as the state's need for the broader search is no longer reasonable relative to the privacy interests of the

112. Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012).

113. *Id.*

114. The first models of the BlackBerry and iPhone, two of the first and most popular multifunctional smart phones, were not even released until 2002 and 2007, respectively. *See* Mathew Honan, *Apple Unveils iPhone*, MACWORLD (Jan. 9, 2007, 12:00 AM), http://www.macworld.com/article/54769/2007/01/iphone.html; David Smith, *The History of the BlackBerry Smartphone*, MOBIMADNESS (Aug. 2, 2009), http://www.mobimadness.com/the-history-of-the-blackberry-smartphone.

115. *See, e.g.*, United States v. Gomez, 807 F. Supp. 2d 1134, 1146 (S.D. Fla. 2011) ("Even though we may disagree with the application of that post-*Chimel* line of cases to the ever-advancing technology of cell phones . . . we are constrained to apply the law as the Supreme Court currently pronounces it."); United States v. Hill, No. CR 10-00261 JSW, 2011 WL 90130, at *7 (N.D. Cal. Jan. 10, 2011) (finding search incident to arrest of a cell phone's pictures lawful, even though they may store "large amounts of personal information" because no guidance otherwise from the Ninth Circuit or Supreme Court existed).

116. *See, e.g.*, Hawkins v. State, 704 S.E.2d 866, 892 (Ga. Ct. App. 2010) (noting that though the case involved suppression of text messages, the phone had greater data storage capabilities, and "[g]iven the volume and diverse nature of data that may be contained in a cell phone or other mobile electronic data storage device," the search of these devices in other instances should be limited).

117. *See supra* notes 100-108 and accompanying text.

arrestee. To determine the reasonable breadth of a search incident to arrest, the Supreme Court refined both the spatial and temporal limitations of the doctrine.[118] The Court also defined the scope of a container as an "object capable of holding another [physical] object,"[119] creating a bright-line rule for reasonable searches incident to arrest. When officers restrict searches to those parameters, the need to conduct a search always outweighs the arrestee's privacy interest. But as Professor Matthew Orso has noted, cell phones and electronic devices bring in an additional dimension—virtual scope.[120] The issue is whether cell phone contents properly fit within the traditional parameters of the container doctrine, or whether the virtual scope of the devices brings them outside the confines of the doctrine.

The container doctrine, as it stands today, is ill suited to address the parameters of virtual scope. The capacities of cell phones and similar electronic storage devices do not fit within the traditional notions of physical scope. Containers, as physical objects, are constrained by their proximity to the arrestee as well as by their dimensions, which determine their ability to hold other physical objects. This reflects the *finite* limitations to the physical scope of the container doctrine; the doctrine implicates clearly demarcated physical boundaries. Wireless and portable data-storage capabilities differ from traditional containers because neither the proximity to an arrestee nor the physical size of the container creates obvious physical search limitations. Rather, modern wireless and data storage devices serve as portals into a nearly *infinite* realm of information, essentially unrestrained by the physical size of the container.

The term "infinite" is not hyperbole. The modern pattern of transitioning data storage to a "cloud computing" model means that unlimited amounts of data may be accessible on any given device, and the storage capacity of the device does not limit its ability to access data.[121] Cloud computing involves centralized servers that maintain enormous quantities of digital space for file and information storage, which are then accessible from any device with Internet access,

---

118. *See* Arizona v. Gant, 556 U.S. 332, 341 (2009) (holding that a constitutionally permissible search incident to arrest must be in the area reachable by arrestee at time of search); United States v. Chadwick, 433 U.S. 1, 2 (1977) (holding that a constitutionally permissible incident to arrest search cannot be remote in time or place from the arrest), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991); Chimel v. California, 395 U.S. 752, 763 (1969) (holding that a constitutionally permissible search incident to arrest must be within the immediate area of arrestee).

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

120. *See* Orso, *supra* note 77, at 206-08.

121. *See* Rivka Tadjer, *What Is Cloud Computing?*, PCMAG.COM (Nov. 18, 2010), http://www.pcmag.com/article2/0,2817,2372163,00.asp.

including cell phones.[122] It is essentially a hub-and-spoke system for data storage, and any cell phone user has access to the hub at all times. As a result, the amount of information and the types of information accessible from a cell phone are immeasurable.

