2-8-2013

Pay Phone Protections in a Smartphone Society: The Need to Restrict Searches of Modern Technology Incident to Arrest

Marty Koresawa

PAY PHONE PROTECTIONS IN A SMARTPHONE SOCIETY: THE NEED TO RESTRICT SEARCHES OF MODERN TECHNOLOGY INCIDENT TO ARREST

*Marty Koresawa**

Since their development in the 1980s, cell phones have become ubiquitous in modern society. Today, cell phones feature large data-storage capacities and can access various types of personal media, making them pocket-sized windows into intimate aspects of an individual's life. Yet many courts treat cell phones as if they were ordinary physical containers, allowing police officers to search the contents of an arrestee's cell phone incident to an arrest. The warrantless search of electronic devices incident to an arrest, however, cannot be justified on the same grounds as a similar search of physical containers. The government does not have a strong interest in searching a cell phone incident to an arrest because the search is exceedingly unlikely to reveal a concealed weapon or prevent the destruction of evidence. Moreover, given the personal nature of cell phones, individuals have a much greater expectation of privacy in their cell phones than they do in physical containers stored on their persons. This Note argues that search of a cell phone incident to arrest should no longer be blindly governed by the same precedent that controls other searches incident to arrest, and it urges the Supreme Court to engage in a fresh and thoughtful balancing of the interests at stake. Only by

* J.D. Candidate, May 2013, Loyola Law School of Los Angeles; B.A., Molecular and Cell Biology, August 2007, University of California, Berkeley. I want to thank Professor Justin Levitt for his incredible support and guidance throughout this process. I also want to thank the staff and editors of the *Loyola of Los Angeles Law Review*, especially Scott Klausner, Kaytee Vota, Sean Degarmo, Leslie Hinshaw, Maya Harel, Emily Shaaya, Roya Rahmanpour, and Andrew Arons. Finally, I owe a tremendous thank you to my family and friends for providing the support to help me get through law school. There are many others I would like to thank, but the Academy has started playing me off the stage.

creating new doctrine can the Supreme Court adequately protect these important interests and restore fidelity to the Fourth Amendment principles that should govern searches incident to arrest.

TABLE OF CONTENTS

I. INTRODUCTION

In 1968, Officer Richard Jenks pulled over and arrested Willie Robinson for driving without a license.[1] Incident to the arrest and pursuant to police department instructions, Officer Jenks conducted a search of Robinson's person.[2] Jenks reached into the breast pocket of Robinson's coat and discovered a crumpled-up cigarette package.[3] When he looked inside the package, Jenks found fourteen "gelatin capsules of white powder which he thought to be, and which later analysis proved to be, heroin."[4]

In *United States v. Robinson*,[5] the United States Supreme Court held that Officer Jenks's conduct in looking inside the cigarette package was reasonable under the Fourth Amendment. The Court stated that because of "the need to disarm the suspect in order to take him into custody" and "to preserve evidence on [the suspect's] person for later use at trial,"[6] officers may search an arrestee and open any containers that they find on the arrestee's person.[7] While the search of a small container like the cigarette package discovered on an arrestee like Robinson might not raise any alarming Fourth Amendment concerns, the *Robinson* Court's decision has had a tremendous impact on modern case law.

In 2007, in *People v. Diaz*,[8] police officers set up a controlled purchase of ecstasy.[9] Gregory Diaz, responsible for driving the ecstasy seller to the meeting where the exchange would take place, was arrested by officers upon his arrival. While conducting a search incident to the arrest, the officers discovered and seized a cell phone from Diaz's pocket.[10] Thereafter, the officers searched the defendant's phone, found a text message that said "6 4 80" and used that message to obtain a confession from Diaz.[11] The California Supreme Court in *Diaz* held that pursuant to U.S. Supreme Court

1. United States v. Robinson, 414 U.S. 218, 220 (1973).
2. *Id.* at 221–22.
3. *Id.* at 221–23.
4. *Id*.
5. 414 U.S. 218 (1973).
6. *See id.* at 234.
7. *See id.* at 236.
8. 244 P.3d 501 (Cal. 2011), *cert. denied*, 132 S. Ct. 94 (2011).
9. *Id.* at 502.
10. *Id.*
11. *Id.* at 502–03.

precedent, the Fourth Amendment did not prohibit officers from searching Diaz's cell phone.[12] The *Diaz* court loosely analogized cell phones to items like the cigarette package in *Robinson* to justify its decision.[13] It went on to say that the propriety of a search incident to arrest did not depend on the character of the item searched.[14]

The search of a drug dealer's phone, the very device used to carry out drug sale transactions, may not sound shocking or outrageous. However, the *Diaz* court's reasoning in justifying the search through its loose analogy to a cigarette package raises one important question: Had Officer Jenks discovered a cell phone in Willie Robinson's pocket, and not a cigarette package, would the U.S. Supreme Court have approved the search of a text message folder incident to arrest?

This Note argues that analogizing cell phones to physical containers, like the cigarette package in *Robinson*, is faulty and results in severe Fourth Amendment violations of privacy. These intrusions signify the need to revisit the decisions governing searches incident to arrest so that future courts will not continue eroding Fourth Amendment protections.

Part II discusses the background of Fourth Amendment principles, the search-incident-to-arrest doctrine, and the doctrine's application to advancing technology. Part III discusses how applying the principles of *Robinson* to cell phones is inherently flawed, and it critiques the way that lower courts have been willing to apply precedent to rationalize warrantless searches of cell phones incident to arrest. Finally, Part IV explores potential solutions that would place much-needed limitations on searches incident to arrest.

II. BACKGROUND

Cell phones have become ubiquitous in modern society,[15] morphing from two-pound portable communication devices into pocket-sized computers with massive capabilities.[16] As a result, the

12. *Id.* at 511.

13. *Id.* at 505–06.

14. *Id.* at 506.

15. As of June 2012, 321.7 million wireless subscriptions existed in the United States. *CTIA Consumer Info: U.S. Wireless Quick Facts*, CTIA, http://www.ctia.org/consumer_info/index.cfm/AID/10323 (last visited Dec. 20, 2012).

16. In 1973, Motorola developed a prototype of the first cell phone, which measured over a foot long, weighed almost two pounds, and could store approximately thirty phone numbers.

collision between advancing technology and the Fourth Amendment was inevitable.[17] The following discussion examines the case law that governs the basic principles behind Fourth Amendment jurisprudence and searches incident to arrest, and it considers the application of those principles toward recently emerging technologies.

A. General Fourth Amendment Principles

The Fourth Amendment prohibits unreasonable searches of "persons, houses, papers, and effects."[18] The Supreme Court has interpreted the Fourth Amendment to govern police conduct that either physically invades an area enumerated in the Fourth Amendment or infringes on a person's justifiable expectation of privacy.[19]

In *Katz v. United States*,[20] the Court held that the Fourth Amendment prohibited attaching a wiretap to the outside of a public telephone booth because it intruded on the defendant's justifiable expectation of privacy.[21] Justice Harlan, in his concurrence, provided a two-prong test to determine what constitutes a reasonable expectation of privacy: (1) the person has a subjective expectation of privacy; and (2) society is willing to recognize that expectation.[22]

Generally, this expectation of privacy requires government agents to obtain a warrant based on probable cause before they can search anything protected under the provisions of the Fourth Amendment.[23] These provisions restrict state action in the following ways:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and

Liane Cassavoy, *In Pictures: A History of Cell Phones*, at 1 of 16, PCWORLD (May 7, 2007, 1:00 AM), http://www.pcworld.com/article/131450/in_pictures_a_history_of_cell_phones.html. Modern-day smartphones are capable of far greater data storage and data access capabilities. *See, e.g.*, *iPhone: Technical Specifications*, APPLE, http://support.apple.com/kb/sp2 (last modified Feb. 19, 2010).

17. *See, e.g.*, *Diaz*, 244 P.3d at 503–04.
18. U.S. CONST. amend. IV.
19. United States v. Jones, 132 S. Ct. 945, 949–51 (2012).
20. 389 U.S. 347 (1967).
21. *Id.* at 353.
22. *Id.* at 361 (Harlan, J., concurring).
23. *See* U.S. CONST. amend. IV.

> 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.[24]

The Fourth Amendment is not an absolute demand for a warrant or probable cause. The touchstone of Fourth Amendment jurisprudence is that searches must be reasonable.[25] A warrantless search may withstand Fourth Amendment scrutiny if "the governmental interest [that] allegedly justifies official intrusion" outweighs "the constitutionally protected [privacy] interests of the private citizen."[26]

Courts have delineated the factors and principles that should be considered to determine the weight of the privacy interest and the weight of the governmental need. These factors include society's expectation of privacy,[27] the officer's safety,[28] the risk of losing evidence,[29] and the need for clear rules that are easily applied.[30] The Supreme Court has also stated that "[t]he scope of [a] search must be strictly tied to and justified by the circumstances which rendered its initiation permissible."[31]

B. Searches Incident to Arrest

One exception to the warrant and probable cause requirements is searches incident to arrest.[32] The Court in *Chimel v. California*[33] was the first to articulate the modern-day conception of a search incident to an arrest.[34] In *Chimel*, police officers arrested the defendant at his

24. *Id.*

25. *See Katz*, 389 U.S. at 353 ("[T]he Fourth Amendment protects people—and not simply 'areas'—against *unreasonable* searches and seizures." (emphasis added)).

26. Terry v. Ohio, 392 U.S. 1, 20–21 (1968).

27. California v. Carney, 471 U.S. 386, 391 (1985); *Terry*, 392 U.S. at 24–25.

28. Chimel v. California, 395 U.S. 752, 762–63 (1969); *Terry*, 392 U.S. at 23.

29. *Chimel*, 395 U.S. at 762–63; Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).

30. Acevedo v. California, 500 U.S. 565, 576 (1991); *see* United States v. Robinson, 414 U.S. 218, 235 (1973) (creating a categorical authority to searches incident to arrest because officers make "quick *ad hoc* judgment[s]" in the field).

31. *Terry*, 392 U.S. at 19 (internal quotation marks omitted).

32. *Robinson*, 414 U.S. at 224 ("It is well settled that a search incident to a lawful arrest is a traditional exception to the warrant requirement of the Fourth Amendment.").

33. 395 U.S. 752 (1969).

34. Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 33 (2008).

home on burglary charges.[35] A subsequent search of the defendant's entire three-bedroom home led officers to discover evidence that linked the defendant to the burglary.[36] The Supreme Court held that the search of the defendant's home was unconstitutional because the rationale underlying the search-incident-to-arrest doctrine could not justify a search of the defendant's entire home.[37]

The Court in *Chimel* reasoned that two compelling needs justified a search incident to an arrest: first, the need for officers to disarm an arrestee; and second, the need to prevent the concealment or destruction of evidence.[38] The Court recognized that searches incident to arrest may extend to areas where an arrestee may obtain a weapon or destructible evidence.[39] However, a full search of an arrestee's house would extend beyond these areas and violate the main evil that the Fourth Amendment sought to proscribe: "general warrants and warrantless searches that had so alienated the colonists."[40]

The language in *Chimel* resulted in some confusion about whether the Court restricted the use of these searches only to situations in which the search would promote officer safety or prevent the loss of evidence that was material to the arrest, or whether the Court granted officers a categorical right to search an arrestee.[41] The *Chimel* Court stressed that a warrantless search should be no more intrusive than is necessary to address the concerns that justify the departure from the Fourth Amendment's warrant and probable cause requirements.[42] However, the plain language of the

35. *Chimel*, 395 U.S. at 753.
36. *Id.* at 754.
37. *Id.* at 768.
38. *Id.* at 762–63.
39. *Id.* at 763.
40. *Id.* at 761, 765–66.
41. Wayne A. Logan, *An Exception Swallows a Rule: Police Authority to Search Incident to Arrest*, 19 YALE L. & POL'Y REV. 381, 392 (2010). In *Chimel*, the Court states the following:

> [I]t 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. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.

Chimel, 395 U.S. at 763.
42. *Chimel*, 395 U.S. at 764 (citing Sibron v. New York, 392 U.S. 40, 67 (1967)).

opinion would suggest that the Court authorized officers to search an arrestee for any purpose incident to a lawful custodial arrest.[43] Put differently, the "bare fact of arrest" grants officers a right to search an arrestee.[44]

In *United States v. Robinson*, the Supreme Court ruled that searches incident to arrest were per se reasonable, placing significant weight on the need for administrable Fourth Amendment limitations in stressful and uncertain situations.[45] In *Robinson*, an officer arrested the defendant for operating a vehicle without a license.[46] When the officer subsequently searched the defendant, he found a "crumpled up cigarette package" in the breast pocket of the defendant's coat.[47] Looking inside the package, the officer found what later turned out to be heroin.[48]

The Court overturned the Court of Appeals for the District of Columbia Circuit decision to suppress the evidence.[49] The appellate court relied heavily on the Supreme Court's decision in *Terry v. Ohio*,[50] reasoning that all searches must be "no more intrusive" than the justifications for initiating the search allow.[51] The appellate court reasoned that the search could not be justified by an evidentiary purpose[52] and that the officer had already recovered the only evidence related to the crime that triggered the arrest that "he could possibly have had probable cause to believe was in the arrestee's possession."[53]

The appellate court further held that searches incident to arrest that were justified only by the need to disarm an arrestee must be limited to a frisk unless "circumstances . . . give the officer reasonable grounds to believe that the person with whom he is

43. *Id.* at 763.
44. Logan, *supra* note 41, at 392.
45. *See* United States v. Robinson, 414 U.S. 218, 234 n.5, 235 (1973).
46. *Id.* at 220.
47. *Id.* at 223.
48. *Id.*
49. *Id.* at 236.
50. 392 U.S. 1 (1968).
51. United States v. Robinson, 471 F.2d 1082, 1094 (D.C. Cir. 1972), *rev'd*, 414 U.S. 218.
52. *Id.* at 1095.
53. *Id.* at 1094. Officer Jenks pulled over Robinson after witnessing him driving a vehicle, and Jenks had reason to believe Robinson's license had been revoked. *Id.* at 1088. Therefore, the only evidence the officer needed or could possibly have found was the fraudulent temporary driver's permit that he had already obtained. *Id.* at 1093.

dealing is armed and presently dangerous."[54] The court acknowledged that while a frisk may not uncover all weapons and would not eliminate all conceivable danger to the officer, it would uncover a majority of weapons. Additionally, the balancing of police and privacy interests favored limiting weapons searches to frisks unless other reasons supported a more intrusive search.[55]

The Supreme Court rejected the appellate court's reasoning and established a bright-line rule that authorized officers to search an arrestee's person as well as the contents of any containers found on an arrestee's person.[56] The *Robinson* Court reasoned that because an officer's extended exposure to an arrestee during a custodial arrest posed a significantly greater risk than during a brief investigative stop, all custodial arrests justified a full search of the person, even if the offense of arrest was a mere traffic violation.[57] The *Robinson* Court rejected a subjective rule that would force officers to assess the probability that an arrestee possessed weapons or evidence and stated that a lawful arrest is sufficient to justify a search of the arrestee's person.[58]

Accordingly, *Robinson* stands for the proposition that searches of the person are automatically permissible after an arrest and need not be supported by the underlying justifications espoused in *Chimel*.[59] Subsequent cases have applied *Robinson* and its progeny to justify searches of wallets and address books found on an arrestee's person.[60]

C. Technology and the Search Incident to Arrest

The Fourth Amendment's clash with technology is not something that the Founders could have foreseen. As new

54. *Id.* at 1097.
55. *Id.* at 1099–1101.
56. United States v. Robinson, 414 U.S. 218, 235 (1973).
57. *Id.* at 234–35.
58. *Id.* at 235.
59. Gershowitz, *supra* note 34, at 34; Chelsea Oxton, Note, *The Search Incident to Arrest Exception Plays Catch Up: Why Police May No Longer Search Cell Phones Incident to Arrest Without a Warrant*, 43 CREIGHTON L. REV. 1157, 1167 (2011).
60. *See, e.g.*, United States v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993) (holding that a search of a wallet and address book incident to arrest was valid); *see also* United States v. Lynch, 908 F. Supp. 284, 288 (D.V.I. 1995) (citing numerous cases upholding searches of wallets and address books incident to arrest across various circuits).

technologies emerge, courts have placed great emphasis on the personal and intrusive capabilities of technologies.[61] Both state and federal courts, however, have generally been hesitant to differentiate modern devices that store electronic data from more conventional items.[62] Courts have either made a direct analogy to conventional containers based on functional equivalence or entirely disregarded the nature and quality of a particular item.[63]

1. Searches of Pagers Incident to Arrest

In *United States v. Chan*,[64] an undercover DEA agent met with a drug dealer in a motel room to purchase heroin.[65] The drug dealer, using the motel telephone, paged the defendant and arranged for a delivery of heroin.[66] After the defendant made the delivery, the agents arrested him and seized an inactive pager from his person.[67] The agents activated the pager and thereafter retrieved several telephone numbers that connected the defendant to the drug dealer in the motel room.[68]

The court denied the defendant's motion to suppress the evidence that the DEA agents retrieved from his pager.[69] The court compared the pager to a closed container and concluded that the Fourth Amendment did not prohibit the agent's search of the

61. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) ("We think that obtaining by sense-enhancing technology any information regarding the interior of a home that could not otherwise be obtained without 'physical intrusion into a constitutionally protected area' constitutes a search—at least where (as here) the technology in question is not in general public use." (internal citation omitted)); Katz v. United States, 389 U.S. 347, 352 (1967) ("To read the Constitution [to not protect telephone booths] is to ignore the vital role that the public telephone has come to play in private communication.").

62. *See* United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) (holding that a cell-phone search incident to arrest was valid because police had the authority to search any containers immediately associated with the person during an arrest); United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993); People v. Balint, 41 Cal. Rptr. 3d 211, 218 (Ct. App. 2006) ("We perceive no reasonable basis to distinguish between records stored electronically on the laptop and documents placed in a filing cabinet or information stored in a microcassette.").

63. *See, e.g.*, United States v. Arnold, 533 F.3d 1003, 1009–10 (9th Cir. 2008); *Chan*, 830 F. Supp. at 535; Hawkins v. State, 704 S.E.2d 886, 891 (Ga. Ct. App. 2010), *aff'd*, 723 S.E.2d 924 (Ga. 2012) (stating that cell phones should be considered a "container that stores thousands of individual containers").

64. 830 F. Supp. 531 (N.D. Cal. 1993).

65. *Id.* at 532–33.

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.* at 536.

defendant's pager because the pager was searched incident to arrest.[70] The court relied on *New York v. Belton*,[71] which stated that a closed container "may . . . be searched whether it is open or closed," to support its conclusion that the search was valid.[72] The court conceded that "there was no danger that [the defendant] would in any way produce a weapon from the pager, and probably no threat that he would access the pager to destroy evidence," but it still found the search constitutional because it considered the pager to be a container.[73]

Subsequent cases analyzed that very same issue and arrived at the same conclusion.[74] In *United States v. Ortiz*,[75] the court upheld the retrieval of telephone numbers from a pager recovered incident to arrest.[76] However, the court in *Ortiz*, while agreeing with the decision in *Chan*, paid particular attention to the specific characteristics of the pager that connected it to one of the justifications behind a search incident to arrest.[77] Specifically, the court noted that because a pager has a finite amount of memory, the data could be lost due to incoming messages, and in some cases, turning off a pager could erase its memory.[78] Accordingly, these characteristics suggested that evidence was at risk of being lost and justified the officer's search of the pager.

While the use of pagers has become a rarity in our society, now replaced by cell phones and more sophisticated technological devices,[79] these cases continue to be relevant today. The pager cases laid the framework for analyzing the propriety of searches of cell phones incident to arrest.[80]

70. *Id.* at 534–36.
71. 453 U.S. 454 (1981).
72. *Chan*, 830 F. Supp. at 535.
73. *Id.* at 536.
74. Gershowitz, *supra* note 34, at 37.
75. 84 F.3d 977 (7th Cir. 1996).
76. *Id.* at 984.
77. *Id.*
78. *Id.*
79. Gershowitz, *supra* note 34, at 38.
80. *See, e.g.*, United States v. McCray, No. CR408-231, 2009 WL 29607, at *3 (S.D. Ga. Jan. 5, 2009) ("[L]aw enforcement officers have the authority to immediately 'search' or retrieve, incident to a valid arrest, information from a pager in order to prevent its destruction as evidence." (quoting *Oritz*, 84 F. 3d at 984)).