With no guidance from the Supreme Court on the permissible virtual scope of a search incident to arrest, courts have generally taken a binary approach: they either entirely permit[123] or entirely exclude[124] evidence from cell phone data. Those permitting searches of cell phone data analyze cell phones under the container doctrine, analogizing information on the phone to the physical contents of a container.[125] But this is problematic because it does not create any limitations on the virtual scope of a police officer's search.[126] The very purpose of the container doctrine is to create parameters within which a law enforcement officer can conduct a per se reasonable search incident to arrest.[127] By analyzing searches of cell phone contents under a doctrine with only physical and temporal constraints, an infinite search of personal information becomes per se reasonable under the Fourth Amendment.[128]

On the other hand, courts that do not categorize all cell phones as containers may prohibit an officer from conducting a reasonable and lawful search incident to arrest.[129] The public may not have a heightened expectation of privacy in certain types of information on a cell phone, such as call logs, address books, calendars, and, arguably, text messages.[130] Thus, it is perhaps an unnecessary limitation on the search-incident-to-arrest doctrine to find that cell phones *as a class* are outside the scope of the doctrine. The real concern is that *some* of

---

122. *See id.*

123. *See, e.g.*, United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007) (extending the container doctrine to cell phones and the information contained therein).

124. *See, e.g.*, Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012).

125. *See, e.g.*, United States v. Wurie, 612 F. Supp. 2d 104, 110 (D. Mass. 2009) ("There is no principled basis for distinguishing a warrantless search of a cell phone from the search of other types of personal containers found on a defendant's person.").

126. *See Schlossberg*, 844 F. Supp. 2d at 1170 ("It is inexplicable as well as inconsistent with the privacy interest at the core of the Fourth Amendment that many courts now allow officers to conduct warrantless searches of electronic devices capable of holding large volumes of private information which may or may not have any relevance to the arrest offense.").

127. *See* United States v. Chadwick, 433 U.S. 1, 15 (1977), *abrogated by* California v. Acevedo, 500 U.S. 565 (1991).

128. *See* United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007).

129. *See, e.g.*, United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008) (finding "no authority for the proposition that a search incident to arrest must be supported by any level of suspicion that the search will uncover evidence" when police officer did, in fact, find evidence of the crime in arrestee's call log).

130. *See supra* Part II.A.

the information on these devices is unrelated to the arrestee's crime[131] and implicates increased privacy concerns.[132]

The container doctrine in its current form insufficiently protects individual privacy interests because, in some jurisdictions, it fails to provide search limits to the virtual scope of cell phones. At the same time, prohibiting the search of cell phones is an insufficient solution because searches of certain information, such as call logs, should be permissible under the search-incident-to-arrest doctrine. As a solution, one court suggested that the scope of the "search must be limited as much as is reasonably practicable by the object of the search."[133] Officers should first narrow their search to certain "sub-containers" of data.[134] While trying to balance the need for law enforcement agents to access some—but not all—data available on a cell phone, this holding fails to provide any guidance for officers as to precisely which sub-containers they may search.[135] It is nonetheless illustrative of how difficult it is to craft limits on the virtual scope of a search incident to arrest while maintaining a bright-line rule to promote the effective application by law enforcement officials.

C. Exigent Circumstances as Justification for a Warrantless Cell Phone Search

In addition to a search incident to arrest, exigent circumstances is another exception to the Fourth Amendment's warrant requirement.[136] Such circumstances exist when there is an imminent threat of the destruction of evidence.[137] The exception requires the reasonable belief by a law enforcement officer that evidence is in imminent danger of being removed or destroyed.[138] This differs substantially from a search incident to arrest, where the

131. *See, e.g.*, Newhard v. Borders, 649 F. Supp. 2d 440, 444, 449 (W.D. Va. 2009) (dismissing claim under section 1823 for constitutional rights violation because officers viewing sexually compromising pictures of arrestee and girlfriend on arrestee's cell phone in a search incident to arrest for suspicion of DUI was not a violation of Fourth Amendment rights).

132. *See supra* Part II.A.

133. Hawkins v. State, 704 S.E.2d 886, 892 (Ga. Ct. App. 2010).

134. *Id.*

135. *See id.* (holding that a search of photos or audio files when looking for a text message would not be appropriate but not articulating a clear test to determine the scope of an appropriate search).

136. *Warrantless Searches and Seizures*, *supra* note 17, at 68-69.