2. Searches of Cell Phones Incident to Arrest

When addressing the search of cell phones incident to arrest, many courts have followed a line of reasoning similar to that used in the pager cases.[81] Like the pager cases, the central question regarding an officer's authority to search a cell phone pursuant to *Robinson* remains the same: whether a device containing digital data is a "container" as contemplated by the *Robinson* Court.[82] However, the reasoning has become far more strained, since courts have shown their willingness to simply ignore the key features that make the analogy work.[83] Although one court described cell phones as novel objects that defy easy categorization,[84] most courts have continued to validate the analogy of cell phones to containers.[85]

For example, in *United States v. Finley*,[86] the court accepted the government's argument that a cell phone is like a closed container.[87] Therefore, the court found that pursuant to *Robinson*, the cell phone fell within the scope of a search incident to arrest.[88] Similar to the way the *Chan* court treated the pager, the *Finley* court treated the cell phone as if it were a physical container.[89] The Court of Appeals of Georgia in *Hawkins v. State*[90] also applied similar reasoning, but instead of treating cell phones as traditional containers, it treated the cell phone as a container with many containers inside.[91]

81. *Id.* (citing "recent cases [that] have treated mobile telephones and digital cameras in the same manner" as pagers).

82. Smallwood v. State, 61 So. 3d 448, 459 (Fl. Dist. Ct. App.), *cert. granted*, 68 So. 3d 235 (Fla. 2011).

83. *See, e.g.*, United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009).

84. State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) ("Given their unique nature as multifunctional tools, cell phones defy easy categorization.").

85. *See, e.g.*, United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) (accepting the defendant's argument that a cell phone is like a closed container); Hawkins v. State, 704 S.E.2d 886, 891 (Ga. Ct. App. 2010) (treating a cell phone as a container containing many containers), *aff'd*, 723 S.E.2d 924, 925–26 (Ga. 2012).

86. 477 F.3d 250 (5th Cir. 2007).

87. *Id.* at 259.

88. *Id.*

89. *Compare id.* at 260 (holding that the search of the cell phone was lawful because "[t]he permissible scope of a search incident to a lawful arrest extends to containers found on the arrestee's person"), *with* United States v. Chan, 830 F. Supp. 531, 536 (N.D. Cal. 1993) (holding that the search of the pager was lawful because the pager was a container that was seized incident to arrest).

90. 704 S.E.2d 886, 891 (Ga. Ct. App. 2010).

91. *Id.* at 891.

Other cases indirectly relate cell phones to the pager-container cases by focusing on the similar functions of pagers and cell phones. In *United States v. Murphy*,[92] the court upheld the search of text messages stored in the defendant's cell phone incident to arrest.[93] The court, citing to *Ortiz* to support its decision,[94] explained that, like pagers, the information stored on a cell phone was volatile; as a result, the officer's search of the cell phone was justified to preserve evidence.[95] However, the court also suggested that data volatility did not depend on storage capacity,[96] diverting from the rationale used in *Ortiz*, which was premised on the limited nature of a pager's memory.[97]

Other courts have employed far simpler analogies that disregard the nature and quantity of the information contained in cell phones altogether. Rather than analogize a cell phone to a container by function, these courts have been willing to equate any object to a cigarette package, as long as the object is found on the arrestee's person;[98] one such case was *People v. Diaz*.[99]

In *Diaz*, officers arrested the defendant for suspected drug dealing.[100] When the officers seized the defendant's cell phone incident to arrest and searched its text message inbox, they found evidence of a drug deal.[101] The defendant moved to suppress the evidence recovered from his cell phone.[102]

The Supreme Court of California affirmed the denial of the defendant's motion.[103] The court relied on U.S. Supreme Court decisions that justified the search of any container found on the person.[104] While the court acknowledged the vast amount of information that is stored on cell phones as compared to other

92. 552 F.3d 405 (4th Cir. 2009).
93. *Id.* at 411.
94. *Id.* (citing United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996)).
95. *Id.*
96. *Murphy*, 552 F.3d at 411.
97. *Ortiz*, 84 F.3d at 984.
98. *See, e.g.*, People v. Diaz, 244 P.3d 501, 506–07 (Cal. 2011), *cert. denied*, 132 S. Ct. 94 (2011).
99. *Id.*
100. *Id.* at 502.
101. *Id.* at 502–03.
102. *Id.* at 503.
103. *Id.* at 511.
104. *Id.* at 506–07.

containers, it nevertheless held that the nature of the object was irrelevant for Fourth Amendment analysis.[105]

In contrast, some courts have reasoned that the nature of the data stored within cell phones is critical to the Fourth Amendment analysis.[106] For example, in *State v. Smith*,[107] the Supreme Court of Ohio suppressed the evidence that was recovered from the defendant's cell phone.[108] The court abandoned the reasoning of the pager cases and rejected the government's analogy that a cell phone is a closed container.[109] The court relied on *New York v. Belton*, which defined a closed container as "any object capable of holding another object."[110] The *Smith* court continued that the contents of an electronic device are "wholly unlike any physical object found within a closed container," and it held that a cell phone was not a closed container as contemplated by *Robinson*.[111]

The flaw in the *Diaz* court's rationale becomes apparent when one considers cell-phone-search cases like *Smith*, in which the court recognized that applying *Robinson* to modern devices conflicts with the underlying principles of the Fourth Amendment.[112] The search-incident-to-arrest doctrine and other Fourth Amendment exceptions are based on the premise that the governmental interest outweighs the privacy concerns of private citizens.[113]

III. CRITIQUE

A. Robinson *and Its Progeny Should Not Control Searches of Cell Phones Incident to Arrest*

Cases that authorize warrantless searches of cell phones incident to arrest often rely on *Robinson* to support their conclusions.[114]

105. *Id.*

106. *See, e.g.*, Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1167–70 (D. Or. Jan. 18, 2012); Smallwood v. State, 61 So. 3d 448, 461 (Fla. Dist. Ct. App. 2011); State v. Smith, 920 N.E.2d 949, 956 (Ohio 2009). .

107. 920 N.E.2d 949 (Ohio 2009).

108. *Id.* at 956.

109. *Id.* at 953–54.

110. *Id.* at 954 (quoting New York v. Belton, 453 U.S. 454, 460 n.4 (1981)).

111. *Id.*

112. *Id.* at 956.

113. Terry v. Ohio, 392 U.S. 1, 20–21 (1968).

114. *See, e.g.*, United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007); People v. Diaz, 244 P.3d 501, 505–06 (Cal. 2011), *cert. denied*, 132 S. Ct. 94 (2011).

However, the analogies to *Robinson* that courts use in these cases fail to account for the key characteristics of cell phones that make *Robinson* inapplicable.

1. *Robinson*'s Scope Was Limited by the Physical Restrictions Inherent in the Technology Available at That Time

One scholar has appropriately criticized the courts' use of functional analogies to equate cell phones to standard containers, stating that this mode of analysis "leads courts to deviate over time (and often subconsciously) from the intended arc of precedent."[115] In order to avoid such faulty analogies, courts must account for any implied limitations of prior decisions when considering whether functional analogies are appropriate.[116] One such implicit limitation has been the physical limits of containers at the time of the decision.

Although the Supreme Court did not explicitly define a "container" as "any object capable of holding another object" until *Belton* in 1981,[117] the historical context of *Robinson* strongly suggests that the Court's holding considered only physical objects.[118] A search of a pocket-sized container would have a natural limit to its invasiveness because only so much information could physically be in someone's pocket. Additionally, the Supreme Court viewed the nature of what could be found as far less personal,[119] unlike the communications, photos, contacts, and other information regularly

115. Luke M. Milligan, *Analogy Breakers: A Reality Check on Emerging Technologies*, 80 MISS. L.J. 1319, 1328–30 (2011).

116. *Id.* at 1332–33.

117. New York v. Belton, 453 U.S. 454, 461 n.4 (1981). By the time the Court decided *Belton* on July 1, 1981, cell phones were already in the headlines. *FCC Plans to Give AT&T Large Share of Mobile Phone Market*, WALL ST. J., Apr. 9, 1981. Therefore, the fact that *Belton* defined containers as "any object capable of holding another object" once portable electronic devices began to impact the United States supports an inference that the Court intended not to adjudicate rules regarding electronic devices until after it understood the capabilities of the devices.

118. This Note adopts *Belton*'s definition of a physical container as "any object capable of holding another object." *Belton*, 453 U.S. at 461 n.4. A physical object is defined as a tangible item.

119. *Cf.* Wyoming v. Houghton, 526 U.S. 295, 303 (1999) (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (stating that vehicles "seldom serve as . . . the repository of personal effects" (alteration in original)).

stored on modern cell phones that could reveal the intimate details of one's life.[120]

Moreover, a rule that treats searches incident to arrest as per se reasonable, as adopted in *Robinson*, would be highly inconsistent with Fourth Amendment principles unless the *Robinson* Court presumed the privacy interests at stake were minimal. The dissent in *Robinson* pointed out that under the majority's reasoning, even when the likelihood of finding weapons is highly remote, officers would be granted authority to conduct highly intrusive searches.[121] However, the examples cited to by the dissent—wallets and an attorney's envelope[122]—either have only limited personal information or are anecdotal. Thus, the level of intrusion that the *Robinson* Court authorized was categorically minimal, and even when accounting for instances in which the government need was trivial, the searches would be reasonable overall.

At the very least, the Supreme Court did not and could not contemplate that searches incident to arrest could potentially intrude into unlimited private information. Because the development of cell phones did not take off until after *Robinson*, the court could not have foreseen the vast and widespread use of technologies available in today's society.[123] These technological advancements have allowed the average amount and personal nature of information within a

120. *See, e.g.*, Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1169–70 (D. Or. Jan. 18, 2012) (noting that in *Newhard v. Borders*, 649 F. Supp. 2d 440 (W.D. Va. 2009), officers found intimate pictures of the owner's girlfriend stored on his cell phone); Smallwood v. State, 61 So. 3d 448, 460–61 (Fl. Dist. Ct. App. 2011) ("[C]ell phones can make the entirety of one's personal life available for perusing by an officer every time someone is arrested for any offense. It seems this result could not have been contemplated or intended by the *Robinson* court.").

121. United States v. Robinson, 414 U.S. 218, 256–57 (1973) (Marshall, J., dissenting) ("Would it be reasonable for the police officer, because of the possibility that a razor blade was hidden somewhere in the wallet, to open it, remove all the contents, and examine each item carefully? Or suppose a lawyer lawfully arrested for a traffic offense is found to have a sealed envelope on his person. Would it be permissible for the arresting officer to tear open the envelope in order to make sure that it did not contain a clandestine weapon—perhaps a pin or a razor blade?").

122. *Id.*

123. *Technology Timeline: 1752–1990*, PUB. BROAD. SERV., http://www.pbs.org/wgbh/amex/telephone/timeline/timeline_text.html (last visited Sept. 26, 2011). In the 1970s, the FCC was still in the process of approving cell phone systems. SRI International, *The Cellular Telephone*, *in* THE ROLE OF NSF'S SUPPORT OF ENGINEERING IN ENABLING TECHNOLOGICAL INNOVATION–PHASE II (David Roessner ed., 1998). The first smartphones were capable of accessing the Internet, running programs, and storing massive amounts of data, Cassavoy, *supra* note 16, at 3 of 16, and became available to consumers in 2001. *Id.* at 6 of 16.

person's pocket today to far exceed what the Court could have expected at the time it decided *Robinson*.

However, many courts continue to discount the importance of physicality and analogize cell phones to conventional items.[124] Some courts even disregard the nature of the item altogether, without ever questioning whether a 1970s decision should apply to twenty-first century technology.[125] This faulty application of *Robinson* has led courts to ratify highly invasive police conduct that is inconsistent with the Fourth Amendment.[126]

2. *Robinson* Sought to Eliminate Quick, Ad Hoc Judgments in the Field in Order to Maximize Officer Safety

When dealing specifically with physical containers, officers face an inherently uncertain situation because the presence of weapons or destructible evidence is unclear.[127] This inherent uncertainty is precisely what necessitated the per se rule established in *Robinson*.

The *Robinson* Court established this rule to prevent officers in the field from being forced to determine in ambiguous circumstances whether a search falls within a recognized exception.[128] The two underlying rationales that justify a search incident to arrest are to disarm arrestees and to prevent the destruction of evidence.[129] When the Court decided that a search incident to arrest was per se reasonable, the Court relied heavily on a policy rationale that police officers should not have to predict how courts would define the permissible scope of a search incident to arrest in ambiguous situations.[130]

The Supreme Court has often established bright-line rules to ensure police officers have a clear understanding of the scope of their

124. *See, e.g.*, People v. Diaz, 244 P.3d 501, 506 (Cal. 2011) (stating that the relevant high court decisions do not "depend[] on the item's character"), *cert. denied*, 132 S. Ct. 94 (2011).

125. *Id.*; *see, e.g.*, United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007). *But see Smallwood*, 61 So. 3d at 461.

126. *Smallwood*, 61 So. 3d at 461 ("[C]ell phones can make the entirety of one's personal life available for perusing by an officer every time someone is arrested for any offense. It seems this result could not have been contemplated or intended by the *Robinson* court.").

127. *Robinson*, 414 U.S. at 234–35 & n.5.

128. *Id.* at 235.

129. Chimel v. California, 395 U.S. 752, 762–63 (1969).

130. *Id.*

authority.[131] Bright-line rules reduce officer hesitation in the field that may endanger the officer or lead to less effective law enforcement.[132] Although the *Robinson* Court acknowledged the need to prevent the destruction of evidence,[133] its analysis suggests that its primary concern was to ensure that officers could disarm an arrestee to protect themselves from physical injury without fear that valuable evidence would later be suppressed in court.[134]

The *Robinson* Court maximized officer safety by allowing officers to fully inspect any item no matter how innocuous it may appear externally.[135] As a consequence, the Court also allowed officers to seize any and all evidence that could be destroyed.[136] However, unlike physical objects, the data stored on cell phones cannot contain a clandestine weapon. Because cell phones only store electronic data, courts have recognized that cell phones do not implicate officer-safety concerns.[137] Therefore, the primary reason behind *Robinson*'s bright-line rule—officer safety—is inapplicable.

3. Cell Phones Do Not Implicate the Evidentiary Concerns Underlying Searches Incident to Arrest

In light of the fact that cell phones do not implicate officer-safety concerns, the only remaining justification to search arrestees incident to an arrest is to prevent the loss of evidence. However, the

131. *See* Atwater v. City of Lago Vista, 532 U.S. 318, 347 (2001) ("Fourth Amendment balance is not well served by standards requiring sensitive, case-by-case determinations of government need, lest every discretionary judgment in the field be converted into an occasion for constitutional review."); Davis v. United States, 512 U.S. 452, 453 (1994) (holding that an ambiguous request for an attorney does not cease questioning because to impose such a rule would force officers to make difficult judgment calls about the suspect's desire for an attorney); United States v. Ross, 456 U.S. 798, 822 n.30 (1982) (expressing concern over "[t]he propriety of the warrantless search . . . turn[ing] on an objective appraisal of all the surrounding circumstances"); New York v. Belton, 453 U.S. 454, 459–60 (1981) (holding that incident to a lawful arrest, police officers may search the entire passenger compartment of a vehicle, resolving a conflict of authorities that reach different conclusions in similar factual circumstances).

132. *Cf.* Hudson v. Michigan, 547 U.S. 586, 595–96 (2006) (discussing the consequences of applying the exclusionary rule to a knock-and-announce violation).

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

134. *See id.* at 234–35.

135. *Id.*

136. *Id.* at 234.

137. *See, e.g.*, United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *9 (N.D. Cal. May 23, 2007).

electronic data stored on a cell phone are different from physical evidence because, as a general matter, they cannot be destroyed.

Unlike physical evidence, electronic data cannot become irrecoverable.[138] Courts have reasoned that text messages and call logs stored on a cell phone are volatile because incoming communications may erase the existing information.[139] Remote-wipe applications that allow users to delete data remotely increase this concern.[140] However, any deleted evidence is not permanently lost because a cell phone's deleted data may still be recovered.[141]

Courts and scholars have recognized this fact.[142] Call records and text messages are available from the service provider.[143] Even if service providers do not keep such information, when a user deletes data on a cell phone, the device marks that data to be overwritten if necessary.[144] This "deleted" data actually remain on a cell phone until new data overwrites them.[145] New devices are capable of

138. *See* United States v. James, No. 1:06CR134 CDP, 2008 WL 1925032, at *7 n.3 (E.D. Mo. Apr. 29, 2008); Matthew E. Orso, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 SANTA CLARA L. REV. 183, 199–200 (2010).

139. *See, e.g.*, United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3–4 (E.D. Wis. Feb. 8, 2008) (finding that "call histories on cell phones could be deleted or lost, giving rise to a legitimate concern about destruction of evidence"); United States v. Parada, 289 F. Supp. 2d 1291, 1303–04 (D. Kan. 2003) (finding that cell phones have limited memory and therefore incoming calls could overwrite earlier stored numbers). However, one court stated that text messages are not volatile because they will remain on the cell phone unless the user deletes them. United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *4 (S.D. Fla. Dec. 22, 2008).

140. Ashley B. Snyder, *The Fourth Amendment and Warrantless Cell Phone Searches: When Is Your Cell Phone Protected?*, 46 WAKE FOREST L. REV. 155, 179 (2011); *see also* Kevin McLaughlin, *McAfee Unveils Strategy to Secure Mobile Devices, Data, Apps*, CRN (Sept. 20, 2011, 8:44PM), www.crn.com/news/security/231601800/mcafee-unveils-strategy-to-secure-mobile-devices-data-apps.htm ("One example on the consumer side is McAfee Mobile Security, which allows customers to . . . remotely wipe data on devices if they're lost or stolen.").

141. *See supra* note 138 and accompanying text.

142. *See supra* note 138 and accompanying text.

143. *James*, 2008 WL 1925032, at *7 n.3 ("The service provider keeps records of the incoming and outgoing calls."); Orso, *supra* note 138, at 199. The Computer Crime and Intellectual Property Section of the U.S. Department of Justice reported that call detail records and text message details may be stored by a service provider for up to seven years, and text message content for up to ninety days. *Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, ACLU, http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart (last visited Oct. 3, 2012).

144. Jacob Leibenluft, *Do Text Messages Live Forever? How a Dirty SMS Can Come Back to Haunt You*, SLATE (May 1, 2008, 6:51 PM), www.slate.com/articles/news_and_politics/explainer/2008/05/do_text_messages_live_forever.html. Data occupy a certain "location" on a memory storage device, and they are not actually erased from the device's memory until new information needs to use the same memory "location" and replaces the old information. *Id.*

145. *Id.*

recovering deleted data off old phones and other portable electronic devices.[146] For example, companies such as Cellebrite offer a mobile forensic device capable of extracting existing, hidden, and deleted data.[147]

Programs for computers, such as "Evidence Eliminator," go a step further than cell phones do by not only deleting any previously existing computer data but also overwriting the computer's memory with random data.[148] Analogous programs for cell phones arguably make data on cell phones volatile and justify searches of cell phones incident to arrest based on the need to prevent the destruction of evidence.

However, computer forensics experts are able to recover data that have been overwritten by many layers of new data.[149] Considering the natural progression of technology and the increasing similarity between modern cell phones and computers,[150] computer forensic experts are likely to soon be able to recover overwritten data from cell phones. Additionally, cell phone programs are dependent on a user or signal to initiate them.[151] Put differently, if an officer is able to prevent a cell phone from receiving a signal, an individual is powerless to eliminate the data on that device. Therefore, programs cannot destroy the data if officers seize an arrestee's phone and either remove the battery or place the cell phone in an area where it cannot receive a signal.[152] Moreover, cutting off a cell phone's signal would be far more effective at preserving evidence than would the officer browsing through a cell phone's contents contemporaneously

146. *See generally*, WAYNE JANSEN & RICK AYERS, GUIDELINES ON CELL PHONE FORENSICS: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 13–23 (2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf (generally describing the capabilities of the tools available to law enforcement for the purposes of recovering data from cell phones and other portable devices).

147. *UFED Ultimate*, CELLEBRITE, http://www.cellebrite.com/mobile-forensics-products/forensics-products/ufed-ultimate.html (last visited Oct. 3, 2012).

148. Daniel Engber, *Can You Ever Really Erase a Computer File? What If You Use Evidence Eliminator?*, SLATE (June 29, 2005), http://www.slate.com/articles/news_and_politics/explainer/2005/06/can_you_ever_really_erase_a_computer_file.html.