137. *Id.* Though other exigent circumstances exist—such as "hot pursuit," the risk of a suspect fleeing, or the safety of law enforcement officials—the imminent destruction of evidence is the only exigent circumstance that is pertinent to the warrantless search of cell phones. *See id.*

138. *Id.* at 69.

preservation of evidence serves as a justification for the exception, but not a requirement to search.[139]

Many courts have reasoned that a search of a cell phone or personal electronic device incident to arrest is lawful because it is a situation where an officer needs to preserve evidence from destruction.[140] The search-incident-to-arrest doctrine, however, does not require an actual showing of exigent circumstances—for instance, the imminent destruction of evidence—so long as the search is within the scope of the doctrine.[141] In effect, the fact that some courts have relied on the imminent need to preserve evidence to rationalize a search incident to arrest indicates that cell phones may not fit cleanly within the search-incident-to-arrest doctrine. Rather than justifying a search incident to arrest, situations concerning the imminent destruction of evidence fall more appropriately under the exigent circumstances warrant exception, which several courts have used to permit the warrantless search of a cell phone's contents.[142]

In cell phone searches, exigent circumstances may arise when there is a fear that incoming calls or messages will replace recent calls or messages in a phone's memory,[143] or that an arrestee's accomplice will activate a remote wipe program to erase the phone's memory entirely.[144] Rapid improvements in technology, however, have obviated the former of these two concerns.[145] Modern cell phones no

---

139. *Id.* at 60, 70, 71.

140. *See, e.g.*, United States v. Parada, 289 F. Supp. 2d 1291, 1303-04 (D. Kan. 2003) (upholding the search of a cell phone because incoming calls would delete entries listed in a call log, thereby destroying evidence).

141. *See* United States v. Robinson, 414 U.S. 218, 235 (1973).

142. *See, e.g.*, United States v. Zamora, No. 1:05 CR 250 WSD, 2006 WL 418390, at *4-5 (N.D. Ga. Feb. 21, 2006) (concluding that the "legitimate concerns" of losing the data from the cell phones created "exigent circumstances [that] authorized the seizure of the cell phones and the search of their electronic contents"); *Parada*, 289 F. Supp. 2d at 1303 ("Because a cell phone has a limited memory to store numbers, the agent recorded the numbers in the event that subsequent incoming calls effected the deletion or overwriting of the earlier stored numbers.").

143. *See, e.g.*, United States v. Young, 278 F. App'x 242 (4th Cir. 2008) (finding that officers have no way of knowing if text messages would be deleted, giving rise to a "manifest need . . . to preserve evidence"); United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *3-4 (S.D. Fla. Dec. 22, 2008) (suppressing cell phone evidence in part because the government failed to establish that text messages at issue would have been destroyed absent agent's intervention).

144. *See, e.g.*, United States v. Rodriguez-Gomez, No. 1:10-CR-103-2-CAP, 2010 WL 5524891, at *3 (N.D. Ga. Nov. 15, 2010) (finding officer's testimony to provide sufficient evidence that cell phone's contents could be remotely deleted, "thus implicating the need to preserve evidence").

145. See *United States v. Gomez*, where the court stated:

> We tend to agree with this position and recognize the ever-weakening argument that a modern cell phone, with its continually advancing technology, is at any risk of deleting its call history or text messages folder to make space for incoming calls or

longer store only a handful of recent text messages and phone calls and greatly expanded digital memories eradicate any real risk of automatic deletion.[146] Thus, the exigent circumstance justification predicated on this pager-era rationale of lost data is no longer valid.[147]

Remote wipe programs, on the other hand, pose a real and substantial risk of destroying evidence. Such programs, designed to protect user data on lost cell phones, allow an individual or third party to erase the memory of a cell phone from a remote location.[148] However, for an arrestee to effectively erase evidence requires the presence of a number of factors: (1) a phone must be enabled with remote wipe capabilities, (2) an accomplice must have access to the remote wipe program, and (3) there must exist some way for the arrestee to contemporaneously alert the accomplice of the arrest.[149] Given these coordination difficulties, one court suggested that law enforcement officials need probable cause of a remote wipe threat in order to implicate the exigent circumstances exception.[150]

Irrespective of the possibility of a remote wipe, law enforcement officers have several simple ways to prevent a loss of cell phone data. The officer may disconnect the wireless access of the phone, remove the phone's battery, depower the phone, or place the phone in a container shielded from wireless signals.[151] For example, recent innovations, such as Faraday bags, allow officers to place the

---

> text messages—the memory capacity of a cell phone is far, far greater than that of an analogized two-decade older pager.

807 F. Supp. 2d 1134, 1150 n.17 (S.D. Fla. 2011).

146. *See id.*

147. *See id.* ("Indeed, pagers pre-dated commercial [I]nternet usage; modern cell phones however are fully [I]nternet capable. The weakness of this analogy is glaringly obvious.").