149. *Id.*

150. *See, e.g.*, Martyn Williams, *Samsung Phone Features a Hard Drive: Windows-based Cell Phone Includes 3GB Hard Drive for Storage*, PCWORLD (Mar. 10, 2005), www.pcworld.com/article/119961/samsung_phone_features_a_hard_drive.html.

151. Jamie Lendino, *Kill Your Phone Remotely*, PCMAG (Sept. 11, 2009), http://www.pcmag.com/article2/0,2817,2352755,00.asp#fbid=2WAnUDlh8gk.

152. *Id.*

with the arrest because it would ensure that the arrestee cannot actually delete the data on a cell phone.

Arguably, there will be rare circumstances in which evidence contained on a cell phone could be destroyed, such as when forensic experts cannot recover overwritten data. However, the Court has been, and should be, guided by general circumstances rather than anecdotal outliers when it sets out to establish the procedural rules relating to the Fourth Amendment and specifically searches incident to arrest.[153] Absent rare circumstances, cell phones generally will not implicate the government's interest of preserving evidence.

Therefore, cell phones, as a category, cannot implicate the need to prevent the destruction of evidence. Unlike physical objects and containers, the data stored in cell phones cannot be irrevocably lost because they are available through alternative sources and can be recovered via current forensic devices.

4. Excluding Cell Phones from *Robinson*'s Bright-Line Rule Will Not Create Confusion

Arguably, excluding electronic data from *Robinson*'s bright-line rule would force officers to engage in fact-specific inquiries while in the field, which would be inconsistent with the Court's policy favoring clear and easily applied rules. Although legitimate, this concern is generally inapposite in the context of electronic data.

Criminal procedure values the "clarity and certainty" provided by a "one size fits all" rule.[154] Key search-incident-to-arrest decisions have relied on this governing principle, noting that an ambiguous rule will impede the enforcement of the law just as much as ambiguous facts.[155] Fact-sensitive exceptions to firm rules have the potential to create uncertainty, but exceptions based on objective

153. *See* J.D.B. v. North Carolina, 131 S. Ct. 2394, 2403 (2011) (accounting for the general characteristics of children rather than looking at the specific characteristics of the child in question); Atwater v. City of Lago Vista, 532 U.S. 318, 354 (2001) (quoting Dunaway v. New York, 442 U.S. 200, 208 (1979)).

154. *J.D.B.*, 131 S. Ct. at 2408–09 (Alito, J., dissenting); Thornton v. United States, 541 U.S. 615, 623 (2004).

155. New York v. Belton, 453 U.S. 454, 459–60 (1981); United States v. Robinson, 414 U.S. 218, 235 (1974).

characteristics that are generally applicable to a whole class will not impede the clarity of a rule.[156]

As discussed above, cell phones do not implicate the twin justifications for searches incident to arrest.[157] The fact that a cell phone's data cannot be used as a weapon and are recoverable despite deletion are objective characteristics about cell phones that are generally applicable to all cell phones. Accordingly, a holding that exempts cell-phone searches from a rule of per se reasonableness will not impede the clarity of the rules that govern searches incident to arrest. The policy rationales underlying *Robinson's* bright-line rule do not compel courts to treat cell phones as "containers."

B. Cell Phones Are Entitled to Heightened Protections Due to the Intrusiveness of a Cell-Phone Search

When assessing the reasonableness of an exception to the warrant and probable cause requirements of the Fourth Amendment, the Supreme Court balances the government's interest in crime prevention with society's privacy interests.[158] When officers undertake more intrusive searches, the Supreme Court has often required a stricter adherence to the Fourth Amendment.[159]

When balancing the public and private interests to determine the reasonableness of a search, the Court often considers what, if any, expectation of privacy was invaded and whether the search was justified by the government's needs.[160] Courts evaluating searches of cell phones incident to arrest have relied on two primary justifications: 1) there is a decreased expectation of privacy following an arrest that justifies a full search of the arrestee's person,[161] and 2) a "lawful custodial arrest justifies the infringement of any privacy interest the arrestee may have."[162]

156. *See J.D.B.*, 131 S. Ct. at 2403–04.

157. *See supra* Part III.A.iii.

158. Terry v. Ohio, 392 U.S. 1, 20–22 (1968).

159. *See, e.g.*, Safford Unified Sch. Dist. No. 1 v. Redding, 129 S. Ct. 2633, 2642 (2009); United States v. Montoya de Hernandez, 473 U.S. 531, 541 (1985).

160. *See, e.g.*, *Montoya de Hernandez*, 473 U.S. at 539–40.

161. People v. Diaz, 244 P.3d 501, 506 (Cal. 2011) (citing United States v. Chadwick, 433 U.S. 1, 16 n.10 (1977)), *cert. denied*, 132 S. Ct. 94 (2011).

162. *Id.* at 507 (citing New York v. Belton, 453 U.S. 454, 460–61 (1981)).

1. Arrestees Do Not Have a Decreased Expectation of Privacy in Cell Phones

Courts have ignored the attributes of items seized during a search incident to arrest because the Supreme Court has justified those searches on the grounds that there is a decreased expectation of privacy following an arrest.[163] However, the constitutionally recognized principles that justify a reduced expectation of privacy during searches incident to arrest should not apply to cell-phone searches.

The Court has stated various circumstances that reduce an individual's expectation of privacy,[164] including when invasions of privacy occur due to governmental needs that exceed general criminal investigations.[165] For example, courts have found that administrative searches may justify investigative searches.[166] However, the Court has often held that one justified invasion of privacy for the purposes of criminal investigation cannot alone authorize additional investigative searches.[167]

Courts have repeatedly stated that searches of an individual's person incident to arrest are justified by a reduced expectation of privacy.[168] However, the Court has failed to provide a valid

163. *See id.* at 506.

164. *See, e.g.*, *Montoya de Hernandez*, 473 U.S. at 537–39.

165. *See, e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 657 (1995) (stating that student athletes have a reduced expectation of privacy because trying out for the team means being subjected to a degree of regulation that requires a preseason physical exam, adequate insurance coverage, a minimum grade point average, and compliance with additional rules of conduct); Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls, 536 U.S. 822, 830–31 (2007) (stating that schoolchildren have a reduced expectation of privacy due to school regulations that require routine physical examinations and vaccinations); New York v. Burger, 482 U.S. 691, 703–07 (1987) (stating that a vehicle-dismantling junkyard has a reduced expectation of privacy due to heavy regulations that subject businesses to meet registration requirements, obtain a license, and make records and inventory available to inspection by the police or an agent of the Department of Motor Vehicles).

166. See *Burger*, 482 U.S. at 702 (stating that industries subject to inspection have a weakened expectation of privacy).

167. *See, e.g.*, Flippo v. West Virginia, 528 U.S. 11, 14 (1999) (stating that an investigation of a murder scene at a home does not authorize a general warrantless search of that home for investigative purposes).

168. United States v. Chadwick, 433 U.S. 1, 16 n.10 (1977); United States v. Edwards, 415 U.S. 800, 808–09 (1974); People v. Diaz, 244 P.3d 501, 506 (Cal. 2011), *cert. denied*, 132 S.Ct. 94 (2011).

constitutional justification for this conclusion.[169] In light of cases that have recognized a heightened expectation of privacy of the individual's person as compared to the areas within an individual's reach,[170] the absence of such a justification is strikingly troubling.[171]

The Court in *Robinson* stated only that a lawful arrest destroys the arrestee's right to privacy to justify an officer's per se authority to search an arrestee.[172] However, as the dissent pointed out, *Chimel* rejected the proposition that one lawful intrusion would justify additional intrusions.[173] As the Court in *Chimel* stated, "[We] can see no reason why, simply because some interference with an individual's privacy and freedom of movement has lawfully taken place, further intrusions should automatically be allowed despite the absence of a warrant that the Fourth Amendment would otherwise require."[174] Therefore, another constitutionally recognized reason must exist to justify the decreased expectation of privacy.

The *Robinson* Court also stated that "a search incident to a lawful arrest is a traditional exception to the warrant requirement."[175] The Court has recognized traditional intrusions as an arena that would warrant a reduced expectation of privacy.[176] However, justifying a search on the grounds of a reduced expectation of privacy caused by the search itself would be unacceptable

169. *See, e.g.*, *Chadwick*, 433 U.S. at 16 n.10; *Edwards*, 415 U.S. at 809 (quoting United States v. DeLeo, 422 F.3d 487, 493 (1st Cir. 1970)); *DeLeo*, 422 F.3d at 493. All three cases state that an arrestee has a reduced expectation of privacy, but none explains the reason for that conclusion.

170. *See* Wyoming v. Houghton, 526 U.S. 295, 308 (1999) (Breyer, J., concurring); United States v. Di Re, 332 U.S. 581, 587 (1948).

171. *Di Re*, 332 U.S. at 587 (explaining that a permissible search of a home or car does not include permission to search the occupants of the home or car even though an occupant could be concealing evidence, because "mere presence" is not sufficient to strip an individual of "immunities from search of his person to which he would otherwise be entitled").

172. *See* United States v. Robinson, 414 U.S. 218, 235 (1973) (stating that "[i]t is the fact of the lawful arrest which establishes the authority to search and "a search incident to that arrest requires no additional justification"); *id.* at 260 (Powell, J., concurring) ("I believe that an individual lawfully subjected to a custodial arrest retains no significant Fourth Amendment interest in the privacy of his person.").

173. *Id.* at 256 (Marshall, J., dissenting) (citing Chimel v. California, 395 U.S. 752, 766 n.12 (1969)).

174. *Chimel*, 395 U.S. at 767 n.12.

175. *Robinson*, 414 U.S. at 224.

176. *See, e.g.*, United States v. Ramsey, 431 U.S. 606, 616–17 (1977).

"bootstrapping."[177] This reasoning also contradicts the reasoning in *Chimel*.[178]

One viable explanation for a decreased expectation of privacy is the administrative consequences of a full custodial arrest. An inventory search is part of the administrative steps of incarceration.[179] An arrestee's items may be searched pursuant to an inventory search.[180] In *Illinois v. Lafayette*,[181] the Court upheld a routine administrative search pursuant to standard police procedures.[182] It stated four governmental interests that support an inventory search: (1) deterring false claims of lost property; (2) reducing incidents of theft or carelessness; (3) preventing weapons from being introduced to the prison system; and (4) helping police identify the arrestee.[183] In *Florida v. Wells*,[184] the Court reemphasized the administrative purpose behind inventory searches by holding that police officers cannot have "uncanalized discretion," and it stated that inventory searches should be designed to "produce an inventory" rather than a "general means of discovering evidence of crime."[185]

The governmental interests supporting an inventory search would not justify a search of the electronic information contained within devices like cell phones. A search designed to "produce an inventory" in order to deter false claims of lost property and prevent the introduction of dangerous instrumentalities would not require the examination and cataloging of data within electronic devices.[186] Although cataloging the device itself would fall within the scope of the general interests of an inventory search, the data on a cell phone

177. *See* New York v. Burger, 482 U.S. 691, 720 (1987) (Brennan, J., dissenting).
178. *Chimel*, 395 U.S. at 766–67 n.12.
179. Illinois v. Lafayette, 462 U.S. 640, 644 (1983).
180. *Id.* at 648.
181. 462 U.S. 640 (1983).
182. *Id.*
183. *Id.* at 646–67.
184. 495 U.S. 1 (1990).
185. *Id.* at 4. Because standard procedures vary, the scope of an inventory search will vary depending on the procedures in place. To address the underlying reasons that justify an inventory search, this Note proceeds assuming that officers conduct every inventory search to the maximum extent possible.
186. United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *11 (N.D. Cal. 2007).

could not possibly contain a dangerous instrumentality, be stolen, or be the subject of a false claim.[187]

Arguably, searches of electronic media stored on devices could help to identify the arrestee. However, inventory searches designed to identify an arrestee have always involved situations in which an arrestee could not be identified by other standard means.[188] Therefore, absent special circumstances, police do not have general authority to use an inventory search to discover identifying information.

Additionally, any official policy that prefers the search of an arrestee's items to standard identification methods would strongly indicate that its purpose was a "general means of discovering evidence of crime" and would therefore be prohibited.[189] Accordingly, an inventory search should not decrease an arrestee's expectation of privacy in the electronic contents of his or her cell phone because law enforcement officials do not have a general authority to search the data within cell phones to recover identifying information.

The Court has cited a decreased expectation of privacy to justify searches of an individual's person incident to arrest,[190] but it has not articulated a clear reason for why an arrest should result in a decreased expectation of privacy. The only rational justification for such a conclusion has no bearing on the expectations of privacy in electronic data contained on cell phones. Thus, the reduced expectation of privacy is merely "a subjective view regarding the acceptability of certain sorts of police conduct"[191] and is an unjustified argument. Furthermore, the only viable argument for a reduced expectation of privacy does not apply to the contents of a cell phone. As a result, to be constitutionally reasonable, a

187. *See, e.g.*, United States v. Wall, No. 08-60016-CR., 2008 WL 5381412, at *4 (S.D. Fla. 2011); *Park*, 2007 WL 1521573, at *11.

188. *See* Commonwealth v. Bowen, 223 N.E.2d 391, 393–94 (Mass. 1967) (upholding a search when the defendant did not have a driver's license and vehicle registration information was inaccessible at that time); State v. Scroggins, 210 N.W.2d 55, 57–58 (Minn. 1973) (upholding a search of the defendant's pocket, which yielded his billfold, when he refused to present identification); State v. Jewell, 469 N.W.2d 247, 1991 WL 74161, at *1 (Wis. Ct. App. 1991) (upholding search of contents of abandoned car when license plates did not match registration information).

189. *Wells*, 495 U.S. at 4.

190. United States v. Chadwick, 433 U.S. 1, 16 n.10 (1977).

191. Chimel v. California, 395 U.S. 752, 764–65 (1969).

sufficiently strong governmental interest must overcome the privacy interest of arrestees.

2. Individuals Have a Greater Expectation of Privacy in Cell Phones

Robinson and its progeny minimize the privacy interests at stake. However, this does not mean that the Court failed to consider the intrusiveness of searches when deciding these cases. Rather, the Court considered only objects limited by their physical characteristics in concluding that a categorical authority to search incident to arrest would involve a minimal intrusion on the privacy interests of individuals.[192] The Court arrived at this conclusion because physical containers that can be immediately associated with the person of an arrestee are small, and their physical capacity inherently limited the intrusiveness of warrantless searches incident to arrest.[193] This assumption likely led the Court to conclude without proof that, absent rare circumstances, searches of vehicles would rarely create a significant intrusion on the privacy of individuals.[194] However, modern cell phones are regularly used for the most intimate aspects of an individual's life and surpass the inherent limitations and boundaries of physical containers.[195]

Recent decisions have recognized that modern cell phones have the capacity to store vast amounts of information and often contain "the most sensitive kinds of personal information, in which individuals may reasonably have a substantial expectation of privacy

192. *See, e.g.*, United States v. Robinson, 414 U.S. 218, 236 (1973) (addressing the search of a cigarette package); Belton v. New York, 453 U.S. 454, 461 n.4 (1981) (explicitly defining a container as any object capable of holding another object).

193. *See* California v. Acevedo, 500 U.S. 565, 574 (1991) (stating that requiring officers to obtain a warrant before searching a paper sack found in a vehicle during a valid vehicle search would "provide[] only minimal protection for privacy and have impeded effective law enforcement").

194. Wyoming v. Houghton, 526 U.S. 295, 303 (1999) (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974)). The Court subsequently retreated from this characterization in *Arizona v. Gant*, 129 S. Ct. 1710, 1720 (2009).

195. City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2630 (2010); Ben E. Stewart, *Cell Phone Searches Incident to Arrest: A New Standard Based on* Arizona v. Gant, 99 KY. L.J. 579, 580 (2011).

and for which the law offers heightened protection."[196] Even the Supreme Court has recognized the intimate nature of cell phones, stating that "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."[197] This characterization is particularly relevant for teenagers who have grown up in the digital age. Surveys show that over 75 percent of teenagers carry a cell phone on a daily basis and use text messaging as a way to communicate personal matters.[198] These teens commonly use cell phones for private communication and will likely continue to use their cell phones in this manner into adulthood.[199]

Moreover, the data within electronic devices can increase even after the arrestee is no longer in control of them.[200] For instance, police officers have answered a defendant's cell phone when the phone received an incoming call after the defendant's arrest.[201] Officers have also used cell phones to obtain additional evidence against an arrestee through incoming text messages received after the arrest.[202] Some phones are able to automatically retrieve e-mails and

196. Smallwood v. State, 61 So. 3d 448, 461 (Fl. Dist. Ct. App. 2011), *cert. granted*, 68 So. 3d 235 (Fla. 2011) (citing *Hawkins*, 704 S.E.2d 886, 891 (Ga. App. Ct. 2010)); *Hawkins*, 704 S.E.2d at 891, *aff'd*, 723 S.E.2d (Ga. 2012); *see also* People v. Diaz, 244 P.3d 501, 513 (Cal. 2011) (Werdegar, J., dissenting) ("A contemporary smartphone can hold hundreds or thousands of messages, photographs, videos, maps, contacts, financial records, memoranda and other documents, as well as records of the user's telephone calls and Web browsing. Never before has it been possible to carry so much personal or business information in one's pocket or purse."), *cert. denied*, 132 S. Ct. 84 (2011); United States v. Park, No. CR 05-375 SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007); Oxton, *supra* note 59, at 1201 (stating that modern cell phones can store massive amounts of private information and describing the capabilities of the iPhone 3GS).

197. *Quon*, 130 S. Ct. at 2630.

198. Amy Vorenberg, *Indecent Exposure: Do Warrantless Searches of a Student's Cell Phone Violate the Fourth Amendment?*, 17 BERKLEY J. CRIM. L. 62, 63, 78 (2012).

199. *Cf.* Press Release, CTIA, National Study Reveals How Teens Are Shaping & Reshaping Their Wireless World. Study Sheds New Light on Teens' Cell Phone Habits, Expectations & Dream Phone Wishes (Sept. 12, 2008), *available at* http://ctia.org/media/press/body.cfm/prid/1774 (describing how cellular telephones have impacted teenagers and their expectations for the future).

200. *See* State v. Carroll, 778 N.W.2d 1, 12 (Wis. 2010); *see also* United States v. Gomez, 807 F. Supp. 2d 1134, 1137–39 (S.D. Fla. 2011) (describing an officer answering a call received after he had seized the cell phone and using the defendant's cell phone to exchange text messages with a third party); United States v. Davis, 787 F. Supp. 2d 1165, 1169 (D. Or. 2011) (describing an officer answering a call that was received after the officer had seized the defendant's phone).

201. *Gomez*, 807 F. Supp. 2d at 1138–39; *Davis*, 787 F. Supp. 2d 1165; *Carroll*, 778 N.W.2d at 12.

202. *Gomez*, 807 F. Supp. 2d at 1139–40.

other data,[203] which is yet another feature that police officers may take advantage of when investigating arrestees.[204] Therefore, electronic devices are further distinguished from any of their physical counterparts because the content of electronic devices may potentially expand, even when an arrestee is already in police custody.

Cell phones do not comport with the physical limitations of standard containers contemplated in *Robinson*; their contents are not limited by the physical restrictions in the way that the contents of standard containers are, making cell-phone searches a far greater invasion of privacy than searches of standard containers. With the infinite amount of private data contained on a cell phone and its ability to continue to collect additional private information, a search of a cell phone's data would likely be a severe intrusion into the most intimate details of a person's life.[205] Accordingly, the cell phone should be subject to a heightened expectation of privacy.

3. The Government's Interest Fails to Overcome the Heightened Expectation of Privacy

Although *Belton* categorically stated that "[a] lawful custodial arrest justifies the infringement of any privacy interest,"[206] *Belton* explicitly defined a container as "any object capable of holding another object."[207] While cases have relied on *Belton*'s rationale to authorize searches of the contents of cell phones,[208] physical containers have inherent limitations that make searches of them far less intrusive than searches of cell phones. Therefore, an analysis of a cell-phone search that relies on the *Belton* rationale would be shallow and faulty because it would ignore key distinguishing

203. *See iPhone*, APPLE, http://www.apple.com/batteries/iphone.html (last visited Oct. 22, 2011) (discussing how reducing data and e-mail retrieval may extend battery life).

204. *See Gomez*, 807 F. Supp. 2d at 1139–40.

205. Smallwood v. State, 61 So. 3d 448, 461 (Fl. Dist. Ct. App. 2011) ("[C]ell phones can make the entirety of one's personal life available for perusing by an officer every time someone is arrested for any offense.").