148. *See, e.g.*, Doug Aamoth, *App of the Week: Find My iPhone*, TECHLAND (Nov. 23, 2010), http://techland.time.com/2010/11/23/app-of-the-week-find-my-iphone (noting that iPhone users can see their lost "iPhone on a map and can remotely lock it, delete all the data, or send a message to the screen asking for it to be returned").

149. *See Find My iPhone*, APPLE, http://www.apple.com/iphone/built-in-apps/find-my-iphone.html (last visited Feb. 27, 2012) (noting that a remote wipe of an iPhone requires the use of either iCloud or another Apple product, access to that software, and implementation of a remote wipe sequence).

150. As the district court in *Gomez* stated:

> [T]he agents never proffered evidence to support an objective belief that the cell phone's call log history was ever at risk of being lost or destroyed. In fact, while agents testified to their speculation that a cell phone could theoretically be 'wiped' remotely by an unknown third party, each agent testified that they had no reason to believe that Defendant's specific cell phone was capable of remote deletion.

807 F. Supp. 2d at 1150 n.17. *But see* United States v. Salgado, No. 1:09-CR-454-CAP, 2010 WL 3062440, at *3-4 (N.D. Ga. June 12, 2010) (finding that exigent circumstances exist when there is a possibility that the data can be compromised through a remote wipe).

151. *See* People v. Diaz, 244 P.3d 501, 515 n.24 (Cal. 2011) (noting that officers may prevent the risk of remote wipe by simply taking out the phone's battery or placing it in a shielded container), *cert. denied*, 132 S. Ct. 94 (2011).

phone in a small container to shield wireless communication without eliminating the officer's access to it.[152] Taking any of these simple precautionary steps would prevent an accomplice from remotely accessing a phone.[153] An officer may perform these operations more quickly than conducting a full search of the phone's data, thereby reducing the window of opportunity for a third party to initiate a remote wipe sequence. The result is that preventive measures to thwart a remote wipe may actually be more effective at preserving evidence than an immediate warrantless search.

At best, exigent circumstances are a tenuous justification for the warrantless search of a cell phone's contents. Though a real threat in the past, the potential for evidence destruction as a result of incoming messages or calls is now virtually nonexistent.[154] While remote wipe programs still pose a threat to the destruction of evidence, there is an extremely low probability that an arrestee has both the capability and coordination to effectively erase a phone's data at the time of the arrest.

D. Suggested Solutions from Courts and Commentators

Courts have been reluctant to explore creative solutions to the inherent Fourth Amendment issues in a search of a cell phone's contents incident to arrest, opting instead to either entirely permit or suppress evidence obtained from a phone's memory. Commentators, on the other hand, have offered a number of solutions drawing lines somewhere between the polar judicial approaches.[155]

Professor Adam Gershowitz considers a series of solutions that courts could adopt. First, he offers the bright-line position of prohibiting all searches of cell phone contents incident to arrest.[156] Alternatively, he suggests four options: (1) encourage legislative bodies to adopt a more protective rule,[157] (2) adopt an open-application

152. Mark Sutton, *Faraday Bags Help Secure Seized Mobile Devices*, ITP.NET (Aug. 26, 2011), http://www.itp.net/585942-faraday-bags-help-secure-seized-mobilc-devices.

153. *Diaz*, 244 P.3d at 515 n.24.

154. *See, e.g.*, David Kravets, *Which Telecoms Store Your Data the Longest? Secret Memo Tells All*, WIRED (Sept. 28, 2011, 6:30 AM), http://www.wired.com/threatlevel/2011/09/cellular-customer-data.

155. *See, e.g.*, Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 45-57 (2008).

156. *Id.* at 45-47.

157. *Id.* at 50.

test,[158] (3) adopt a five-steps-of-searches test,[159] or (4) distinguish between data stored on the device and remotely-stored data.[160]

State statutes aimed at reducing the scope of a search incident to arrest with respect to cell phone contents could swiftly and effectively reduce the warrantless search abilities of law enforcement officials. But implementation of such policy faces two fundamental obstacles. First, legislators are generally inclined to favor broader police enforcement powers, and thus they are reluctant to take positions that appear criminal-friendly.[161] Second, as Gershowitz acknowledges, "it is unlikely that a lobby will form to press for a law exempting iPhones from the search-incident-to-arrest doctrine."[162] While circumstances may arise to overcome these obstacles,[163] courts should not wait for legislative action. A search incident to arrest is fundamentally a privacy issue, not a policy issue. Thus, the appropriate forum to address a breach of Fourth Amendment rights is in the courts, not in the legislature. Any limitations on the doctrine from the judiciary would not preclude further policy-based limitations by rule-making bodies.