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

207. *Id.* at 460 n.4.

208. *See, e.g.*, People v. Diaz, 244 P.3d 501, 507 (Cal. 2011), *cert. denied*, 132 S. Ct. 94 (2011); People v. Nottoli, 130 Cal. Rptr. 3d 884, 904 (Ct. App. 2011).

features, namely the breadth and nature of information,[209] at the heart of Fourth Amendment concerns.

Furthermore, electronic devices do not implicate the policy rationales underlying searches incident to arrest. Rather, searches of cell phones incident to arrest require a novel examination of the police and privacy interests at stake because such searches are not tethered to the underlying rationales that originally justified the search-incident-to-arrest doctrine.[210]

Few, if any, governmental interests support searching the data on a cell phone incident to arrest. The only identifiable police interests would be a need for a clear, bright-line rule that encompasses the electronic data of cell phones and a greater authority for crime prevention.[211] However, the needs that justify a bright-line rule are inapplicable in the cell-phone context because cell phones do not present inherently ambiguous situations regarding potential weapons or the potential destruction of evidence; excluding cell phones would not blur the bright-line rule. Furthermore, the remaining police interest in general crime prevention, although compelling, must yield to the Fourth Amendment.

On the other hand, the privacy interests at stake are exceptionally high due to the intimate nature and sheer volume of the content of cell phones.[212] Cell phones implicate great privacy concerns due to the breadth of information they contain and their ability to continue to expand their content even when outside of the owner's control.[213]

A fresh balancing of the governmental and privacy interests shows that the blanket authority to search a cell phone incident to arrest is not reasonable. Cell phones implicate heightened privacy concerns demanding greater Fourth Amendment protections. Additionally, they do not trigger the concerns about officer safety and loss of evidence that justify other searches incident to an arrest. Finally, the police interest in bright-line rules does not provide a

209. *Smallwood*, 61 So. 3d at 461.

210. *See* Arizona v. Gant, 556 U.S. 332, 343–46 (2009).

211. *See Belton*, 453 U.S. at 459–60 (stating that citizens cannot know the scope of their constitutional rights and that police officers cannot know the scope of their authority when a doctrine is not settled); United States v. Robinson, 414 U.S. 218, 235 (1973) (stating that officer decisions are usually ad hoc decisions and need not be subsequently scrutinized by the courts).

212. *See supra* Part III.B.2.

213. *See supra* Part III.B.2.

strong argument for a categorical authority to search cell phones incident to arrest. One court agreed, stating the following:

> The bright-line rule established by *Robinson* may have been prudent at the time, given the finite amount of personal information an arrestee could carry on his or her person or within his or her reach. However, the *Robinson* court could not have contemplated the nearly infinite wealth of personal information cell phones and other similar electronic devices can hold.[214]

4. The Fourth Amendment Requires a Retreat from *Robinson*'s Unqualified Authority to Search Cell Phones Incident to Arrest

A principal purpose of the Fourth Amendment is to prohibit general warrants that authorize police officers to arbitrarily search individuals.[215] The bright-line rule in *Robinson*, when combined with the vast amount of information that can be accessed by cell phones, enables officers to engage in the "unrestrained and thoroughgoing examination of [an arrestee] and his [or her] personal effects" that the *Chimel* Court condemned.[216] The current rules governing searches incident to arrest essentially authorize and encourage such behavior, which is antithetical to the principles behind the Fourth Amendment.

A significant risk of abuse arises when the wealth of information stored in cell phones collides with the broad authority of police officers to search an arrestee incident to arrest.[217] The evidentiary interest supporting searches incident to arrest is virtually limitless[218] and essentially authorizes the type of unrestricted search that Judge

214. *Smallwood*, 61 So. 3d at 461.

215. *Gant*, 556 U.S. at 345 ("A rule that gives police the power to conduct [an unjustified] search . . . creates a serious and recurring threat to the privacy of countless individuals. Indeed, the character of that threat implicates the central concern underlying the Fourth Amendment—the concern about giving police officers unbridled discretion to rummage at will among a person's private effects."); Chimel v. California, 395 U.S. 752, 761 (1969).

216. *See Chimel*, 395 U.S. at 764 (quoting Sibron v. New York, 392 U.S. 40, 67 (1967)).

217. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring); United States v. Robinson, 414 U.S. 218, 248 (1973) (Marshall, J., dissenting); *see Chimel*, 395 U.S. at 767–68.

218. 3 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 5.2 (4th ed. 2011).

Learned Hand stated was "indistinguishable from what might be done under a general warrant."[219] The dissent in *Robinson* recognized that granting a broad authority to conduct investigative searches provides police officers with a tremendous incentive to arrest individuals for minor offenses, such as traffic violations, as a pretext to search for evidence of other offenses without a warrant.[220]

Furthermore, because searching privately-owned cell phones is inexpensive,[221] this authority is even more susceptible to abuse because it escapes one of "the ordinary checks that constrain abusive law enforcement practices: limited police resources."[222] Worse yet, even though the courts have recognized the impropriety of using arrests as a pretext to search for evidence,[223] the Court in *Whren v. United States*[224] essentially eliminated any legal prohibitions on such a practice and has left private citizens without a remedy.[225]

IV. PROPOSAL

The expansion of the search-incident-to-arrest doctrine seems to reflect a judicial reluctance to exclude credible evidence.[226] The cases that expand the search-incident-to-arrest exception have always involved situations in which the admissibility of evidence was highly probative of a defendant's guilt.[227] These decisions were likely colored by the potential consequence of "set[ting] the criminal loose in the community without punishment."[228] Under these circumstances, the judiciary's willingness to narrow procedural protections is not surprising.[229] Even lower courts that disagree with

219. United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926).

220. *Robinson*, 414 U.S. at 248 (Marshall, J., dissenting).

221. *Cf. Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (discussing GPS tracking as opposed to traditional police surveillance).

222. *Id.* (quotation marks omitted) (citing Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

223. *Robinson*, 414 U.S. at 248 (Marshall, J., dissenting).

224. 517 U.S. 806.

225. *See id.* at 812–13.

226. Davis v. United States, 131 S. Ct. 2419, 2427 (2011) ("Exclusion exacts a heavy toll on both the judicial system and society at large . . . [because] its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment.").

227. *See, e.g.*, New York v. Belton, 453 U.S. 454, 456 (1981) (finding evidence of cocaine in a jacket); *Robinson*, 414 U.S. at 222–23 (finding evidence of heroin within a cigarette package).

228. *Davis*, 131 S. Ct. at 2427.

229. Moran v. Burbine, 475 U.S. 412, 457 (1986) (Stevens, J., dissenting) ("The cost of suppressing evidence of guilt will always make the value of a procedural safeguard appear 'minimal,' 'marginal,' or 'incremental.' . . . The individual interest in procedural safeguards that

Supreme Court precedent often hesitate to distinguish cases.[230] This attitude resulted in the doctrine that wholly departs from the principles of the Fourth Amendment, a problem that can now be remedied only at the Supreme Court level.[231]

Although cell phones have been the primary focus of recent decisions, the same analogies seen in cell-phone cases have been applied to other devices, though not in the context of searches incident to arrest. Courts have already justified searches of other advanced technologies by applying poor functional analogies or disregarding their characteristics.[232] To restore fidelity to the Fourth Amendment, the Supreme Court must make a new doctrine for electronic devices that (1) prohibits courts from applying outdated approaches to modern technologies and (2) restricts the tremendous potential for abuse. Without a rule that restricts searches of the data stored on cell phones and other technological devices in the future, citizens will be "at the mercy of advancing technology."[233] However, the rule must maintain clarity and eliminate the need for officers to conduct a fact-sensitive inquiry in order to determine the scope of their authority.

minimize the risk of error is easily discounted when the fact of guilt appears certain beyond doubt.").

230. *See, e.g.*, Smallwood v. State, 61 So. 3d 448, 460 (Fla. Dist. Ct. App. 2011), *cert. granted*, 68 So. 3d 235 (Fla. 2011); People v. Diaz, 244 P.3d 501, 517 (Cal. 2011) (stating that if precedents need to be reevaluated to account for modern technology, only the Supreme Court may do so), *cert. denied*, 132 S. Ct. 94 (2011). *But see* State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009).

231. *See, e.g.*, Arizona v. Gant, 129 S. Ct. 1710, 1721 (2009) (rejecting the broad reading of *Belton* as an "anathema to the Fourth Amendment").

232. 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."); United States v. Arnold, 533 F.3d 1003, 1009–10 (9th Cir. 2008) (upholding the suspicionless search of a laptop at the border because the quality and nature of a laptop is irrelevant to the Fourth Amendment analysis). *But see* United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008) (quoting United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001)) ("[B]ecause computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the intermingling of documents and a consequent invasion of privacy when police execute a search for evidence on a computer." (original quotation marks and brackets omitted)); United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (stating that analogizing a computer to a file cabinet "may be inadequate," and that relying on such analogies "may lead courts to oversimplify a complex area of Fourth Amendment Doctrines and ignore the realities of massive modern computer storage" (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 104 (1994)) (original quotation marks omitted)).

233. Kyllo v. United States, 533 U.S. 27, 35 (2001).

Though scholars have advanced many proposals, they fail to address the concerns that attend to searches incident to arrest in the modern era. The most effective approach to restore fidelity to Fourth Amendment principles would be to restrict the applicability of *Robinson* and its progeny to physical containers only and to address new technologies based on general Fourth Amendment principles that govern searches incident to arrest.

A. Flaws of Prior Proposals

Prior proposals that address searches of digital media on cell phones fail to account for one or more of the concerns stated above. One scholar suggests drawing a distinction between older generation cell phones and new "smartphones," requiring a warrant for "smartphones" and distinguishing between coding and content-based information stored on older cell phones.[234] The scholar further suggests using the presence of a touch screen or a full keyboard as "an easily ascertainable line of distinction."[235]

Although this suggestion proposes a seemingly clear rule, cell phones are constantly evolving and its distinction may not be relevant in the near future.[236] Already, over two thousand cell phone models are available in the United States alone.[237] Additionally, this distinction presupposes that older generation cell phones lack the storage capacity and access to information of new generation cell phones.[238] Moreover, this rule would be impractical because it would require police officers to determine whether a phone is new or old generation.[239]

Other suggestions include (1) limiting the search to a set number of "steps," in which, for example, opening a file would constitute a step, or (2) distinguishing between data stored on the device and

234. Orso, *supra* note 138, at 221–22. Orso defines coding information as data that "reveals only the identity of a party to a communication without disclosing the subject matter of that communication." *Id.* at 188. He also defines content-based information as "the subject matter of a communication as well as privately stored data reserved for one's personal use." *Id.* at 193.