In an "open-application test," police could search the contents of any application that is open on the phone at the time of the seizure, but could not open any others.[164] Though Gershowitz offers several critiques of this approach,[165] the most compelling critique is absent—the open application could likely be one containing expansive quantities of highly private information. Consider an open email application, which would allow an officer to search the entirety of the arrestee's inbox. Likewise, an application enabling access to a home

158. *Id.* at 53.

159. *Id.* at 54.

160. *Id.* at 56.

161. *See* Jonathan Simon, *Megan's Law: Crime and Democracy in Late Modern America*, 25 LAW & SOC. INQUIRY 1111, 1111-12 (2000) ("The centrality of crime to electoral politics and the formal actions of state and federal politicians has long since become conventional wisdom."); Eli Lehrer, Op-Ed., *It's Hard to Be Soft on Crime*, NAT'L REV. (Dec. 14, 2009), http://www.national review.com/corner/191574/its-hard-be-soft-crime/eli-lehrer ("[P]oliticians across the political spectrum just want to be seen as 'tough on crime' and are unwilling to bend at all even when they know that other policies might be better for the public.").

162. *See* Gershowitz, *supra* note 155, at 53.

163. Gershowitz suggests that it is highly likely that legislators or their immediate family could own smart phones, and that concerns about exposure of financial crimes could prompt them to action. *Id.* Likewise, he suggests that a prominent executive or connected individual could be caught in a scandal involving a search incident to arrest of his cell phone, and as a result lead a lobby against the practice. *Id.*

164. *See id.*

165. *See id.* (noting that it would be difficult to gauge the honesty of law enforcement officials and that it does not prevent the destruction of evidence because an arrestee could delete messages and then close the application).

computer would permit an officer to view all of the contents of the arrestee's personal files. Medical- or financial-record apps would be equally intrusive. This approach fails to provide a definitive limit to the scope of a search incident to arrest.

Permitting officers to carry out a five-step search—essentially allowing officers to make five inputs or clicks on the phone[166]—could similarly reveal highly personal information about an individual. There are also evidentiary problems inherent in determining the number of steps that an officer took, and as Gershowitz indicates, the choice of five steps is entirely arbitrary.[167] The arbitrary selection of permissible steps would result in an uneven application of the rule, allowing different levels of access on different devices. In some cases it could reveal personal information, and in others it could prohibit an officer from accessing a call log. Selecting the appropriate level of steps is "beyond the institutional capacity of courts."[168]

Gershowitz's final suggestion—distinguishing between data stored on the device and remotely stored data[169]—has both privacy and application concerns. While limiting the scope of a search to data stored on the device reduces privacy concerns, this solution fails to address the ever-expanding storage capacity of the phones themselves. For example, the sixty-four gigabyte iPhone has over sixteen hundred times the capacity of the average personal computer manufactured in 1990.[170] A significant privacy concern is the protection of data *on* the phone. The test is likewise problematic in that it requires officers to distinguish information that is remote from that which is local—a virtually impossible task and highly prone to error. Furthermore, phone developers seek to seamlessly integrate remote data into the phone's functionality, enhancing the difficulty of discerning which data is permissible to search. With thousands of cell phone models, it is not the type of bright-line rule needed for Fourth Amendment jurisprudence.

Another suggested approach is to distinguish between smart phones and conventional cell phones.[171] Professor Matthew Orso proposed that for conventional, older-generation cell phones, officers could search coding but not content-based information.[172] Coding

166. *Id.* at 54.

167. *Id.* at 55.

168. *Id.* at 55-56.

169. *Id.* at 56.

170. *See Amazing Facts and Figures About the Evolution of Hard Disk Drives*, ROYAL PINGDOM (Feb. 18, 2010), http://royal.pingdom.com/2010/02/18/amazing-facts-and-figures-about-the-evolution-of-hard-disk-drives.

171. Orso, *supra* note 77, at 221.

172. *Id.* at 212-13.

information is information that identifies the parties to a communication, such as phone numbers, email addresses, or pager numbers.[173] Content-based information is the "substance of a communication" or private information stored for personal use, including "text messages, emails, voicemails, digital photographs, and other data."[174]

The coding-content distinction creates a clear line of demarcation in the virtual scope of a search, and does so in a manner that seems to accurately reflect the point at which an individual's expectation of privacy increases. But Orso indicates that a coding-content distinction is not workable for smart phones.[175] For example, it may be difficult for a law enforcement official to see the sender of a text message or email without inadvertently viewing some of the content, such as the title or body of the message.[176] This would create difficult fact-finding inquiries in suppression cases and prevent desirable bright-line rules.[177]

Instead, Orso argues that because of its likeness to a computer, a search of a smart phone incident to arrest should require a warrant.[178] He suggests that courts should distinguish between coding and content-based information to address privacy concerns for conventional cell phones, while requiring a keyboard-touchpad examination in order for officers to quickly determine if a device is a smart phone.[179]

In *Smith*, both the majority and the dissent rejected this approach for two reasons.[180] First, the rule is unworkable because it would assign officers the difficult task of distinguishing the capabilities of a cell phone prior to each search and then correctly categorizing it as a smart phone or conventional cell phone.[181] Second, a conventional cell phone is not an object limited in functionality to the placing of calls.[182] Rather, even conventional cell phones can connect to the Internet, transfer data, send text messages, take pictures, and more.[183]

---

173. *Id.* at 187-88.

174. *Id.* at 188.

175. *Id.* at 222.

176. *See id.* at 212; *cf. id.* at 222.

177. *Id.* at 222.

178. *Id.* at 221-22.

179. *Id.*

180. State v. Smith, 920 N.E.2d 949, 954-55 (Ohio 2009); *id.* at 957 (Cupp, J., dissenting) ("It would be unworkable to devise a rule that required police to determine the particular cell phone's storage capacity.").

181. *See id.* at 954 (majority opinion).

182. *Id.*

183. *See id.*

Distinguishing a smart phone from a conventional phone by examining whether the phone has a touch screen or a full keyboard seems to be a clean distinction and easy for law enforcement officers to apply. Generally speaking, smart phones have these features and conventional phones do not. But phone designers are now implementing touch screens and full keyboards into conventional cell phones. Orso notes that as this trend grows, "more devices would be protected against warrantless searches incident to arrest."[184] It is not unlikely that progress will incorporate these features into all phones, which would effectively create a rule prohibiting the search of any phone incident to a lawful arrest. Such a rule, however, is contrary to Orso's own conclusion, and that of this Note.[185] A complete restriction on cell phone searches incident to arrest is not an appropriate solution, "because the custodial arrest context does justify a 'reasonable intrusion' into an arrestee's belongings."[186]

Applying a different rule for conventional cell phones and smart phones, no matter the manner of the delineation, may have Equal Protection implications. Smart phones tend to be a more expensive product than conventional cell phones and require costly monthly data plans.[187] The result of a more expensive product is that smart phone owners are likely to be wealthier than owners of conventional cell phones.[188] As such, wealthier individuals who can afford a smart phone would be entitled to more privacy than those who could only afford a conventional cell phone. Hypothetically, in two identical arrests, law enforcement officials could conduct a more intrusive search on a conventional-phone owner than on a smart-phone owner, even though both owners carry the same searchable information. Analysis of whether this implicates a violation of the Equal Protection Clause is an analysis outside the scope of this Note; however, courts should consider the policy rationale resulting from this distinction.

---

184. *Id.* at 222-23.

185. *Id.* at 212.

186. *Id.*

187. *See, e.g.*, Roger Cheng, *AT&T Hikes Data Prices, Caps for Smartphones*, CNET NEWS (Jan. 18, 2012, 2:06 PM), http://news.cnet.com/8301-1035_3-57361397-94 (noting that AT&T smartphone data plans range from twenty to fifty dollars per month).

188. Josh Wolford, *Nielsen: Smartphones Are for the Young, Wealthy*, WEBPRONEWS (Feb. 20, 2012), http://www.webpronews.com/nielsen-smartphones-young-wealthy-2012-02 (noting that Nielsen study indicates that smartphone purchasers are either young or wealthy, or both).

III. USING THE TRADITIONAL FUNCTION OF A CELL PHONE TO DRAW A BRIGHT LINE FOR THE SCOPE OF CELL PHONE SEARCHES INCIDENT TO ARREST

This Note proposes that the appropriate test for the scope of a cell phone search incident to arrest should concern the function of a cell phone. Such a search should be limited to the traditional functions of a cell phone—namely, phone calls and text messages. Under this rule, a law enforcement officer would be allowed to search an arrestee's call log (the record of phone calls), text messages (the record and content of text message communications), and address book (the universe of recipients to whom the owner can call or text), but nothing more. Other functions, such as email, Internet access, mass data storage, photographs, and other software apps are more akin to functions traditionally associated with a computer. When a mobile device incorporates those same computer-like functions, it does not follow that an owner abandons the high expectation of privacy associated with those functions.