235. *Id.* at 222.

236. Snyder, *supra* note 140, at 181.

237. *Id.*

238. *Id.* at 181–82.

239. State v. Smith, 920 N.E.2d 949, 954 (2009) ("[I]t would not be helpful to create a rule that requires officers to discern the capabilities of a cell phone before acting accordingly.").

remotely stored data that are accessible from the device.[240] However, both of these suggestions are severely flawed.

The "steps" approach has no constitutional basis, is entirely arbitrary, and would lead to "fuzzy inquiries" regarding what constitutes a step.[241] Furthermore, there would be no principled way to determine the appropriate number of steps. In addition, this method presupposes that more private data take more "steps" to access. However, because private data are often located in commonly used features, such as e-mail, text messaging, call logs, and stored phone numbers,[242] phones can be configured to provide quick access to those features.[243]

Permitting searches incident to an arrest based on where the data are actually stored creates practical problems. Officers would be required to understand how cell phones store data, and certain pieces of data would blur the lines. For instance, if a cell phone accesses e-mails and stores them locally for quick access, would this data be considered locally or remotely stored? The potential ambiguities make this approach impractical, and an officer is ill equipped to distinguish between remote and local data without specialized knowledge that is most likely outside of his or her area of expertise.

Others have proposed a rule that follows *Arizona v. Gant*.[244] *Gant* addressed vehicle searches incident to arrest and crafted a rule based on "circumstances unique to the automobile context."[245] The Court authorized searches of vehicles incident to arrest in situations in which an arrestee could still reach the passenger compartment of a vehicle or the officer had a reasonable belief that "evidence of the offense of arrest might be found in the vehicle."[246]

Although this rule may be appropriate in the vehicle context, this standard could be susceptible to abuse when applied to cell phones. The breadth of information stored in a cell phone, especially

240. Gershowitz, *supra* note 34, at 54–57. Gershowitz also discusses other potential solutions in his paper that are not discussed in this Note. *Id.* at 45–57.

241. *Id.* at 54–55.

242. City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2630 (2010).

243. *E.g.*, *Windows Phone: Pin Things to Start*, MICROSOFT, http://www.microsoft.com/windowsphone/en-us/howto/wp7/start/pin-things-to-start.aspx (last visited Feb. 28, 2012).

244. 129 S. Ct. 1710 (2009); Stewart, *supra* note 195, at 598.

245. *Gant*, 129 S. Ct. at 1714.

246. *Id.*

its stored communications, would allow officers to claim that they reasonably believed that an arrestee's cell phone contained evidence of the crime. For example, an officer could claim that an arrestee's cell phone contained communications with suspected accomplices. Thus, this standard is susceptible to abuse and may not provide a meaningful constraint on police authority. Furthermore, a reasonableness standard involves a fact-based analysis that does not clearly define the scope of an officer's authority.

Another scholar proposed that courts follow *State v. Smith*, which categorically prohibits warrantless searches of cell phones incident to arrest and forces officers to rely on other traditional exigencies.[247] The California legislature took a similar approach with SB 914.[248] The limitations on police conduct pursuant to SB 914 would be similar to the holding in *State v. Smith*, in that officers would not be able to search a cell phone without a warrant or an exigent circumstance.[249]

Although both *Smith* and SB 914 are steps in the right direction, the categorical prohibition of warrantless cell-phone searches fails to address one of the core problems that taints the current jurisprudence of cell-phone searches incident to arrest: the tendency of courts to poorly analogize novel technologies to standard containers in an effort to bring them within the scope of *Robinson*.

B. A Simple and Effective Approach to Reconnect Searches Incident to Arrest with Fourth Amendment Principles

In order to reconnect searches incident to arrest with Fourth Amendment principles, the Supreme Court must take a more drastic approach than simply limiting the applicability of *Robinson* to cell phones. It should restrict *Robinson*'s rule to physical containers only, and when addressing novel technologies, courts should engage in a fresh balancing of the interests at stake rather than analogize to

247. Snyder, *supra* note 140, at 180–81.

248. Amy Gahan, *California Governor Allows Warrantless Search of Cell Phones*, CNN (Oct. 11, 2011), http://articles.cnn.com/2011-10-11/tech/tech_mobile_california-phone-search-veto_1_cell-phones-smartphone-text-messages?_s=PM:TECH. Governor Brown subsequently vetoed this bill, much to the dismay of its supporters. *Id.*

249. State v. Smith, 920 N.E.2d 949, 956 (Ohio 2009); Bob Egelko, *Bill Would Require Warrant to Search Cell Phone*, SF GATE (July 4, 2011, 4:00 AM), http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/07/04/BAQF1K3SVJ.DTL.

precedent. Without a rule that restricts the application of old precedents to novel technologies, citizens will be left "at the mercy of advancing technology."[250]

After *Robinson*, searches incident to arrest operated outside of Fourth Amendment principles.[251] When combined with the wealth of private information stored on cell phones,[252] *Robinson* created a tremendous incentive to abuse searches incident to arrest.[253] Furthermore, limited police resources will not provide a check on this abuse, as officers can search privately-owned devices easily and inexpensively.[254] Restricting *Robinson* and its progeny to only physical containers will minimize the incentive for officers to utilize abusive tactics because it would prevent officers from accessing cell phone data.

Additionally, this approach would still allow officers to engage in reasonable searches. Physical containers are inherently ambiguous and might contain hidden weapons that threaten an officer's safety or physical evidence that can be destroyed.[255] These situations implicate the twin concerns underlying a search incident to arrest,[256] and the inherent ambiguities surrounding physical containers necessitate a bright line rule, especially when officer safety is at stake.[257]

250. Kyllo v. United States, 533 U.S. 27, 35 (2001); *see also* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (questioning whether old Fourth Amendment doctrines are "ill suited to the digital age").

251. *See* United States v. Robinson, 414 U.S. 218, 235 (1973); *id.* at 239 (Marshall, J., dissenting) ("In the present case, however, the majority turns its back on [Fourth Amendment] principles, holding that 'the fact of the lawful arrest' always establishes the authority to conduct a full search of the arrestee's person, regardless of whether in a particular case 'there was present one of the reasons supporting the authority for a search of the person incident to a lawful arrest.'").

252. *See, e.g.*, *Smith*, 920 N.E.2d at 955; *see also* Smallwood v. State, 61 So. 3d 448, 461 (Fla. Dist. Ct. App. 2011) (stating that cell phones and other electronic devices hold an "infinite wealth of personal information"); Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1169 (D. Or. Jan. 18, 2012) (stating that a rule authorizing searches of electronic devices incident to arrest would put "any citizen . . . at risk of having his or her most intimate information viewed by an arresting officer.").

253. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("[T]he Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.").

254. *Id.* (citing Illinois v. Lidster, 540 U.S. 419, 426 (2004)) (stating that limited police resources is an ordinary constraint on abusive police conduct).

255. *See supra* Part III.A.2.

256. Chimel v. California, 395 U.S. 752, 762–63 (1969).

257. *See* United States v. Robinson, 414 U.S. 218, 234 n.5 (1973).

Moreover, physical containers implicate minimal privacy concerns. The physical dimensions of a container necessarily limit the intrusiveness of a search,[258] and containers are subject to a decreased expectation of privacy because all physical items are within the scope of an administrative inventory search.[259] Therefore, the broad authority to search physical containers is reasonable because the police interests in preserving evidence, protecting officers, and clarifying uncertain situations outweigh the privacy interests at stake.

On the other hand, the balance of factors compels data stored on cell phones to be categorically excluded from searches incident to arrest.[260] Electronic data on cell phones cannot hide weapons, and any information they contain would be very difficult to erase permanently.[261] Remote wipe applications may increase the threat of losing data, but an officer can remove the battery or cut off the signal without searching the cell phone to address that risk.[262] Because electronic data fall outside the scope of an inventory search, they are not subject to a reduced expectation of privacy.[263] Furthermore, categorically excluding data stored on cell phones will not create uncertainty because electronic data are clearly distinguishable from the contents of a physical container.

This analysis strongly suggests that data on all electronic devices should fall outside the scope of a search incident to arrest. New technologies share many characteristics with modern cell phones.[264] Even older technologies, such as pagers, have advanced to the point that the concerns expressed in *United States v. Ortiz* may be outdated.[265] Additionally, a rule that excludes all electronic devices would eliminate the need for officers to categorize devices. However, even without a blanket rule governing electronic devices, an officer may address uncertain situations by obtaining a warrant

258. *See supra* Part III.A.1.

259. *See supra* Part III.B.1.

260. *See supra* Parts III.A.3 and III.B.1.

261. *See supra* Part III.A.3.

262. *See supra* Part III.A.3.

263. *See supra* Part III.B.1.

264. *iPad: Technical Specifications*, APPLE, http://www.apple.com/ipad/specs/ (last visited Feb. 26, 2012).

265. United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996); *see, e.g.*, *Advisor II: Overview*, MOTOROLA, http://www.motorola.com/Business/US-EN/Business+Product+and+Services/Two-Way+Radios+and+Pagers+-+Business/Pagers/Advisor+II_US-EN (last visited Feb. 27, 2012).

with minimal risk of evidence loss. If circumstances present a high likelihood that evidence will be destroyed, an officer may still rely on other exceptions to the warrant requirement.[266]

V. CONCLUSION

When old Fourth Amendment doctrines collide with modern technologies, once-reasonable decisions create unreasonable results. Prior courts crafted rules without considering the technologies available today. Modern courts have continued to apply these precedents but have not considered the implied limitations of prior decisions that often make their reasoning inapplicable to the unique qualities of modern technologies. When combined with a judicial reluctance to exclude relevant evidence, doctrines expand and deviate from Fourth Amendment principles. Searches incident to arrest are no exception to this result and have been expanded to allow officers to conduct highly invasive searches without any procedural safeguards.

The Supreme Court must restrict the search-incident-to-arrest doctrine so that searches of cell phones, and all future technologies, do not become general warrants that authorize police officers to intrude into the most intimate details of an individual's life. The Court must take action to ensure that modern devices do not eviscerate the fundamental protections at the core of the Fourth Amendment.

266. Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).