A rule predicated on the particular cell phone function has several advantages. The rule is applicable to all cell phones irrespective of their technology and is simple for law enforcement officials to implement. It also addresses an arrestee's heightened privacy concerns and is consistent with much of the early jurisprudence for cell phone searches relying on the container doctrine.

This rule would be simple for law enforcement officials to apply. First, they would not have to distinguish between smart phones and conventional phones, as the rule would apply equally to both. Second, the call log, text message, and address book features operate independently of the proscribed computer-like functionality, such as email. Thus, officers can access these functions on a cell phone without navigating through proscribed features.

Finally, adopting a function-based rule would allow many courts to maintain precedent with respect to the search of a cell phone incident to arrest. The test implicitly acknowledges two types of devices: devices with a finite capacity to hold information and devices with immeasurable storage capacities. The former devices should be subject to the container doctrine, while the virtual scope of the latter devices takes them outside the scope of that doctrine. When a device, such as a smart phone, contains the features of both, it is necessary to determine which functions have an unlimited virtual scope, because the virtual scope creates a heightened expectation of privacy. Because traditional phone functions such as call logs, text messages, and address books have a limited virtual scope, they are associated with

devices that fit within the parameters of the container doctrine, such as a physical address book or a purse.

This function-based rule is consistent with legal precedent; courts have typically validated a cell phone search incident to arrest when the case concerned traditional cell phone functions. Therefore, adopting the rule would not require courts to assert that previous decisions were overly broad or wrongly decided. Rather, a container capable of holding a call history, text message history, and an address book falls within the scope of the container doctrine and does not violate the Fourth Amendment. Where cell phone funtionality appears more like that of a computer, courts should find that the information contained therein falls outside the scope of the container doctrine, thereby preserving heightened expectations of privacy in that information.

The features that fall within the realm of traditional phone functionality, while limited, are not arbitrary. Each feature either raises minimal privacy concerns or has strong analogical ties to accepted container doctrine jurisprudence. For example, courts widely consider call logs, unlike other cell phone features, to have little or no expectation of privacy. An address book on a cell phone is nearly identical to a handwritten address book, which courts have previously deemed within the scope of the container doctrine.[189]

Text messages are the most controversial feature in a function-based rule. But there are strong justifications supporting their inclusion in a search-incident-to-arrest rule. First, text messages are very similar to pager messages, which courts have long upheld as searchable without raising many privacy concerns.[190] While not perfect, the similarities between a pager message and a text message, as opposed to a pager message and an email, are apparent. Second, courts have doubted whether there is a reasonable expectation of privacy in text messages under the third-party doctrine.[191] Unlike a phone conversation, wireless phone companies maintain records of the

189. *See* United States v. Lynch, 908 F. Supp. 284, 288 (D.V.I. 1995) ("Just as police can lawfully search the contents of an arrestee's wallet or address book incident to an arrest, we hold that the agents here could lawfully search the contents of Thomas' pager incident to his arrest."); United States v. Chan, 830 F. Supp. 531, 534 (N.D. Cal. 1993) ("The expectation of privacy in an electronic repository for personal data is therefore analogous to that in a personal address book or other repository for such information.").

190. *See, e.g.*, United States v. Hunter, No. 96-4259, 1998 WL 887289 (4th Cir. Oct. 29, 1998); United States v. Charles, 138 F.3d 257 (6th Cir. 1998); United States v. Ortiz, 84 F.3d 977 (7th Cir. 1996); United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996); United States v. Galante, No. 94 Cr. 633 (LMM), 1995 WL 507249 (S.D.N.Y. Aug. 25, 1995); *Chan*, 830 F. Supp. at 531.

191. *See, e.g.*, United States v. Meriwether, 917 F.2d 955, 959 (6th Cir. 1990).

contents of text messages.[192] Additionally, the message sender does not know if an unknown third party is in possession of the receiving device. Third, the weight of jurisprudence overwhelmingly supports inclusion of text messages.[193]

IV. NARROWLY LIMITING THE EXIGENT-CIRCUMSTANCES JUSTIFICATION FOR CELL PHONE SEARCHES

Because of the increased privacy concerns in cell phone content, judicial rules should not permit officers to merely circumvent a limited search-incident-to-arrest doctrine through a broadly applied exigency justification. As previously noted, the exigency exception to the warrant requirement necessitates an imminent threat to the destruction of evidence.[194] In cell phones, this means the loss of data as a result of subsequent calls or text messages, or the destruction of data by a third party through a remote wipe program.

Technological innovations have made the first concern moot, as modern mobile devices have large storage capacities that do not delete recent communication history.[195] While the threat of a third party erasing the cell phone's data *always* exists so long as the phone can connect to the Internet, the coordination problems in alerting a third party to the arrest and providing instructions to erase the phone's contents greatly reduce the threat of a remote wipe.[196] Thus, the exigency exception should apply only when a law enforcement officer demonstrates that he had probable cause to believe that a third party had been contacted or was prepared to delete the phone's data.[197]

The exigency exception is otherwise inapplicable. An officer with unsubstantiated concerns of a remote wipe has myriad ways of protecting the phone's contents.[198] The officer can disconnect the phone from the Internet, power the phone off, remove the battery, or place the phone in a transmission-resistant container, such as a Faraday bag.[199] Such bags have the ability to block mobile

192. *See Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, ACLU (Aug. 2010), http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.

193. *See, e.g.*, United States v. Young, 278 F. App'x 242, 245-46 (4th Cir. 2008) (finding that officers permissibly accessed and copied text messages in a search incident to arrest); United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007) (holding that officers could search a cell phone's call records and text messages incident to arrest).

194. *Warrantless Searches and Seizures*, *supra* note 17, at 70.

195. *See* United States v. Gomez, 807 F. Supp. 2d 1134, 1151 n.17 (S.D. Fla. 2011).

196. *See supra* Part II.C.

197. *See Gomez*, 807 F. Supp. 2d at 1151 n.17.

198. *See supra* Part II.C.

199. *See* Sutton, *supra* note 152.

transmissions while maintaining the officer's ability to access the phone, and they are not cumbersome for an officer to have on his person or in his patrol vehicle.[200] The ample means to preserve the phone's contents and the low probability of remote wipe actually occurring mitigate any imminent threat of the destruction of evidence.

By narrowly limiting the exigency exception for law enforcement officials, a search incident to arrest would be confined to the function-based test. This test permits police to view traditional cell phone functions, including call history, text messages, and address books. But the rule prohibits officers from viewing any other function of the cell phone, most of which have an unlimited virtual scope and an increased expectation of privacy. The result is a bright-line rule that officers can apply in the field, that takes into consideration the search-incident-to-arrest rationale and precedent, and that also protects the arrestee's heightened expectations of privacy in cell phone data.

V. CONCLUSION

The ubiquity of cell phones and similar wireless devices in society creates many challenges for our legal system. Fundamentally, it requires that the system adapt legal principles to changing norms. With the advent of cell phones and smart phones, individuals have access to a wealth of information in the palm of their hand; however, these devices are also portals to their most personal information.

The Supreme Court created the container doctrine with the purpose of establishing a bright-line rule that permitted an invasion of privacy but limited the encroachment to the physical scope of what an individual could carry. Smart phones effectively remove this basic constraint; digital access to information has become virtually limitless and can be carried in nothing larger than a pocket. Courts must therefore adjust the legal principles of a search incident to arrest to account for the increased expectation of privacy in wirelessly accessible personal information.

Where an absolute prohibition on evidence obtained from a cell phone is contrary to the principles of the search-incident-to-arrest doctrine, unlimited access to that information intrudes upon Fourth Amendment privacy rights. Thus, the balance must be somewhere in between. A function-based test, applying the standard of the container doctrine to the traditional functions of a cell phone, strikes that balance. It provides an easily applied, bright-line rule for law enforcement officials. And it protects privacy expectations by creating

200. *Id.*

definitive boundaries in the virtual scope of a cell phone search. At the same time, this rule does not require a majority of courts to reverse prior decisions regarding the permissible scope of a cell phone search, but instead only narrowly limits those holdings. Only through enunciating a firm line between privacy expectations and the search-incident-to-arrest doctrine can courts protect the guaranteed rights of the Fourth Amendment.

Samuel J. H. Beutler[*]

[*] J.D. Candidate, Vanderbilt University Law School, 2013; B.A., Political Science, History, Yale University, 2007. The Author would like to thank the editorial staff of the VANDERBILT JOURNAL OF ENTERTAINMENT AND TECHNOLOGY LAW for their suggestions, assistance, and tremendous attention to detail during the preparation of this Note.